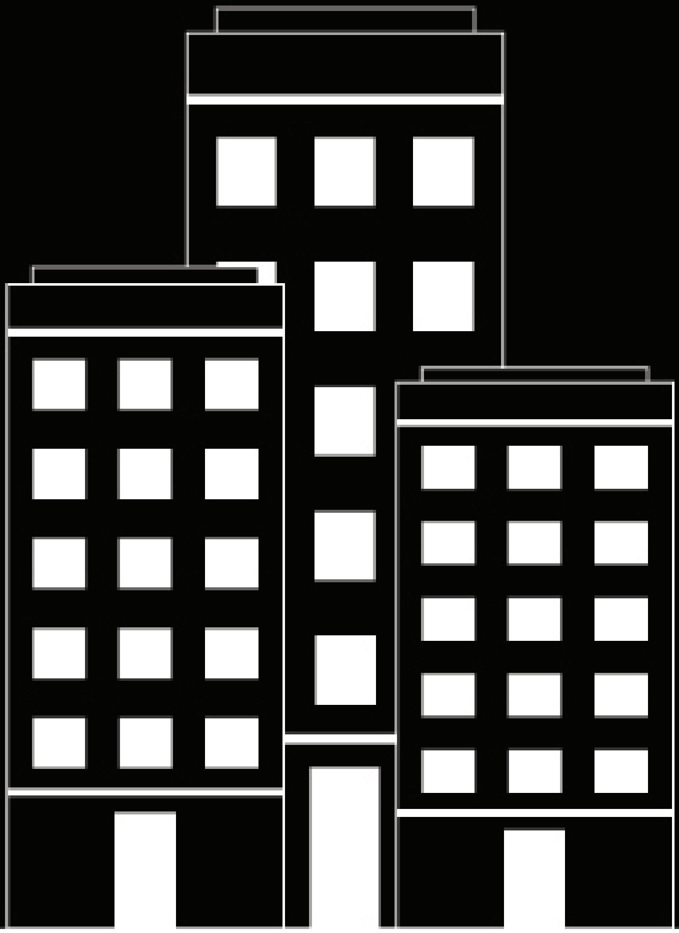

BlackBerry AtHoc

Release Notes

7.20

Contents

What's new in BlackBerry AtHoc 7.20.......... 4

Behavior changes..........10

Breaking changes..........12

Resolved issues.......... 13

Known issues..........15

BlackBerry AtHoc Customer Support Portal.......... 17

Legal notice.......... 18

What's new in BlackBerry AtHoc 7.20

These release notes contain information about new and changed functionality for BlackBerry® AtHoc® release 7.20. 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.

AtHoc Geofencing App

AtHoc Geofencing is a standalone application that enables operators to accurately and easily track the location of users in the field. Using AtHoc Geofencing, operators can easily identify where a user currently is, where they've been, and how long they've been there. AtHoc Geofencing provides automated entry and exit tracking, giving the operator greater situational awareness of their users. For details see: https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc/geofencing/1_0

Management system

- **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 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.
- **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.
- **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.
- **Operator Audit Trail**: Data in the Operator Audit Trail is now retained for 12 months. Previously, it was retained for 6 months.
- **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.
- **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.
- **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.
- **Self Service logout in the Operator Audit Trail**: User log outs from Self Service are now captured in the Operator Audit Trail. Previously, only log in attempts from Self Service were captured in the Operator Audit Trail.
- **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.
- **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.
- **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.
- **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.
- **Operator Audit Trail for User Move actions**: 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.

Alerting

- **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.
- **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.
- **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.

AtHoc Account

- **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 is targetable 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.
- **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 account 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.
- **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.
- **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.

  Users granted the External Operator role of Accountability Officer 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 assigned and from the organizations above (enterprise and super enterprise organizations.)

  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.

AtHoc Connect

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.

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
- Custom attribute translation accessed from the Users menu
- User attribute manager accessed from the Usersmenu
- New distribution list and edit a distribution list pages
- Feature Enablement settings page

Browser support

BlackBerry AtHoc release 7.20supports the latest versions of the following browsers: Edge, Safari (Mac), Chrome, and Firefox.

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.

Mobile app

BlackBerry AtHoc 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 are automatically 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.

Desktop App 7.7 (Windows), 2.6 (Mac)

Desktop 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 the desktop app. 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.

Integrations

- **IPAWS Event Types are now configurable per organization**: BlackBerry AtHoc now allows administrators to configure the IPAWS event types that are available for each organization's IPAWS devices. This provides more flexibility and control over the event types presented to operators. Administrators can add, delete, and edit the available event codes for each IPAWS device. The current set of event codes has been migrated to all enabled IPAWS devices, and duplicating a device will also copy the associated event codes. Scrolling is available if there are more than six event codes configured.
- **UEM Notifications**: Support for UEM release 12.19 and 12.20 was added.
- **ServiceNow updates**:

  - Users can select templates from BlackBerry AtHoc that have the "Available for Quick Publish" option configured. Select the "Enable Alert Templates" option on the ServiceNow settings page to enable this feature.
  - Distribution lists from BlackBerry AtHoc can be selected in ServiceNow for targeting alerts. Select the "Enable Distribution Lists" option on the ServiceNow setting page to enable this feature.
  - A BlackBerry AtHoc logo button was added to enable sending an AtHoc alert from a ServiceNow Incident.
- **New ATI and American Signal Outdoor Warning Sirens devices**: Two new mass notification devices have been added for ATI and American Signal outdoor warning sirens. These devices only support the 'Key' option, without any pre-tone, post-tone, pre-recorded audio, text-to-speech, or play alert content options. The new devices are named:

  - ATI Outdoor Warning Sirens
  - ASC Outdoor Warning Sirens

  The installation, configuration, gateway, addressing, and endpoints for these new devices are the same as for the existing ATI and American Signal devices.

IIM

- **ATI – 6.1.0.151**

  - The ability to activate groups of sirens that are not pre-defined in the ATI REACT CCU was added. A way to set the timing for both repeater and non repeater-based activations was added.
  - The Siren Grouping feature, including siren activation, was added.
  - Support for group dictionary, including dynamic determination of siren groups based on configurations, was added.
  - A sorting mechanism for siren activation, prioritizing groups with lower numbers followed by individual sirens, was added.
  - Logic for sirens was optimized. Dynamic removal of siren and group duplications was introduced.
  - Logging was improved.
  - The Text-To-Speech (TTS) engine was upgraded to the latest version.
- **American Signal – 6.1.0.121**

  - Support for redundant failover and geosiren targeting was added.
  - An activation of sirens whose sound coverage area intersects with the area of the alert was provided.
  - American Signal was deployed with 2 IIMs that work in tandem so that if the primary IIM fails to activate the sirens or is down, the secondary IIM takes over and performs the activation.
- **Federal Signal – 6.1.0.100**: An issue where the CapConService builder did not create the CapCon service was fixed.
- **INFPe – 6.1.0.247**:

  - INFPe now enables the attachment of multiple USB-based relay cards to a single IIM, increasing the number of fire panel inputs that can be controlled. This eliminates the need for multiple IIMs, even in scenarios where fire panels require more than 16 inputs.
  - Expanded the number of inputs from 16 to 128 inputs.
  - Reduced costs associated with the need to configure and maintain multiple IIMs.
  - Improved ability to maintain audio synchronization across all inputs and connected relay cards.

Behavior changes

Behavior changes are changes in existing functionality that you need to be aware of when upgrading to BlackBerry AtHoc release 7.20. These changes require that you re-learn existing functionality.

- **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 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 👤✓.
- **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.
- **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 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.
- **Enhanced IIM mass device capabilities**: The following mass devices were enhanced with the ability to configure pre-recorded audio, pre-tones, post-tones, and text-to-speech:
  - Federal Signal
  - ATI
  - SiRcom
  - Whelen V2
  - American Signal V2
  - Monaco
  - Motorola ACE3600
- **Fill count in geofence targeting**: Geofence alerts can now use fill counts. Previously, when geofence targeting was enabled, fill count was disabled.
- **Remove Accountability Officer and SDK User roles from Security Settings**: In BlackBerry AtHoc, in Settings > System Setup > Security Policy, the Revoke Operator Permission Section was updated to remove the Accountability Officer and SDK User roles from the selection list. 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 in 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. To avoid these issues, 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. This ensures that these critical roles are never inadvertently revoked through the security setting that revokes operator roles due to inactivity.

- **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 also blocks the import of Password fields and returns an error message.

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
- Attributes and Devices APIs
- Audit APIs
- Publishing APIs
- Reporting APIs
- SelfService APIs

Resolved issues

The following issues were resolved in BlackBerry AtHoc release 7.20.

Jira ID	Description
IWS-65737	The BlackBerry AtHoc logo is broken on the System Generic Template delivery template when viewed on the Preview and Save page.
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-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.
IWS-68476	BlackBerry AtHocAPI 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.

Jira ID	Description
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 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.
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.

Known issues

This section lists known issues in BlackBerry AtHoc releases.

7.16

Jira ID	Description	Workaround
	Alerting	
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.	—

7.15

Jira ID	Description	Workaround
	Users	
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.	—

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.	—

Jira ID	Description	Workaround
IWS-61074	Tabbing does not navigate correctly in alerts sent to the desktop app using the default template.	—
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.	—
	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