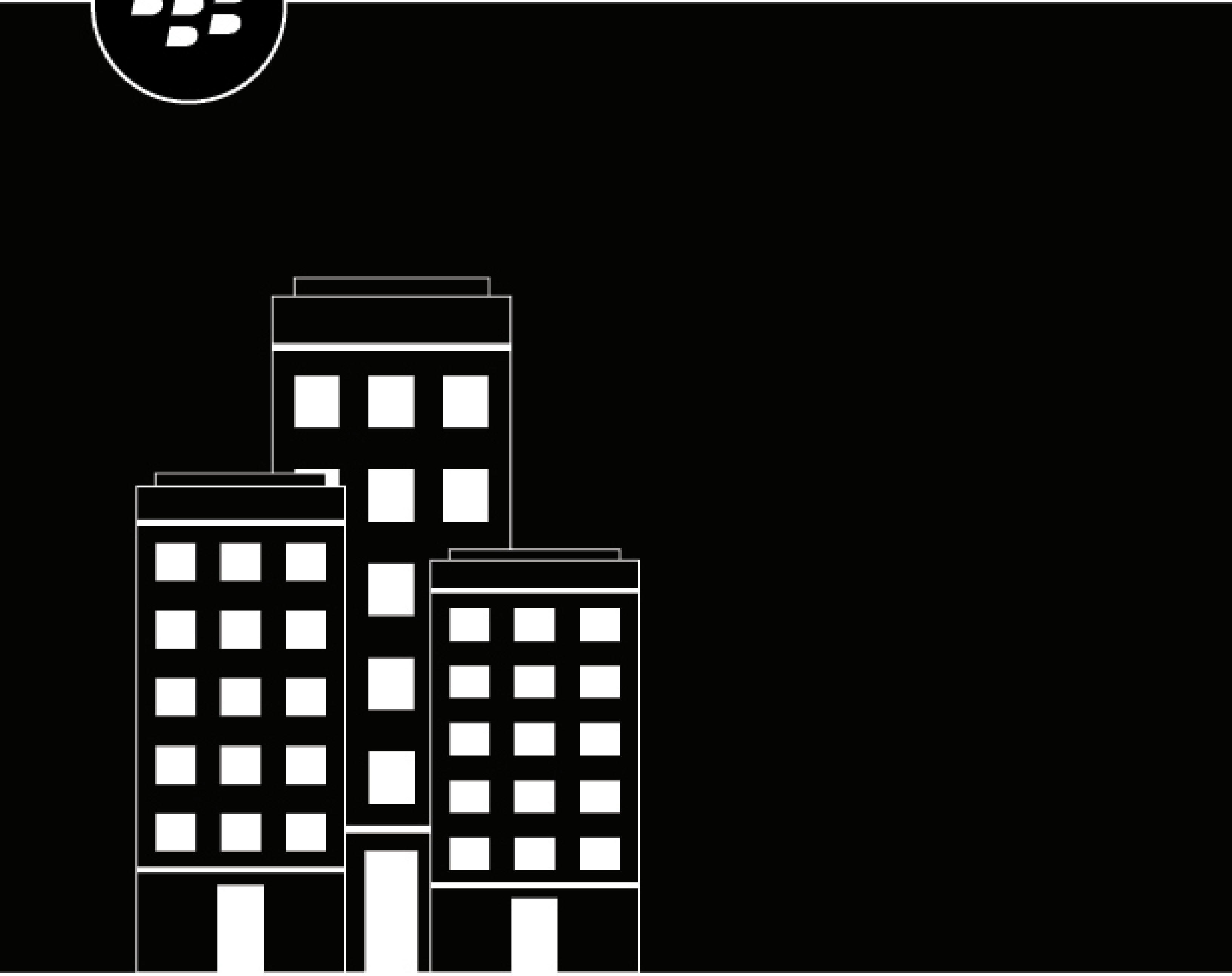

BlackBerry AtHoc

Release Notes

7.21 (OnPrem)

Contents

What's new in BlackBerry AtHoc 7.21 (OnPrem)

These release notes contain information about new and changed functionality for BlackBerry® AtHoc® release 7.21 (OnPrem). For more information about BlackBerry AtHoc or its related functionality, see the BlackBerry AtHoc documentation here: https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc.

Alerting

- **Alert Approval**
  - Use the alert approval publishing flow when you need to have a second operator review, approve, and publish an alert.
  - Alert templates that require approval are indicated by a .
  - The alert approval publishing flow can only be used for alerts that are published manually by an operator.
  - Alert approval cannot be used to publish an alert that is being used in a Connect or weather alert rule, or in mobile alert settings.
  - An entry is added to the Operator Audit Trail when a notification is sent to the alert approvers and when an alert approver approves and publishes an alert.
- **Area name export**: When an end user performs a check-in or check-out on the mobile app, BlackBerry AtHoc now matches the latitude/longitude of the location with imported shape files and updates the check-in or check-out with the values in the shape file. A new Shape Name column was added when exporting entries from the Inbox.
- **Dynamic Hierarchy personnel reports**: Personnel reports can now be created for dynamic hierarchy attributes. The hierarchy levels and values are displayed in a list in the Value column and as a bar chart. For more information, see "Create a personnel report based on a user attribute" in the *BlackBerry AtHoc Alert Tracking and Reporting* guide.
- **Email device preview and formatting**: Operators can preview and format email alert templates. Alert publishers can preview and edit email alerts during publishing. For more information, see "Preview and publish an alert" in the *BlackBerry AtHoc Create and Publish Alerts* guide and "Create an alert template" in the *BlackBerry AtHoc Alert Templates* guide.
- **Geo-aware Single-select picklist attribute**: The number of attribute values was limited to 2000. The attribute value import logic was improved to support batch processing of Geo-aware Single-select picklist attributes.
- **Locale search for delivery templates**: A new "Locale" search pull-down list was added to the Delivery Templates settings screen. This enables operators to search for delivery templates assigned to a specific locale. This new "Locale" search can be used in conjunction with the existing search capabilities on the Delivery Templates settings screen to enhance the ability to find and manage delivery templates.
- **Localized delivery templates**: BlackBerry AtHoc now supports desktop and email delivery templates for the following delivery locales:
  - Arabic
  - Chinese
  - Greek
  - Japanese
  - Korean
  - Polish
  - Portuguese (Brasil)
  - Portuguese (Portugal)
  - Russian
  - Swedish

- Turkish

  This update ensures that users can select any of the supported delivery locales and receive fully translated desktop and email notifications. The desktop and email delivery templates are available for the five severity levels (High, Moderate, Low, Informational, and Unknown) and match the associated delivery colors.
- **New delivery locales**: BlackBerry AtHoc now supports 5 new delivery locales: Malay, Vietnamese, Slovak, Hindi, and Indonesian. The 5 new locales are also available for bilingual alerting and can be selected from a pull-down menu in the BlackBerry AtHoc management system at General Settings > Customization > Delivery Locales.

  BlackBerry AtHoc now supports a total of 24 delivery locales. Desktop and email templates to support all delivery locales were added. A new Locale search pull-down menu was added to the Delivery Template settings page.
- **Sent alerts summary**: The tooltip that is displayed when hovering-over the title of an alert on the Sent Alerts page was updated to include the Alert ID.
- **Special characters in response options for desktop alerts**: The following special characters in response options result in a tracking status of "Other" for alerts received on the desktop app: `!$%^(){}=,,;\:?"'<>
- **Targeting by advanced query**: When targeting using an advanced query, an OR condition is included between geolocation targeting and any additional advanced queries.
- **Zoom level for map**: The zoom level for a map added in an alert was increased to a 200 feet-per-inch scale to show greater detail when a single point is being displayed.

Alert templates

- **Alert rule warning**: If an operator edits an alert template that is currently being used in an active alert rule, and the edits would cause the template to no longer be ready to publish, a message is now displayed informing the operator that their changes will deactivate the alert rule.
- **Alert template export and import**: Administrators can now export and import alert templates and share them with suborganizations. For more information, see "Import or export an alert template" in the *BlackBerry AtHoc Alert Templates* guide.

  Note: If an imported alert template contains a More Info link without http:// in the URL, clicking the Test URL button results in a 404 error.
- **Alert template history**: A new "Version History" button was added to the Alert Template screen. When clicked, the "Version History" button opens a window that displays the history of changes made to the alert template, including:

  - The specific fields that were changed (for example, Title, Body, Response Options, Targeted Users, and Devices)
  - The original and updated values for each changed field
  - The operator who made the change
  - The date/time of the change

  This feature is available to Organization Administrators, Enterprise Administrators, and System Administrators. If the alert template has "Inheritable" mode enabled, the Version History button is hidden for organizations that inherit the template.
- **Alert template type**: A new "Exercise" type was added for alert and accountability event templates.
- **Inheritable check box**: The "Inheritable" check box is no longer displayed on the Alert Template screen when creating a template in a suborganization.
- **Location check box**: In the alert template settings, if the Location check box is selected on the Content tab and the operator unchecks the enable targeting By Advanced Query check box in the Target Users tab and clicks Apply, an error message is displayed and the change cannot be applied.

- **Updated On column**: A new sortable "Updated On" column was added to the alert template manager page. For more information, see "Access the Alert Templates screen" in the *BlackBerry AtHoc Alert Templates* guide.

API

New APIs

The following APIs were added:

- **POST /orgs/{orgCode}/template**: Creates a new alert template.
- **POST: /orgs/{orgCode}/Alerts?action=publish**: Publishes a new alert.

Modified APIs

- The following APIs were modified to support bilingual alert publishing:
  - **GET /orgs/{orgCode}/alerts/{auId}**: Returns alert details for the specified organization.
  - **GET /orgs/{orgCode}/alerttemplates/{templateCommonName}**: Returns alert template details for the specified common name.
  - **POST /orgs/{orgCode}/alerts**: Publishes an alert using a template.
- **GET /orgs/{orgCode}/DeliveryTemplates/{DeliveryTemplateCommonName}**: This API was updated to include "None" for the EntranceMotion option.
- **OrgUsers API enhancement**: The OrgUsers API was updated to enable users to retrieve information about both sponsor and dependent users. Previously, the OrgUsers API did not pull dependent information into the user profile. The OrgUsers basic and advanced search endpoints now enable the retrieval of both sponsor and dependent user information and assign it to the user profile.
- **POST /orgs/{orgCode}/AccountEvent**: This API was updated to fix an issue where an accountability event fails to publish when the targeted users list includes either disabled or deleted users.

AtHoc Account

- **Account folders**: Account folders were introduced to help operators manage their accountability templates more efficiently before, during, and after accountability events. Key features include:
  - A System Default folder that all out-of-the-box and new accountability templates are assigned to.
  - A new Account Folders manager that can be accessed from the General Settings and Account sections of the BlackBerry AtHoc management system.
  - Operators with access to AtHoc Account can create, edit, and delete account folders.
  - Operators can assign accountability templates to account folders, with folders inherited from the enterprise and super-enterprise levels.

  For more information, see "Manage account folders" in the *BlackBerry AtHoc Account* guide.
- **Account folder restrictions**: BlackBerry AtHoc now supports the ability to organize accountability events with account folders. This enables administrators to restrict groups or divisions to an account folder that contains their specific accountability templates. Account Managers, Enterprise Administrators, Plan Managers, and Plan Incident Managers can be assigned access to specific account folders. An Account Folder section was added above the Distribution Lists folder section on the Operator Permissions page, allowing for restricted or unrestricted access to accountability events. Folder restrictions limit operators to view only the accountability events assigned to the folders they have been granted access to.

- **Accountability Officer initial email delivery template update**: The Accountability Officer initial email delivery template was updated to include a deep link that allows Accountability Officers to access Self Service and update user information for accountability events started at the enterprise or super enterprise levels. This deep link provides AOs with the ability to update user responses and add notes for accountability events that originate at the enterprise and super enterprise levels, based on their assigned AO roles, subscriptions, and restrictions. The Self Service page accessed through the deep link allows AOs to search for users by name and status, view User Status and Comment fields, and update the status and comments while the accountability event is still active. Once the accountability event ends, the edit functionality is longer available. This update ensures that AOs have the necessary access and tools to effectively manage user information for accountability events across all organizational levels.
- **Accountability Officer organization subscriptions**: When granting an existing operator the Accountability Officer role from the External Operator Permissions screen, the Organization Subscription section is displayed only if the operator account exists in the same enterprise organization. If the operator account is from a different enterprise, the Organization Subscription section is not displayed.
- **Accountability Officer role enhancements**: In a super enterprise configuration, the Accountability Officer role can now be assigned at the suborganization level. Accountability officers can respond on behalf of users from accountability events started at all levels of the enterprise (suborganization, enterprise organization, and super enterprise) without needing additional roles to be assigned.

  Operators granted the Accountability Officer external operator role and subscribed to a suborganization can be targeted in accountability events and can respond on behalf of users from accountability events at all organization levels in a super enterprise organization.

  Accountability Officers can respond on behalf of users based on their roles in the suborganization, enterprise organization, or super enterprise organization. Any user base restrictions assigned to the operator with the Accountability Officer role are applied at the organization level where they were assigned and from the organizations above (enterprise and super enterprise organizations.)

  If you assign an operator the Accountability Officer role in a suborganization, that operator can access the enterprise or super enterprise organization so that they can respond on behalf of other users during an accountability event. When the Account Officer role is assigned, the first time an operator logs in to the management system, they are taken automatically to the Change Organization page and must select an organization. On subsequent logins, the operator will automatically be logged in to the organization where they last logged out from.

  Accountability Officers can log into the organization where the accountability event was started, access the Account and All Events tabs, view events, and update users from the BlackBerry AtHoc management system and from the mobile app during a live event. User base restrictions are applied, and only allowed users are visible to the Accountability Officer.
- **API support for placeholders for accountability templates**: Operators can now add placeholders to their accountability templates to customize the event name and details. The following JSON payload fields were added to support placeholders in accountability templates:

  - <Placeholders>: This field contains one or more Placeholder nodes. The Placeholder tag searches for placeholders added in the header, body, and response options fields and replaces them with the provided values.
  - <Placeholders.Key>: The name of the Placeholder.
  - <Placeholders.Value>: The replacement value for the placeholder. The placeholder value can be one of these types: Text, Date, Timer, DateTime, Single-selection, Multiple-selection.
- **Automatically subscribe to organizations when the Accountability Officer role is granted from External Operator Permissions**: When granting the Accountability Officer (AO) role from the External Operator Permissions settings page, the operator is now automatically subscribed to the associated organization. This ensures that the AO has access to user accounts to update user status and can be targeted in accountability events. The subscription selection is only available when assigning the AO role at the suborganization level. There is no subscription option when granting the AO role at the enterprise or super enterprise levels. The

subscription is for the organization that the External Operator Permission is granted from. The start date for the subscription will be recorded and displayed as read-only on the External Operator Role page. If the AO role is revoked, the subscription remains and must be manually revoked from the organization where the user account was created. The Operator Audit Trail displays when the AO role is assigned or revoked, as well as when the subscription is revoked from the user profile.

- **Enhanced web API for Accountability Officers to respond on behalf of others**: Accountability Officers can now respond on behalf of users for accountability events published at the enterprise and super enterprise level using the BlackBerry AtHoc mobile app. Accountability Officers can update the User Status and Comment fields for accountability events at the enterprise or super enterprise level even if the Accountability Officer role is only assigned at the suborganization level. The user experience for Accountability Officers remains the same when managing users through the mobile app, regardless of the organization context of the accountability event.
- **Export accountability events**: Accountability events can now be exported from the Accountability Events page to a CSV file. For more information, see "Export accountability events" in the *BlackBerry AtHoc Account* guide.
- **Placeholders for accountability event templates**: Operators can now add placeholders to Accountability Event templates. Using placeholders enables customizing the event name and details to the specific situation. Operators can select from existing alert placeholders and add them to the Event Name and Event Description fields. When publishing an Accountability Event, a new "Custom Fields" section enables operators to fill in the placeholder values, which are then resolved and included in the event messages.
- **Respond on behalf of others in Self Service**: Self Service was updated to display the user list and response options for Accountability Officers targeted from an accountability event started at the enterprise or super enterprise level. Accountability Officers can now access and update users through Self Service. The Self Service page provides AOs a way to view, update, and provide comments on all users assigned to them from any suborganization below an enterprise or super enterprise. This functionality is based on the AO's role, subscriptions, and restrictions at the suborganization level. Operator Audit Log entries are captured when an AO logs in to the Self Service page, accesses users from an accountability event at the enterprise or suborganization level, updates users, or logs out.
- **Retain columns on Users tab**: Any columns that an operator adds on the Users tab of an Accountability Event summary page are retained after navigating away from the Users tab. Added columns are displayed only to the operator who added them.
- **Self Service drop-down for suborganizations**: Accountability Officers with subscription and external operator permissions to multiple suborganizations can now access accountability alerts from the Inbox in Self Service to view and update users across those organizations. A drop-down list allows Accountability Officers to select the appropriate organizations when an event is started at the enterprise or super enterprise level. User base subscriptions applied to the Accountability Officer in the external operator role are now applied to the Accountability Officer in each suborganization. The sending organization name is displayed in the Accountability Event Details section to assist in identifying the originating organization.
- **Target Accountability Officers**: The ability to add Accountability Officers in an accountability template or event by distribution list, advanced query, and location was added. For more information, see "Add Accountability Officers" in the *BlackBerry AtHoc Account* guide.

AtHoc Connect

- **Attachments in Connect alerts**: Alerts sent to Connect organizations can now include attachments. The attachments appear with the alert in the Inbox in the target organization and can be viewed or downloaded. When an incoming Connect or mobile app alert from a connected organization triggers another alert, any attachments in the incoming alert are not included in the triggered alert.
- **Connect alerts with attachments**: Incoming Connect alert rules that trigger Connect alerts with attachments are sent immediately after all attachments are received, or after ninety seconds. If any attachments are not processed within the ninety seconds, they are not included in any triggered Connect alerts. The attachments will appear in the Inbox with the received alert after they are processed.

- **Severity setting**: When a Connect alert triggers another alert, the severity of the incoming alert no longer overwrites the severity of the triggered alert template. Previously, the severity of the incoming alert overwrote the severity of the triggered alert. The $SenderSeverity$ placeholder was created to display the severity setting of the incoming alert.
- **Support for Call Bridge**: Call bridge numbers and their passcodes in Connect alerts are now shared across organizations.

BlackBerry Feed Service (V2)

New feed types: The following feed types were added to the BlackBerry Feed Service (V2):

- Transportation
  - Public Transit Delays
  - Road Closure
  - Traffic Advisory
  - Transportation Disruption
- Safety
  - Active Shooter
  - Carjacking
  - Evacuation
  - Police Activity
  - Robbery
  - Shooting
  - Stabbing

These feed types are supported in Virginia, Maryland, and Washington D.C. only.

Browser support

BlackBerry AtHoc release 7.21 supports the latest versions of the following browsers: Edge, Safari (Mac), Chrome, and Firefox.

Collaboration

Collaboration error: Customers who see a "*[2005] Collaboration session could not be accessed. Please try again.*" error when attempting to start a Collaboration can work around this issue by whitelisting the following URL on their reverse proxy server: https://*.bbmenterprise.com.

Integrated Weather Alerts

- **Additional weather types**: The following weather types were added:

  - High Surf Warning
  - Hurricane Force Wind Warning
  - Hurricane Force Wind Watch
  - Hydrologic Advisory
  - Hydrologic Outlook
  - Ice Storm Warning
  - Lake Effect Snow Advisory
  - Lake Effect Snow Watch
  - Lakeshore Flood Advisory
  - Lakeshore Flood Statement
  - Lakeshore Flood Warning
  - Lakeshore Flood Watch
  - Law Enforcement Warning
  - Local Area Emergency
  - Low Water Advisory
  - Marine Weather Statement
  - Nuclear Power Plant Warning
  - Radiological Hazard Warning
  - Red Flag Warning
  - Shelter In Place Warning
  - Short Term Forecast
  - Small Craft Advisory For Hazardous Seas
  - Small Craft Advisory For Rough Bar
  - Small Craft Advisory For Winds
  - Small Stream Flood Advisory
  - Storm Warning
  - Storm Watch
  - Test
  - Tropical Depression Local Statement
  - Tropical Storm Local Statement
  - Tsunami Advisory
  - Typhoon Local Statement
  - Typhoon Warning
  - Typhoon Watch
  - Urban And Small Stream Flood Advisory
  - Wind Chill Warning
  - Winter Weather Advisory

  To view all supported weather alert types, see "Weather Types" in the *BlackBerry AtHoc Integrated Weather Alerts* guide.
- **Integrated Weather Alerts filtering**: Test alerts sent from the NWS CAP system are now automatically filtered out from Integrated Weather Alerts to prevent end users from receiving too many irrelevant test alert messages.

Live map and geo-targeting

- **Geo-aware single-select picklist attribute**: Administrators can now create geo-aware single-select picklist attributes that allow end users to specify their location by selecting an alias value instead of entering a full address. For more information, see "Create a geo-aware single-select picklist attribute" in the *BlackBerry AtHoc Manage Users* guide.
- **Last Known Location attribute**
  - The ability to clear Last Known Location attribute data for all users in an organization was added.
  - The Last Known Location attribute now includes the ability to select a time frame to apply to the attribute when selecting it in advanced queries for user targeting.
- **Live map shape file**: A descriptive error message displays on the Map Settings > Add Shape Layer dialog if an attempt is made to import a shape file that contains invalid parameters.
- **Live map updates**
  - Individual external events are displayed on the External Events section in the External Layers panel. These events can be hidden or displayed on the live map from the External Layers panel.
  - External events received in the Inbox contain a link that opens the live map with the relevant external layer and event selected.
  - Clicking on an event on the live map displays a details pop-up.
  - The automatic refresh interval for external events on the live map was increased to 5 minutes.

  For more information, see the *BlackBerry AtHoc Live Map* guide.
- **Location pins on the Live Map**: Alerts and accountability events can now be displayed on the Live Map with location pins. Location pins can be added when creating an alert or event template or when publishing an alert or event. A pin icon (📍) was added to the Create Custom Locations toolbar on the publisher map to add location pins.

Location pins are indicated by a 📍 on the Live Map and are displayed only for live alerts and events. Operators can add a brief description of up to 30 characters for each location pin and can click on a pin to move it to a different location. Multiple location pins can be added as part of a single alert or event.

Location pins cannot be used to target users or organizations.

Location pins displayed on the Live Map are visible at all zoom levels. The pin description text appears when the location pin is moused over. At maximum zoom, location pins are consolidated and a circle indicates the number of live alerts or events in close proximity. When a location pin is clicked on the Live Map, the alert or event details are displayed.

Management system

- **Advanced reports performance**: The load time for advanced reports for sent alerts in organizations that have a large number of sent alerts was improved.
- **Alert placeholders**: When an alert is published, a space is now automatically inserted before any placeholder values to prevent text from running together. Previously, no space was added automatically.
- **Attribute value import**: The help text on the "Import Values" dialog that appears when importing attribute values was improved to provide additional information about reordering values in an existing attribute.
- **BlackBerry AtHoc notification to PSS about device deletion**: BlackBerry AtHoc now makes a call to the Personal Safety Service (PSS) when a device is deleted, using intervals and job batching to provide this information. This ensures that the PSS can then make a call to the mobile app about the device deletion, allowing the mobile app to display a relevant error code to the end user.
- **CSV Export for User Tracking Report - with Events**: BlackBerry AtHoc now enables operators to export the "User Tracking Report - with Events" advanced report to a CSV file. An "Export this Report" option has been added, which allows users with the appropriate permissions to download the full report contents to a CSV file named "UserTrackingwithEvents.csv". The exported CSV file includes all rows and columns from the report, with date fields displayed in date/time formats.
- **Desktop Popup behavior options (Windows only)**: For Desktop Popup delivery templates, in the Popup Settings section, the option to choose "None" for the Entrance Motion was added. When this option is selected, the alert immediately appears in the selected location of the screen without motion. The Exit Motion option was removed.
- **Distribution list folders**: The Distribution List Folders section is now available on the Users tab on the top navigation bar, making it more accessible for operators. This change ensures that operators with the appropriate roles (Enterprise Administrator, Organization Administrator, or System Administrator) can access and manage distribution list folders more easily. Operators without these roles will not see the Distribution List Folders section.
- **Dynamic hierarchy attribute**: A new dynamic hierarchy type of user attribute was added. Dynamic hierarchy attributes are linked attributes that are displayed as a single field in a user profile but contain multiple levels of data. Operators can create and modify dynamic hierarchy attributes and define the levels and values (nodes) in them. When an operator or end user selects a dynamic hierarchy attribute, they can step through a selection of levels within the attribute. When a user selects an attribute node, the next available selections are dependent on the selected node. For more information, see "Create a dynamic hierarchy attribute" in the *BlackBerry AtHoc Manage Users* guide.
- **Dynamic hierarchy attribute search**: The "is empty" and "is not empty" operators can now be used for dynamic hierarchy attributes in advanced searches in the BlackBerry AtHoc management system.
- **Fallback authentication option for desktop app**: The option to fall back to Windows Authentication for the desktop app was added. When selected, Windows Authentication is used if the authentication method for the desktop app is set to "LDAP attribute" and authentication with LDAP fails.

- **Geofence refresh enhancements**: The geofencing refresh rates were enhanced to enable operators to gain additional real-time situational response awareness. The geofence refresh rate enhancements have cut delays by about 70%. The system refresh now detects new users in a geofence every 3 minutes.
- **Increased organization subscriptions**:Users can now subscribe to up to 50 organizations within an enterprise or super enterprise. Previously, users could subscribe to up to 10 organizations.
- **Imperial and metric measurement units**: Operators can define the default measurement unit (Imperial or Metric) displayed on the Live Map for their organization. Shapes then reflect the selected area in either miles or kilometers.
- **Improved export of users with dependents**: When exporting users, the "Include all Dependents of selected Sponsors" option now correctly includes the dependent records in the export count and data. The export now includes all sponsors and their dependents, with the count accurately reflecting the total number of users exported.
- **Improved Mac client version parsing**: The server has been updated to parse the existing Mac client version format in the request header. The expected format is now: "bb-athoc/[version] (macintosh-macos; [OS version]; [Mac model]; [locale]; Apple) c:none". This change ensures that the server can correctly identify the Mac client version without requiring customers to update to a new version.
- **Improved operator export functionality**: The error message displayed when attempting to export only disabled operators has been updated to provide clearer guidance to users. When exporting a mix of enabled and disabled operators, the message has been updated to indicate that disabled operators will not be included in the export.
- **LDAP authentication enhancements for the desktop app**: The desktop app now supports a custom LDAP URL field on the User Authentication page. This allows users to override the LDAP root node when using LDAP authentication. The custom LDAP URL field is formatted to accept only valid URLs in the format LDAP://<DOMAINNAME>.<TOP-LEVELDOMAIN>:<(Optional) PORT#>. For more information, see "Desktop App" in the *BlackBerry AtHoc Manage Users* guide.
- **Mobile App Work and Personal devices**
  - **New Mobile App - Work device**: Two distinct device types are now available for the mobile app: Mobile App - Work and Mobile App. End users who register through MDM can automatically be assigned to the Mobile App - Work device type. Users who register manually are assigned to the Mobile App device type. This separation of devices types enables operators to send alerts to either work devices, personal devices, or both, ensuring that sensitive content can be sent only to users' work devices.
  - **Publishing and user response tracking for Mobile App - Work device**: Alerts and accountability events can be sent to the Mobile App - Work device. Operators can target the Mobile App - Work device and configure notification settings such as repeat notifications, pause between notifications, and sound delivery. Operators can also view and track alert responses from the Mobile App - Work device. The Mobile App - Work device is displayed in the Sent Alert Details, Delivery Distribution by Devices, and User Tracking reports.
  - **Advanced search support for Mobile App - Work device**: BlackBerry AtHoc now supports searching for the Mobile App - Work device. Users can target advanced queries based on the status (Active, Inactive, or Select all) of the new device. The Mobile App - Work device can be selected as a column in table views and displayed in user profiles, showing the status and details of the device.

    The Mobile App - Work device is searchable in these advanced search areas:

    - Alert template - user targeting
    - New alert - user targeting
    - Accountability template - user targeting
    - Accountability template - Accountability Officer targeting
    - New accountability event - user targeting
    - Static Distribution Lists - user selection advanced queries

    The Mobile App - Work device is also searchable in these areas:

    - Accountability event summary
    - Users manager
    - Dynamic distribution lists (when selecting membership criteria)
    - Auto disable and delete users
    - User base restriction
  - **API support for the Mobile App - Work device**: The following APIs support the Mobile App - Work device:
    - **GET /devices and GET /devices/{deviceId}**: Returns the details of the Mobile App - Work device.
    - **GET /orgs/{orgcode}/devices**: Returns the details of the Mobile App - Work device if it is active.
    - **POST /orgs/{orgCode}/users/search/advanced**: Supports user search for the Mobile App - Work device. Conditions include equals, not equals, is empty, and is not empty for the Active, Inactive, and Not Available values.
    - **GET /orgs/{orgCode}/users/{loginId}/profile**: Returns the device status for the specified profile with values of Active, Inactive, or Not available.
    - **POST /orgs/{orgCode}/alerts**: Supports the Mobile App - Work device as a targetable device by its common name in the request format of TargetUsers.PersonalDevices.Devices.DeviceCommonName and TargetUsers.PersonalDevices.DeviceGroupOptions.
    - **GET & PUT /orgs/{orgCode}/alerts/{auId}**: Supports the Mobile App - Work device as a targetable device by its common name in the request format of TargetUsers.PersonalDevices.Devices.DeviceCommonName and TargetUsers.PersonalDevices.Devices.Options and TargetUsers.PersonalDevices.DeviceGroupOptions.
    - **GET /orgs/{orgCode}/alerts/{auId}/reports/devicesummary**: Support for the Mobile App - Work device that displays its tracking summary for a specified alert.
    - **GET /SelfService/{orgCode}/Devices**: Supports the Mobile App - Work device as a device that displays its details in this endpoint if it is enabled.
    - **GET & PUT /SelfService/{orgCode}/{loginId}/Profile**: Supports the Mobile App - Work device as a device that displays in this endpoint if it is enabled.
- **More Info link field update**:

  The automatic "http://" prefix was removed from the "More Info" link field when a placeholder (indicated by $) is used as the first character. When an operator enters a standard URL in the "More Info" link field, the "http://" prefix will continue to be added automatically. When an operator uses a placeholder in the "More Info" link field, the "http://" prefix is no longer added automatically. Any placeholder entered in the "More Info" link field are saved as-is, without any additional prefixes or text. This ensures that when a receiving organization sets up an alert template with a placeholder in the "More Info" link field, it can correctly display the URL provided by the sending organization's alert template.

  The "Test URL" button continues to function, but displays an error if a placeholder is used instead of a valid URL.
- **Operator audit trail updates**
  - Data in the operator audit trail is now retained for 12 months. Previously, it was retained for 6 months.
  - The Move Users dialog now logs the "Move locked users" and "Lock all users after move" actions in the operator audit trail. This provides more detailed tracking of user move activities.
  - When a deleted user is recovered, a "Deleted Users Recovered" entry is recorded in the operator audit trail.
- **Organization contact information**:
  - Administrators can now provide the name, email, and phone number of an organization's administrator or help desk to assist users with administrative tasks such as resetting or retrieving their passwords.
  - Administrators can customize the Organization Contact Info section in the BlackBerry AtHoc management system at Settings > General Settings.
  - Organization contact information is displayed on the login, username retrieval, and password retrieval pages to assist users in the BlackBerry AtHoc management system, Self Service, and on the mobile app.

- Organization contact information is also displayed at the bottom of the BlackBerry AtHoc management system homepage welcome message.

  For more information, see "Customization" in the *BlackBerry AtHoc System Settings and Configuration* guide.

- **Organization hierarchy values for users in subscribed organizations**: An issue where stale organization hierarchy values were displayed in the user manager for users in subscribed organizations was resolved. Additionally, users in a subscribed organization could be incorrectly targeted using advanced queries that referenced the organization hierarchy node they previously belonged to.

  Organization hierarchy values displayed in the user manager list view are now kept up-to-date and advanced queries in the subscribed organization only target users based on their current organization hierarchy assignment.
- **Password reminder notification updates**:

  - Operators and users can now receive email reminders prior to their password expiring.
  - Administrators can configure the number of days before expiration that the reminders are sent (15, 10, 7, 5, 4, 3, 2, or 1 days.)
  - By default, reminders are sent 7, 5, 3, 2, and 1 days before expiration.
  - Enable the password expiration reminder in the BlackBerry AtHoc management system at Settings > Setup > Security Policy > Password Update Rules.

  For more information, see "Send a reminder before a password expires" in the *BlackBerry AtHoc System Settings and Configuration* guide.
- **Prevent operators from deleting or disabling their own account**: BlackBerry AtHoc was updated to prevent operators with user manager permissions from deleting or disabling their own user accounts through the "Disable and Delete Users" settings page. Operators with any of these roles can no longer delete or disable their own account even if they have included it in a disable or delete rule: Alert Manager, Advanced Alert Manager, End Users Manager, Enterprise Administrator, Organization Administrator, and Basic Administrator. If an operator attempts to delete or disable their own account, a warning message is displayed informing them that they cannot perform this action on their own user account. The "Selected users" count excludes the operator's own account, and the "Deleted or Disabled users" count will be reduced by 1 to account for the operator's account being skipped. This change ensures operators cannot accidentally or intentionally remove their own access to the BlackBerry AtHoc system, improving security and preventing service disruptions.
- **Preview and Save page**: A Reset Content button was added to the Preview and Save page that enables operators to reset edits made to alert content for Email delivery.
- **Publisher map user export**: Batch user exporting was added to the publisher map. When exporting more than 25,000 users, operators must select a batch of users to export from a drop-down menu. Only 25,000 users can be exported from the publisher map in a single export.
- **Recover deleted users**: End Users Managers, Organization Administrators, and Enterprise Administrators can now recover deleted users for up to 7 days after deletion. The recovery period is dependent on the Purge Deleted Users setting in the Disable and Delete Users settings section. Deleted users cannot be recovered after they are purged from the system. Operators cannot delete their own user accounts. The operator audit trail captures the names of deleted users and the operator who performed the deletion.
- **Redirection support across different desktop app authentication methods**:

  - Customers can now configure redirection between systems with Windows Username and Smart Card authentication.
  - Customers can now redirect desktop clients between systems with different desktop software authentication methods, such as Windows Username and Smart Card.
  - This update resolves an issue where desktop clients could not connect when redirected between systems with different authentication methods.
  - The limitation of requiring the same desktop software authentication method in both organizations has been removed.

- **Self Service logout in the operator audit trail**: User logouts from Self Service are now captured in the operator audit trail. Previously, only login attempts from Self Service were captured in the operator audit trail.
- **Sent alerts**: The default order of alerts displayed on the Sent Alerts page was updated so that live alerts are displayed before draft, scheduled, or ended alerts. Previously, draft and scheduled alerts were displayed before live alerts.
- **Service operator accounts**: A new Service Account option was added to operator profiles. Use this option to designate an operator account as a service account for use with features such as the API, User Sync, or SMS Opt-In. Service accounts cannot be disabled, deleted, or have their operator permissions revoked automatically. For more information, see "Grant operator permissions to a user" in the *BlackBerry AtHoc Operator Roles and Permissions* guide.
- **Setting pages UI updates**: The UI of the following System Setup setting pages was updated:

  - System Jobs
  - Database Archiving
- **Status attribute for deleting users**: The Status attribute is now available for selection in the Delete Users section on the Disable and Delete Users settings screen. This enables organizations to use the Disabled status as a criteria for deleting users. Users with a Disabled status can now be automatically deleted. The Status attribute is available with the following operations: equals and not equals. The available values for the Status attribute are: Select All, Disabled, and Enabled.

  The Status attribute is not available in the Disable Users section.
- **Translation for custom device names**:

  - On the Custom Translation screen, a new "Translation Type" option was added, enabling users to choose between translating devices or attributes.
  - When "Devices" is selected, a new typeahead-enabled "Select Device" drop-down list is displayed, with Personal and Mass Devices grouped separately.
  - The "Select Device" drop-down list shows all enabled personal and mass devices.
  - A new table displays translation fields for Language, Name, Alert Targeting Help Text, Contact Info Help Text, and Tooltip.
  - Clicking "Save" will save all translation changes for both Devices and Attributes.
- **User move and organizational hierarchy**: When a user is moved, their position in their 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.
- **User Last Updated attributes**: The following User Last Updated attributes can now be exported as part of a user export:

  - User Last Updated On
  - User Last Updated By
  - User Last Updated Source

  These attributes are system-created attributes and are not supported in user imports.

Mass devices

New CAP Feed device: A new CAP Feed device was added. The CAP Feed device is a collection of multiple CAP feed payloads which can be accessed through a single URL by mass devices such as digital signs. Operators can use the CAP feed device to render alerts based on the values of CAP payload fields such as category, event, type, urgency, severity, and certainty. For more information, see "CAP Feed" in the *BlackBerry AtHoc System Settings and Configuration* guide.

Section 508-compliance improvements

- 508-compliance improvements for keyboard navigation, text-to-speech readability, color contrast, image accessibility and form elements were made in the following areas:
    - Advanced searches
    - Alert Preview and Publish page
    - Alert Preview and Save page
    - Change Organization page
    - Change Password page
    - Custom attribute translation accessed from the Users menu
    - Feature Enablement settings page
    - Live Map
    - Log In page
    - My Profile page
    - New distribution list and edit a distribution list pages
    - Operator audit trail
    - Operator permissions profile page
    - Profile edit page
    - Sent Alerts page
    - Top navigation bar
    - User attribute manager accessed from the Users menu
    - User manager page
- 508-compliance improvements for keyboard navigation were made in the following areas:
    - Diagnostic Log settings page
    - Inbox
    - Personnel Reports
    - System Jobs settings page

Self Service

Section 508 compliance improvements: The following section 508 compliance improvements were made:

- The contrast ratio on the top navigation bar was improved to 5.92.
- A missing header for the Prioritize Personal Devices column on the Dependents page was added.
- A missing header for the Attachments column on the Inbox page was added.

Server platforms

Upgraded server platforms: BlackBerry AtHoc now supports SQL Server 2022 and Windows Server 2022. Upgrading to the latest server versions enables organizations to benefit from the latest security and performance improvements. The updated server platforms are fully supported for both BlackBerry AtHoc 7.21 OnPrem and cloud releases.

Smart card authentication

- **Smart card authentication clarification**: Clarifying help text was added to the User Authentication page to better explain Smart Card authentication options. The "Enabled Authentication Methods" section now includes a description for the Smart Card option, stating "Selecting this option will make Smart Card authentication usable for Mobile App, Desktop App, and Self Service. Management System authentication can be controlled in the Security Policy." The "Management System Authentication Method" drop-down list now includes a description stating, "To select Smart Card as an Authentication Method, go to the Security Policy."
- **Support for custom CAC certificate attributes**: BlackBerry AtHoc now supports the ability to specify custom attributes for CAC (Common Access Card) certificates. Users can configure these attributes when selecting Smart Card as the authentication method for an application. This enables customers to use their CAC certificates even if the format differs from the default supported format. The Custom Attribute field is not mandatory, supports up to 100 characters, and does not allow the use of < and > special characters.

SMS Opt-In

- **SMS vanity codes**: Support for SMS vanity short and long codes by account was added.
- **Support for French (fr-CA)**: The SMS Opt-In feature now supports the French (fr-CA) locale.

Super Enterprise

The Super Enterprise enables enterprise-scale organizations to combine their currently splintered organizations under one organization enabling advanced administration. With the super enterprise, users can build out a risk intelligence map for their organization.

- **User management and organization subscription**
  - Users can subscribe to different suborganizations within their super enterprise.
  - Enterprise Administrators and Organization Administrators can move users across enterprises and suborganizations within their super enterprise.
  - Super enterprise operators can easily search for users across their enterprises and identify which organization they belong to.
- **Alerting and accountability**
  - Operators can publish an alert to all enterprises and suborganizations in their super enterprise.
  - Operators can select and deselect users in all enterprises and suborganizations when publishing an alert from the super enterprise.
  - Super enterprise operators can view live and sent alerts across their enterprises and suborganizations from the super enterprise level.
  - At the super enterprise level, operators get a comprehensive look at current live alerts and accountability events across their enterprises and suborganizations from the live map.
- **Reporting**

  Aggregated Personnel, Alerts Usage, and User Summary reports from all enterprises and suborganizations are visible from the super enterprise.
- **Inheritance**
  - Administrators in super enterprise and enterprise organizations can now create alert templates in the super enterprise or enterprise and configure them to be inherited to their sub enterprises and suborganizations.
  - Alert folders and alert placeholders created in a super enterprise organization are now automatically inherited by sub enterprises and suborganizations.

For more information, see "Inherited content and settings in the enterprise or super enterprise" in the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide.

Users

View, edit, and export dependents

- When the dependents feature is enabled, dependents can be viewed from the user manager page.
- A new filter was added to the Users screen to filter users by Sponsors and Non-Sponsors, Sponsors, or Non-Sponsors. When the "Sponsors and Non-Sponsors" or "Sponsors" filter is selected, the Include Dependents option is displayed.
- When dependents are displayed in the user manager, click the Sponsor column to sort users by sponsor. Dependents are displayed beneath their sponsors.
- Click a displayed dependent to edit the dependent's user profile.
- Individual dependents displayed in the user manager can be deleted from the More Actions pull-down menu.
- Dependent users can only be disabled, enabled, or moved from the More Actions pull-down menu.
- When dependents are displayed, if a sponsor is exported, their dependents are also exported.

Behavior changes

Behavior changes are changes in existing functionality that you need to be aware of when upgrading to BlackBerry AtHoc release 7.21 (OnPrem.) These changes require that you re-learn existing functionality.

- **Accountability alert targeting validation**: BlackBerry AtHoc now validates the status of affected users before allowing an accountability alert to be published. If only blocked users are targeted as affected users, the accountability template is marked as not ready to publish, preventing the alert from being sent to zero recipients. Previously, the accountability template displayed as Ready to Publish even when all affected users were blocked.
- **Accountability event duplication**: Alerts sent as part of accountability events cannot be duplicated. Alerts sent as part of an accountability event are indicated on the Sent Alerts page with a 👤✓.
- **Accountability event recurrence**: Accountability templates that are configured to recur and have a next occurrence date set must have affected users and devices selected for the scheduled accountability event to publish. If affected users or devices are removed from the accountability template, the scheduled accountability event does not start and has the recurrence setting removed. This prevents accountability events from being published without affected users or targeted devices. Previously, accountability events could be published without any affected users or targeted devices when an accountability template configured with recurrence was updated to remove the affected users or targeted devices.
- **Accountability Officer enhancements**:
  - The Initial Message must now be selected whenever one or more Accountability Officers are selected for an accountability event.
  - If Accountability Officers are selected but the Initial Message is unchecked, the Accountability Officer section status is set to Not Ready, preventing the accountability event from being started until the Initial Message is checked.
  - The Ending Message option is available only if the Initial Message is checked and Accountability Officers are selected.
  - If no Accountability Officers are selected, the Accountability Officer section is not required and the accountability event can still be published.
- **Accountability template readiness**: To be ready to publish, accountability templates must have an Initial Message, a Reminder Message, or an Ending Message selected in the User Messages and Workflow section.
- **Alert publishing**: When a user publishes an alert, their "Last Updated On" attribute is no longer updated.
- **Alert Publisher role updates**: Operators with Alert Publisher permissions cannot access the Advanced Reports or User List on the Sent Details page of an alert. Operators with the Advanced Alert Publisher role can still access these features. The Advanced Reports button and User List button are now hidden or disabled for operators who have only the Alert Publisher role. A tooltip is displayed on hover, indicating that the operator does not have the necessary permissions and should contact their administrator. The Add Column button in the User Targeting panel is also hidden or disabled for operators with only Alert Publisher permissions, with a similar tooltip displayed on hover.
- **Alerts API extension**: The following API was extended to return complete end dates: /api/v2/orgs/{orgCode}/alerts/{auId}
- **Alert template severity setting**: Previously, if the severity of an alert or alert template was changed to High, the "Recipient Does Not Answer the Call" personal device option was changed to "Leave callback information." Now, changing the alert or alert template severity does not alter the "Recipient Does Not Answer the Call" setting.
- **API alert publishing**: When an alert being published via API included targeted users that were disabled or deleted in BlackBerry AtHoc, the alert would fail. Now, a new validation check filters out any users that are not in the "Enabled" status, ensuring that only valid, active users are included. The 200 status response payload was enhanced to include a new "TargetUser.Failed" field so that the alert publisher can identify targeted users that were rejected.

- **Attribute value length limit for response options**: A 64-character limit on attribute values used as response options was added. If an attribute value exceeds this limit, an error message is displayed, and the attribute is not saved until the value is shortened or the "Use as a Response Option" setting is unchecked. This helps ensure that response options fit within the character limit for alerts.
- **Bilingual alerts**:
  - When Bilingual is selected in an alert template, the Content section is ready even when there are no response options. Previously, response options were required for bilingual alerts.
  - BlackBerry AtHoc now supports delivering bilingual alerts using the preferred language templates for email and desktop notifications. When a bilingual alert is sent, the selected second language uses the corresponding email and desktop locale templates to ensure the message is fully displayed in the user's preferred language. The severity level also matches the delivery locales in both languages. If no delivery template exists for the selected language, the system defaults to the organization locale. Bilingual alerts do not support custom delivery templates. This enhancement ensures that users receive alerts in their preferred language.
- **BlackBerry AtHoc API documentation update**: The API documentation link on the Help & Support page was updated to point to the latest Swagger v2 documentation at /api/v2/docs/. The previous documentation at /athoc-iws/OpenAPI/services/main/index.html is no longer supported.
- **Change Organization screen updates**:
  - Click anywhere in a row other than the link in the Name column to change to an organization.
  - Organization filters were added. Click the All Organization link to open a pull-down menu and select an organization type to filter the list of organizations.
  - An Organization Hierarchy dialog was added. Click the name of an organization in the Name column to open the Organization Hierarchy window. From there you can view the organization hierarchy or click the Manage Organization Hierarchy button to open the Organizations Manager.
  - A Switch button was added to the Change Organization screen. Clicking the Switch button or on the row for an organization opens the change organization dialog.

  Note: If the Change Organization screen is blank, clear your browser cache and try again.

  For more information, see "Change organization" in the *BlackBerry AtHoc Operator Quick Start* guide.
- **Confirmation dialog for Scheduled Alert edit**: When an operator updates a scheduled alert on the Sent Alerts pages, edits the Schedule section, and then clicks Save, the Review and Publish dialog is displayed. Previously, clicking Save published the alert.
- **Dependents display**: Administrators can view dependent users grouped by their sponsors by selecting the Include Dependents option on the Users page. Administrators can export the sponsors and their dependents to a CSV file.
- **Enhanced IIM mass device capabilities**: The following mass devices were enhanced to support pre-recorded audio, pre-tones, post-tones, and text-to-speech:
  - Federal Signal
  - ATI
  - SiRcom
  - Whelen V2
  - American Signal V2
  - Monaco
  - Motorola ACE3600
- **Extended GetOperators API to filter by object ID**: The /orgs/{orgCode}/operators API endpoint was updated to return results based on a specified organization code and object ID. The updated API endpoint now returns operators based on object ID.
- **Fill count in geofence targeting**: Geofence alerts can now use fill counts. Previously, when geofence targeting was enabled, fill count was disabled.

- **FIPS code validation and delivery for IPAWS alerts**: An issue where IPAWS alerts were rejected due to FIPS codes that fall outside of the customer's approved alerting jurisdiction was fixed. This update ensures that IPAWS alerts include all necessary FIPS codes without restrictive validations, IPAWS alerts are successfully delivered, and the risk of IPAWS rejections due to jurisdictional issues is reduced.
- **Hide Password reset**: If the authentication method for Self Service is set to anything other than Username/Password, the Password section is not displayed in Self Service by default. If the authentication method for Self Service is Username/Password, the Password section is displayed in Self Service by default. This section can be hidden by removing it in General Settings > Layouts > User Details - My Profile.
- **Improved alert response reporting**: BlackBerry AtHoc was updated to address delayed reporting of alert responses. When an operator refreshes the Alert Summary Report page, the system checks for new data in the database and recalculates the report data if necessary. A configurable backend timer was added with an initial setting of 5 seconds. If the user refreshes the page before the timer expires, the system pulls the available data instead of fully recalculating the summary. Upon each refresh, the alert summary charts are updated to provide more timely and accurate information.
- **Lithuania phone number format update**: BlackBerry AtHoc now supports the change in Lithuania's domestic dialing code from 8 to 0. BlackBerry AtHoc correctly displays Lithuanian phone numbers with a 0 prefix when the +370 country code is selected. This change was applied across BlackBerry AtHoc, including in the User Manager, Self Service, user import, and API.
- **Logout message**: When logging out from the management system, a logout page with a message that the user has successfully logged out is displayed. Previously, after logging out, users were presented with a Log In page.
- **Operator Export**: Three columns were added to Operator Export: First Name, Last Name, and Display Name.
- **Organization Hierarchy attribute**: Organization Hierarchy attribute names can no longer contain a comma (,) character.
- **Operator import**: Operator import does not support these fields: Firstname, Lastname, Displayname, Password Changed Date, and Last Login Date. If the import file contains these columns, they are ignored and the import proceeds without error. These columns may appear in your import file if you exported operator information and then modified the export file for import.
- **Remove Accountability Officer and SDK User roles from Security Settings**: The Accountability Officer and SDK User roles were removed from the Operator Roles pull-down list in the Revoke Operator Permission section on the Security Settings page to ensure that they are never inadvertently revoked through the security setting that revokes operator roles due to inactivity. The Accountability Officer and SDK User roles should never be automatically revoked.

  Accountability Officers generally log in only when they are targeted to respond on behalf of other users during an accountability event. If the Accountability Officer role is revoked, the Accountability Officer cannot log in to respond on behalf of other users in the organization.

  The SDK User role is used for features such as the API and User Sync. If the SDK User role is revoked, APIs and features such as User Sync will stop working.
- **Restrict user import from accepting passwords**: BlackBerry AtHoc has removed the ability to import passwords in the user import flow to improve performance. This change was made due to recent security policy updates that require more intensive password hashing, which was slowing down user imports. The following changes have been made:

  - The user import flow will not allow selection of a "Password" column for import. A message is displayed indicating that the user does not have permissions to import the Password column.
  - The API endpoints for the POST /orgs/{orgCode}/users/SyncByCommonNames API returns a 400 response code if a Password field is included in the payload with a message instructing the user to update the payload and try again.
  - The User Sync Client blocks the import of Password fields and returns an error message.
- **Self Service Last Sign-On**: The Self Service Last Sign-On user attribute now captures the date and time when a user signs in to Self Service from a URL or from the desktop app, and when they access their user profile on the mobile app.

- **Stop calling options improvement**: When an operator creates an alert with no responses and selects Phone as a delivery device, the Stop Calling options now correctly override the Call Attempts and Retry Interval settings. If the Stop Calling options are met, such as delivering the alert as a voicemail, additional call attempts are not made. The Bilingual feature no longer impacts the Stop Calling functionality.
- **Super Enterprise updates**: When mapping enterprise organizations to a super enterprise organization, if there are inherited entities, a Duplicate Entities Found dialog appears informing the operator about the duplicates. The operator has the option to continue mapping with the duplicates or to export the list of duplicate entities to a CSV file. Inherited entities that must have unique names include attributes, placeholders, alert templates, accountability templates, folders, delivery templates, and audio files.

  When entities with duplicate names are inherited from the super enterprise to its mapped enterprise organizations, on hover-over, a tool tip appears that indicates that the entity was inherited and from which organization the entity was inherited. These tooltips appear in these areas:

  - The Folder drop-down menu on the New Alert, Sent Alerts, and Alert Templates pages
  - The Folder drop-down menu when creating a new alert template or a new blank alert
  - The Placeholder drop-down menu when creating a new alert or accountability template, or a new blank alert
  - The Delivery Template selection in the personal device options on alert preview pages
  - The Audio File selection when selecting personal device options for an alert or accountability event
  - All drop-down menus when selecting or filtering user attributes

  For more information, see "Inherited content and settings in the enterprise or super enterprise" in the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide.
- **Target users By Location**: The "By location" tab was removed from the Target Users section in alert templates. Now, operators can target users by location by selecting the location on a map in the Content > Location section. All users that have a geolocation attribute in the selected location with a Last Known Location attribute that was updated within the last 4 hours are automatically targeted. The Last Known Location interval for targeting can be configured in the Target Users section on the By Advanced Query tab.
- **Unique alert placeholder names**: Alert placeholders are inheritable in super enterprise and enterprise organizations. Due to this inheritance, all alert placeholder names must be unique across all organizations within an enterprise or super enterprise. New alert placeholder names must be unique. An error message is displayed if a duplicate name is entered when creating a new alert placeholder.
- **User profile fields update**: The "Do not Auto Disable" attribute was updated to the "Do not Disable." The "Do not Auto Delete" attribute was updated to "Do not Delete." These attributes prevent users from being manually disabled or deleted.
- **User Search API**: In the User Search API, the “nco” (DoesNotContain) operator for Path type attributes (such as Organization Hierarchy) is no longer supported and returns an error message. For more information, see "AtHoc Query Language attribute types" in the *BlackBerry AtHoc API Quick Start* guide.

Breaking changes

Breaking changes are changes that will cause existing integrations and functionality to break unless you take remedial action.

- **APIs return Date/Time in UTC**: The following API endpoints were updated to return Date and Time fields in Coordinated Universal Time (UTC) to ensure a uniform time representation across all BlackBerry AtHoc API responses:
  - Accountability APIs
  - Attribute and Device APIs
  - Audit APIs
  - Publishing APIs
  - Reporting APIs
  - Self Service APIs
- **Benin phone number format update**: BlackBerry AtHoc now supports the change in Benin's phone number format from 8 to 10 numbers. Existing international phone number libraries were updated to support the new 01 phone prefix. The phone country code selector in the User Manager continues to show +229 beside the Benin flag.
- **EventLog API support**: The EventLog/Post API is no longer supported.
- **Integrated Weather Alerts**: In weather alert rules, the weather and message types were redesigned to map to the same or similar fields received from NWS weather feeds. After upgrading to BlackBerry AtHoc release 7.21, existing weather alert rules with weather or message types that are no longer supported are disabled and must be reconfigured to match the appropriate weather and message types. For more information, see "Create a weather alert rule" and "Weather alert types" in the *BlackBerry AtHoc Integrated Weather Alerts* guide.
- **Removed Map APIs**: The following Map APIs were removed:
  - /api/v2/MapService/{orgCode}/GetLiveIncomingAlerts
  - /api/v2/MapService/{orgCode}/GetOrganizations
  - /api/v2/MapService/{orgCode}/GetDistributionListUsers
  - /api/v2/MapService/{orgCode}/GetMapSettings
  - /api/v2/MapService/{orgCode}/GetShapeLayerDataById
  - /api/v2/MapService/{orgCode}/GetUserCountByGeo

Resolved issues

The following issues were resolved in BlackBerry AtHoc release 7.21.

Jira ID	Description
IWS-51450	After a mobile user is disabled or deleted, they are still able to send messages and attachments in collaborations.
IWS-55305	When filtering by time in the diagnostic log, the time specified must be in Pacific time, not the time zone specified in the organization.
IWS-56565	The tooltips displayed for the "Export Delivery Summary (CSV)," "Send Alert to These Users" and "User List" response detail options in an alert summary are incorrect.
IWS-60340	For any API call made to retrieve alert details, the alert TYPE field returns the COMMON_NAME value instead of the actual name of that TYPE.
IWS-62013	In an accountability template, entering invalid entries in the Recurrence Pattern field does not display a relevant error.
IWS-62197	The ReachableUsers parameter count was incorrect in the Alert Users Targeted API.
IWS-62371	When an initial attempt to send an SMS alert fails, but then is successful upon retry, the user tracking report continues to display an error message.
IWS-62434	The Custom Field section for alert placeholders is not visible after duplicating a draft alert when logged in as an Advanced Alert Manager.
IWS-62529	On the Sent Alerts page, response options are not visible on the tool tip for draft and scheduled alerts.
IWS-62791	Entries are not being captured in the operator audit trail for events that are marked as reviewed or unreviewed.
IWS-63015	Selected devices on the External Events settings page cannot be deselected.
IWS-63252	When exporting the activity log, the export CSV file has incorrect dates when the DD-MM-YY or DD/MM/YY date formats are used.
IWS-63364	Connect alerts reach the Inbox of the destination organization, but they are not processed by alert rules, even though the alert rules satisfy the conditions to process the alert.
IWS-63459	When an alert template is configured to hide the Target Users section, it is still visible to alert publisher operators.

Jira ID	Description
IWS-63512	In an accountability template, if the Affected Users tab section is set to read-only mode, the template does not load and an error is displayed.
IWS-63534	When an Indoor Fire Panel device is duplicated and an alert is created to send to that duplicated device, the duplicated device can not download any pre-tones or post-tones to be broadcast over the IIM device that is running as the duplicated device. The XML that is delivered by the organization to the duplicated Indoor Fire Panel device does not include the pre-tones and post-tones information in the XML file.
IWS-63686	When publishing an alert, custom text is not displayed for the Text Messaging and Email - Work personal device.
IWS-63818	When selecting More Actions > Edit for a live alert from the Sent Alerts screen, the date picker does not display correctly and the user count displays 0.
IWS-63862	The User Tracking Report with Devices does not display records beyond the first page.
IWS-63874	If an imported alert template contains a More Info link without http:// in the URL, clicking the Test URL button results in a 404 error.
IWS-64334	User export does not work when the Subscribed Organizations attribute is included in the export.
IWS-64335	User export fails after finding a user by using an advanced search for a geo-aware attribute.
IWS-64402	A Personnel Report with Summary does not work for operators using SSO login.
IWS-64413	Saving a Geo-aware Single-select Picklist attribute with a large number of values fails intermittently.
IWS-64562	Using the ✎ Edit & Format button to edit an alert on the Review and Publish page causes white spaces and lines to be removed from the body text, changes the content format, and makes the alert look compact.
IWS-64700	When an alert is resent from the Sent Alerts screen using results-based targeting and it is targeted to a connected organization, the connected organizations from the original alert are not displayed and changes cannot be made to mass devices. The alert is sent to the targeted connected organization.
IWS-64736	A new user is created when a user attempts to log in with a disabled user email.

Jira ID	Description
IWS-64776	The desktop app transmits session variables required to perform authentication to the Enterprise Administrator account via plaintext.
IWS-64786	Device fields set in the management system as mandatory are not mandatory on the mobile app in the Devices section.
IWS-64834	When importing values in a geo-aware type attribute, the Save button is grayed out.
IWS-65025	The timestamp of the next occurrence for a scheduled alert is off by one hour when an organization's time zone is changed from one that observes daylight savings time to another time zone that does not.
IWS-65090	If the total number of characters in the values of a user attribute is more than 4000 and this attribute is used in a user's profile, the profile cannot be saved after being edited.
IWS-65122	If you create and save an alert template with a map, and then create and save a second alert template with a map, when you open the first saved template, the map from the second saved template is displayed.
IWS-65225	Incoming Connect alerts or events with attachments take up to 90 seconds to process.
IWS-65264	When an alert is sent from an enterprise organization that is part of a super enterprise organization, the Type field is blank on the Sent Alerts page of the super enterprise.
IWS-65279	When a scheduled accountability event that uses the "Last day of the week" recurrence interval is reviewed, the recurrence interval changes to "First Sunday."
IWS-65365	If there are more than 18 records on the Geocoding Summary and Logs settings page, scrolling is not available and not all records can be viewed.
IWS-65439	The Organizational Hierarchy and Preferred Language user attributes are not translated to the selected locale on the My Profile page in Self Service.
IWS-65502	Alert publishing through the API does not support bilingual alerts.
IWS-65565	The sequence of keyboard tab navigation in the Inbox is incorrect.
IWS-65566	A scheduled accountability event that is configured with the "Last [day of the week]" recurrence interval reverts to the "First Sunday" interval when the accountability event is reviewed.
IWS-65568	An alert template uses the default delivery template when an accent character is used in the title.

Jira ID	Description
IWS-65622	When an alert is sent from the "Resend an alert to these Recipients" link with the "Not Responded" option selected in a User Tracking Report, all of the original targeted users are targeted.
IWS-65653	On the Live Map, sometimes the default map location displays an incorrect location.
IWS-65685	When importing users with geo addresses, the batch geocoding postprocessor system job fails and the import remains in an "In Progress" state.
IWS-65736	After modifying the recurrence schedule of an alert template, if an alert was already published from that template, the recurrence does not happen.
IWS-65737	The BlackBerry AtHoc logo is broken on the System Generic Template delivery template when viewed on the Preview and Save page.
IWS-65748	If a duplicate alert is created and a placeholder is added to or removed from the Title or Body, the Email preview section on the Preview and Save page displays the details of the original template.
IWS-65778	Tool tips added when creating a single-select picklist, multi-select picklist, or geo-aware single-select picklist user attribute are not displayed on user profile pages in Self Service or the BlackBerry AtHoc management system.
IWS-65857	A delivered email alert does not contain alert placeholder values if the alert template was edited from the Preview and Publish page.
IWS-65866	Response options are not displayed during result-based targeting for an alert from an enterprise organization that was mapped to a super enterprise organization.
IWS-65950	When a dependent user is disabled through a user import, they no longer appear on the dependents display page.
IWS-66076	Disabled weather alert rules attempt to publish alerts with templates that are not ready to be published.
IWS-66109	If there are more than 9 response options, only the first 9 are displayed.
IWS-66161	When performing an advanced search from the Users tab of an accountability event details page, selecting a Geo-aware Single-select Picklist attribute causes the page to crash.
IWS-66463	An operator with Draft Alert Creator permissions is able to publish an alert using the Alerts API.

Jira ID	Description
IWS-66526	If all users are deleted from an alert template, and an alert targeting those users is published from the live map, the operator is not redirected to the alert edit page and error messages are displayed.
IWS-66879	When an operator clicks the Edit & Format button on the Email Preview window, the UI (color, font, and font size) of the alert's title and body changes to black color with a small font. When the operator clicks the Edit & Format button and chooses the alignment of the alert to right/ middle and then clicks on Apply, the title does not move to the right/ middle in the preview window. However, after the alert is published, the operator can see the alignment as right/middle, as selected.
IWS-66939	Performance issues occur with large shape files on the publisher map caused by unneeded multi-polygon points.
IWS-66963	An error is displayed when the SSO Self Service URL is clicked.
IWS-66989	Geo imports fail when an address containing a line feed/carriage return is included in the import. The following error message is displayed: "the remote server returned an error: (400) Bad Request."
IWS-67049	The DetailsByUsersDevices alert tracking API displays an unhandled exception for datetime.
IWS-67083	When targeted users have different preferred languages, bilingual alerts sent to the desktop app do not honor the users' preferred languages.
IWS-67199	On a user profile page, the More Actions > View Activities page can take more than 2 minutes to load.
IWS-67419	Changes made on the desktop pop-up delivery template are not honored on the Preview and Save page.
IWS-67571	When viewing a Distribution List Report from the Advanced Reports on an alert summary page, clicking the link in the Sent or Targeted column displays a pop-up that shows the number of recipients. Clicking the "Show Recipient List " link on the pop-up opens a User Tracking Report. When the "Show User & Device Level Report" link on the User Tracking Report is clicked, an error is displayed.
IWS-67591	The Preview button for an email delivery template configured with a Japanese locale starts loading but does not complete.
IWS-67713	When creating a draft alert using placeholders with similar value names, the draft alert now correctly selects only the intended placeholder value on save.
IWS-67886	The Self Service profile page does not display some picklist fields for some users when editing their profile. This issue occurs intermittently in Chrome and Edge browsers.

Jira ID	Description
IWS-68476	BlackBerry AtHoc API updates to address several gaps identified in the SDK, including: • Ability to retrieve EventLogs by ID, User Summary Report, Alert Activity Summary Report, User Device Coverage Summary, User Attribute Coverage Summary, and User Attribute Coverage Summary by Organization Hierarchy. • Improved error handling for incorrect GET or POST payloads. • Verification of the above scenarios across all levels (super enterprise, enterprise, and suborganization) and non-English locales (German and French.)
IWS-68679	Alert templates do not honor the targeting settings for devices when publishing alerts. The alert screen displays devices that were unchecked in the template's target setting.
IWS-68734	The label in alert templates to enable mobile publishing for a German organization is "Für die Veröffentlichung verfügbar" which translates into "Available for publishing," and is missing the word "mobile."
IWS-68885	Organization names containing an ampersand (&) are not handled properly in Usage Summary and Alert Usage reports.
IWS-68944	Subscribed organizations appear in user profiles, but not in the user list. Deleting an existing subscribed organization removes it, but it then reappears in the user's profile when a new subscribed organization is added.
IWS-68946	Users are unable to delete mobile devices after importing a CSV file with an invalid value for the "Mobile App" device.
IWS-68983	When searching for a value inside a Dynamic Hierarchy attribute, the search result list is reset after every selection.
IWS-69075	The wrong country flag is displayed on the Registration page on the mobile browser. The indexing and association of flags to countries in the mobile browser country selector drop-down was fixed.
IWS-69168	For large alerts, the "User Tracking Report - with Devices" report crashes and displays an error in the diagnostic log.
IWS-69169	After clicking More Actions > View Activities from a user profile page, activities are displayed out of order.
IWS-69174	When updating an operator's permissions using a CSV upload from an enterprise organization, the import fails and an error message that the Organization field is invalid is displayed.

Jira ID	Description
IWS-69497	Customers can now create and use custom locale email templates for alerts. When an alert is published, the custom email template matching the selected locale and severity is used to deliver the alert, ensuring the content is fully localized for the recipient.
IWS-69544	When performing an advanced search from the Inbox with the alert type (CheckIn/CheckOut) and datetime range as filter criteria, the search takes a long time to complete, especially for organizations with a large number of rows in the Inbox.
IWS-69580	Multiple operators are deleted when the DELETE button is pressed even though only one operator is selected to be deleted.
IWS-69618	An issue where the default map view occasionally displayed a location in China, even when the default location was set to another location has been fixed. An intermittent loader was added to ensure that the default organization location is properly loaded and displayed.
IWS-69918, IWS-69919	Only the first condition of a dynamic distribution list with an OR condition is respected in the Advanced User Search API, resulting in incorrect users being delivered to the geofence service.
IWS-70011	If all users are selected on the user manager page and then several users are deselected, clicking on the "Edit User" icon for a user causes the page to load continuously.

Known issues

This section lists known issues in BlackBerry AtHoc releases.

7.21

Jira ID	Description	Workaround
	Mobile App publishing	
IWS-72872	Users cannot publish alerts that contain a pin location from the BlackBerry AtHoc mobile app even when the alert template is properly configured and marked for mobile publishing. The publish fails with the following error message: "Failed to publish alert." This issue occurs on both Android and iOS devices.	—

7.14

Jira ID	Description	Workaround
	Alerting	
IWS-58156	Alerts triggered from the mobile app do not display the icons on the map that are defined in the mobile event rules.	—
IWS-61074	Tabbing does not navigate correctly in alerts sent to the desktop app using the default template.	—
	External event alert	
IWS-58065	Alerts are not triggered for external events when placeholders are added to the alert title in the out-of-the-box External Feeds Template. The External Feeds Template contains a [BFSTitle] placeholder by default. Adding additional placeholders to the title field can cause the title to have more than the maximum number of characters.	Do not add additional placeholders to the title field.
	IPAWS	
IWS-58653	IPAWS COG to COG alerting does not function.	—
	Reporting	
IWS-62851	The Alerts Usage report should not count silent ping alerts.	—

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.

Legal notice

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