



BlackBerry AtHoc

Release Notes

7.15 (OnPrem)

Contents

- What's new in BlackBerry AtHoc 7.15 (OnPrem)..... 4**
 - Live map.....4
 - External event management.....5
 - Integrations..... 6
 - Management system.....6
 - API.....14
 - Attributes..... 17
 - Authentication and validation.....19
 - Account..... 19
 - Mobile device management..... 19
 - Situation Response..... 19
 - Self Service..... 20
 - SMS opt-in.....21
 - User sync client.....21
 - Cloud and delivery services.....21
 - Mobile app..... 21
 - Desktop app.....24
 - IIM..... 27
 - Security.....27
 - SDK specification..... 27

- Behavior changes.....28**

- Breaking changes.....31**

- Breaking changes (7.15 FE-11)..... 32**

- Resolved issues..... 33**

- Known issues..... 40**

- BlackBerry AtHoc Customer Support Portal..... 42**




- Legal notice..... 43**

What's new in BlackBerry AtHoc 7.15 (OnPrem)

These release notes contain information about new and changed functionality for BlackBerry AtHoc Release 7.15 (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>.

Live map

The following improvements were made to the live map:

- **Access to BlackBerry AtHoc settings:** You can click the Settings icon () to go directly to the Map Settings in the BlackBerry AtHoc management system.
- **Basemap layers improvements:** The Basemap Layers list is now organized so that the most commonly-used map types appear at the top of the list. All Basemap Layer components are localized.
- **Dynamic map zoom:** When an operator is following a specific user or user group (distribution list), when the live map automatically refreshes, the map keeps focus on the followed user or group.
- **External layers:** Public layers can be viewed on the External Layers panel on the live map. Administrators can add up to 30 external layers in the Map Settings. Once added, data from external layers update automatically on the live map. Feature, Image, and KML layer types are supported. The transparency of external layers on the live map can be adjusted. For Feature and Image type layers, a legend can be displayed if one is present in the layer source. The following external feeds are available out of the box:
 - Floods – NDFD Rainfall Total Forecast
 - Floods – Live Stream Gauges
 - Floods – USA Flood Hazard Area
 - Hurricanes – Forecast Position
 - Hurricanes – Observed Position
 - Hurricanes – Forecast Track
 - Hurricanes – Observed Track
 - Hurricanes – Forecast Error Cone
 - Hurricanes – Watches and Warnings
 - Hurricanes – Hurricane Force
- **Improved zoom level:** When an operator clicks on a panel to display multiple alerts or events, the map does not zoom out past where the map labels can be viewed clearly.
- **Layer layout and functionality:** Items in the BlackBerry AtHoc, Predefined Zones, and Distribution List layers can be selected individually or by parent folder. Select a folder to display the items on the map. You can select individual folders or parent folders. Click a specific item in a folder to zoom the map to view that item.
- **Live map access:** The new live map can be accessed from the Recently Received Alerts section or from the "View Live Map" button on the home page, from the Sent Alerts screen, or from the Accountability Events page.
- **Mobile emergency:** Message updates sent for mobile emergencies are displayed on the live map in the emergency details pop-up.
- **Performance improvements:** Various performance improvements to live map flows were made, including caching Esri basemap layers in memory to improve the live map load time.
- **Redesigned user-interface:** Content on the live map was organized into the following panels:
 - Basemap Layers (): Select the type of map to display.
 - BlackBerry AtHoc Layers (): Display accountability events from enterprise and suborganizations, live sent alerts, live incoming alerts, and connected organizations. Live incoming alerts include Connect alerts and emergencies, check-ins, check-outs, and reports from the mobile app.

- **Predefined Zones** (📍): Display predefined zones. Predefined zones are also known as imported shape layers. Select the check box beside an imported layer or shape file to display it on the map. Click the name of a displayed item in the panel to zoom the map to its location.
- **Distribution Lists Layers** (👤): Display users from distribution lists. Click a selected distribution list to zoom the map out to display all users in the distribution list.
- **Send a quick alert:** Operators with alert publishing permissions can draw a shape on the live map or select a predefined shape, target users in the shape, and send the targeted users a quick alert. When a shape is drawn or selected on the live map, the User Action panel opens to the Users tab. On the Users tab, select organization and attribute filters and select targeted and blocked users to refine the list of targeted users found in the shape. User information can be exported to a .csv file. Select an alert template and personal devices on the Quick Alert tab of the User Action panel. Alert templates must have the "Available for quick publish" option enabled and have "location" enabled in the alert template settings to be available for selection. On the Quick Alert tab, operators can verify the number of reachable users and publish a quick alert. The sent quick alert appears under the Live Sent Alerts in the BlackBerry AtHoc Layers panel on the live map. Details about the alert can be viewed in the Sent Alerts page in the BlackBerry AtHoc management system.
- **Shape drawing capability:** Operators can use the Draw Shapes panel to draw shapes on the live map and see the number of users in the shape.
- **Subscribe to geographic locations:** The ability for end users to subscribe to geographic locations of interest was added. Administrators can create user attributes that are based on shape layers on the live map. When an administrator creates the user attribute, then configures it to be visible in user profiles, users can subscribe to those locations and then be targeted in quick alerts from the live map based on those subscriptions.
- **Tool tip display search box:** When searching for a location, the tool tip for the search field displays the full address.
- **User details pop-up:** The user details pop-up for individual or clustered users displays devices, attributes, and groups. A Last Known Location timestamp is displayed on the user details pop-up.
- **Zoom to functionality:** The "Zoom to" function was improved so that a single click moves to the street-level view for the following alerts:
 - Live alerts
 - Live accountability events
 - Live incoming alerts (including emergencies, reports, check-ins and check-outs from the mobile app.)

For more information, see "Live map" in the *BlackBerry AtHoc Map User Guide*.



External event management

- BlackBerry AtHoc helps emergency managers stay aware of external events that impact their organization and employees with the BlackBerry Feed Service (BFS.) An organization can specify a geolocation of interest and request to start receiving alert notifications in their alert inbox. BlackBerry AtHoc also provides an out of the box External Feeds Template that an Organization Administrator can configure to receive alert notifications in parallel to the inbox alert. As part of the inbox alert experience, BlackBerry AtHoc provides impacted geolocation view and users count in that location. For more information, see "[View external events in the inbox](#)" in the *BlackBerry AtHoc Manage Incoming Alerts from the Inbox User Guide*.
- System Administrators can now enable the External Events feature in **Settings > Feature Enablement**. When external events are enabled, Organization Administrators can select the locations and types of external events they want to monitor in **Settings > External Events**. External events that impact the selected locations appear in the Organization Administrator's Inbox in the management system. Organization Administrators can select administrators to receive alerts about the external events that appear in the Inbox. These alerts can be received on SMS, email, and the mobile app. Only one alert will be sent for each event type every 24 or 48 hours. For more information, see "[External Events](#)" in the *BlackBerry AtHoc System Administrator Configuration Guide*.

Integrations

- **CUCM 12.5:** Support was added for on-prem TAS installations.
- **IIM V2:**
 - IPAWS now supports WEA 2.0. With WEA 2.0, alert content can be provided in both English and Spanish. Up to 360 characters of text can be included in a WEA 2.0 alert. The FEMA standard text option (CMAM authentication) was removed. WEA 2.0 must be enabled as a device in BlackBerry AtHoc.
 - User experience improvements.

For more information, see the [BlackBerry AtHoc IPAWS Plug-In for NDS Installation and Configuration Guide](#).

- **IPAWS WEA 2.0:** Reporting improvements.
- **Microsoft Teams, BlackBerry AtHoc client app 1.0.41:** The BlackBerry AtHoc integration with Microsoft Teams enables emergency managers and incident response teams to collaborate using BlackBerry AtHoc's critical event communication platform and infrastructure within the Microsoft Teams platform. Install and use the BlackBerry AtHoc app within Microsoft Teams to send alerts from Microsoft Teams chat by using a chat bot and to deliver alerts to targeted users in Microsoft Teams and other devices.
 - **Account credentials requirement:** Microsoft Teams operators must use the same account credentials to sign in to the BlackBerry AtHoc Microsoft Teams app and Microsoft Teams.
 - **Adaptive card text in dark mode:** An issue was fixed where the text in the Publish Alert adaptive card did not display when Microsoft Teams was in dark mode.
 - **Sign In:** Frequent sign in requests for BlackBerry AtHoc Microsoft Teams operators to connect to the BlackBerry AtHoc server were removed.
 - **Icon update:** The BlackBerry AtHoc icon () was replaced with the BlackBerry icon (.

For more information, see [BlackBerry AtHoc Microsoft Teams Integration Administrator Guide](#).

- **RMG Digital Signage:** Improvements and support for Windows 2016 and SQL 2016.
- **ServiceNow:**
 - Support for the ServiceNow Quebec and Rome releases was added.
 - The ability to send ServiceNow alerts to the BlackBerry AtHoc mobile and desktop apps was added.
 - Support for APIv2 was added.
 - The use of the BlackBerry AtHoc SDK was deprecated.
- **UEM Notifications:** UEM Notifications is now compatible with UEM release 12.11 and 12.12.
- **Workday 1.0.3.7:**
 - **Configurable timeout parameters:** The TokenRequestTimeout and WorkerDataRequestTimeout parameters were added to the Workday\WS.config file. The TokenRequestTimeout parameter sets the timeout for the access request token. The WorkerDataRequestTimeout parameter sets the timeout for the worker data request. Previously, the timeout values were 60 seconds. Now, these timeout values can be configured.
 - A utility was created to export user data from Workday and import it to BlackBerry AtHoc.
 - Support for REST API was added.

Management system

Alerting

- **Alert and event response tracking threshold:** The thresholds for response update tracking for alerts and accountability events were updated:
 - First 10 minutes: Every 30 seconds

- Next 50 minutes: Every 60 seconds
- After 1 hour to end of alert: Every 5 minutes

After the alert ends, there is an update within 5 minutes to track any remaining responses not captured in the final update made when the alert was live.

- **Alert folder restrictions:** Alert folders with restrictions can no longer be seen by users in organizations that should not have access to those folders.
- **Apple push notification:** BlackBerry AtHoc supports the Apple push notification. The legacy API is deprecated.
- **ATI Key:** An issue was corrected where if a user with an ATI-configured IIM and giant voice system attempted to publish an alert by using the KEY selection and did not select a target (pole, zone, group of poles, or all poles), no warning was displayed and the alert appeared to be sent. However, because no target was selected, the giant voice controller discarded the alert. Now, BlackBerry AtHoc does not allow an ATI alert to go to the Ready to Publish state until an endpoint target is selected.
- **Attachments:** Support for the following new file types as attachments was added: .html, .kml, and .xml.
- **Bilingual alerts:** Operators can now send an alert in two languages. End users can select their preferred language through Self Service or the mobile app. For more information, see "[Add a bilingual alert](#)" in the *BlackBerry AtHoc Create and Publish Alerts User Guide*. The Bilingual Alerts feature does not support the following types of alerts:
 - API
 - Connect rules
 - Mobile events
 - WAM
 - BlackBerry Feed Service (BFS)
 - IPAWS
- **Character count in SMS device Custom Text:** The character count was updated to 1250 characters in the Custom Text field in the Personal Devices Options for Text Messaging devices.
- **Clear Last Known Location:** A **Clear** button was added to user profiles in Self Service and in the BlackBerry AtHoc management system that deletes the user's last known location.
- **Device delivery preference:** When sending an alert, operators can select a device delivery preference of System defined, Organization defined, or User-preferred. When System defined is selected, the alert is sent to all targeted devices simultaneously. When Organization defined is selected, the operator-defined device sequence and interval are used. Selecting the Organization defined device delivery preference prevents end users from simultaneously receiving the same alert on multiple devices. When the device delivery preference is user-preferred, the user-defined sequence, configured in either the BlackBerry AtHoc management system or in Self Service, is applied. End users targeted in the alert receive the alert on their enabled devices in the specified sequence. Once a user responds to the alert on one device, they do not receive the alert on any additional enabled devices. For more information about configuring the Organization defined device delivery preference and interval, see "[Set device delivery priority](#)" in the *BlackBerry AtHoc System Administration Configuration Guide*. For more information about selecting the device delivery preference when sending an alert, see "[Select the device delivery preference](#)" in the *BlackBerry AtHoc Create and Publish Alerts User Guide*.
- **Delivery locales:** The following delivery locales were added or modified: Korean, Russian, Chinese, Swedish, Greek, Polish, Portuguese, Dutch, and Turkish. For more information, see "[Supported delivery locales](#)" in the *BlackBerry AtHoc Localization Guide*.
- **Export alerts from the Inbox:** BlackBerry AtHoc operators and administrators can export alerts and events from their Inbox to a .csv file. When exporting an alert from the Inbox to a .csv file, the alert description is included in a "Message" column. For more information, see "[Export alerts from the Inbox](#)" in the *BlackBerry AtHoc Manage Alerts from the Inbox User Guide*.
- **Export check-in and check-out details from the Inbox:** Operators can export check-in and check-out events from the Inbox to a .csv file. A new "Export to CSV" button was added to the Search field. For more information, see "[Export alerts from the Inbox](#)" in the *BlackBerry AtHoc Manage Incoming Alerts from the Inbox User Guide*.

- **Geofence targeting:** Geofence targeting enables operators to target users who are part of a defined geo perimeter on the map. When geofence targeting is enabled, BlackBerry AtHoc looks for updates made to users' locations that match the geo perimeter selected in the alert. BlackBerry AtHoc sends an alert to users who are added to the targeted users for the alert. For more information, see "[Publish a geofence alert](#)" in the *BlackBerry AtHoc Create and Publish Alerts* guide.
- **Google phone library:** The Google phone library was updated to version 8.12.38.
- **Increased attachment size:** The maximum size for attachments in events and alerts was increased from 1 to 5 MB.
- **Localized characters:** Localized characters that contain diacritic marks such as à, é, ñ, ü, or å are now displayed correctly in attributes, template content, and system tray menu items.
- **Location services:** If a valid location cannot be determined during a check-in, check-out, emergency, report, or other location service, "Location Not Available" is displayed instead of "lat/long (0,0)."
- **Message termination:** The BlackBerry AtHoc management system performs message termination on telephony devices for users with multiple targeted devices. When a targeted user for an alert has multiple devices in the system, and responds on one device, for example email, the user does not receive duplicate alerts on their targeted phone. Message termination is performed only on BlackBerry AtHoc hosted telephony. It is not performed on NDMS telephony. Message termination is enabled by default.
- **Prerecorded audio limit:** The time limit for pre-recorded audio in alerts was increased to 2 minutes.
- **Redundant message stop:** When device delivery preference is enabled, and Operator defined or Organization defined device delivery preference is selected, BlackBerry AtHoc performs redundant message stop. Redundant message stop prevents users from receiving alerts on lower-priority devices after they have responded to the alert from a higher priority device. For more information, See "[Redundant message stop](#)" in the *BlackBerry AtHoc Create and Publish Alerts User Guide*.
- **Reset button:** A Reset button was added to new alert templates. On enterprise organizations, Enterprise Administrators, Organization Administrators, and System Administrators can use the reset functionality on the alert template to synchronize the Content section template settings to the out of the box default settings. On suborganizations, the reset functionality synchronizes the Content section template settings to the enterprise organization settings.
- **Scheduled location access:** Operators can actively track a group of users for a selected interval. Scheduled location access enables operators to more accurately track where mobile personnel are without relying on end users to perform manual check-ins from the mobile app. For more information, see "[Configure scheduled location access](#)" in the *BlackBerry AtHoc Manage Incoming Alerts from the Inbox User Guide*.
- **Test alerts:** The **Test** button is now available to all operators who have publishing permissions on an organization, including operators who are granted permissions from the External Operator Permissions screen. Previously, operators could only send test alerts on their home organization. For more information, see "[Test an alert](#)" in the *BlackBerry AtHoc Create and Publish Alerts User Guide*.
- **User-preferred device delivery preference:** Support for user-preferred device delivery preference was added. When the device delivery preference is user-preferred, the user defined sequence, configured in either the BlackBerry AtHoc management system or in Self Service, is applied. End users targeted in the alert receive the alert on their enabled devices in the specified sequence. Once a user responds to the alert on one device, they do not receive the alert on any additional enabled devices. For more information see "[Select the device delivery preference](#)" in the *BlackBerry AtHoc Create and Publish Alerts User Guide*.
- **View all sent alerts from an enterprise organization:** Enterprise Administrators can view sent alerts from their suborganizations on the Sent Alerts screen when logged in to the enterprise organization. When an Enterprise Administrator is logged in to the enterprise organization and exports alerts from the Sent Alerts page, sent alerts from their suborganizations are included in the export. A new "Organization" drop-down menu was added to the search options on the Sent Alerts page. Enterprise Administrators and System Administrators can search by organization from the enterprise organization. The default value is "All Organizations." When an Enterprise Administrator publishes an alert from the enterprise organization that was published originally at the suborganization level and that alert includes a fill count, the following error message is displayed: "This feature is disabled because the attribute specified for Fill Count and Escalation from the original organization is not available here."

- **Weather alert rule:** The Message Type "Update" was added to weather alert rule conditions.

Configuration and settings

- **BlackBerry AtHoc provisioning application settings:** Application settings were moved from web.config to a table in the database. This enables BlackBerry AtHoc to be upgraded without the need to update the web.config file.
- **Caller ID Field:** The Caller ID field limit was increased to 15 digits. Access the Caller ID field in Settings > General Settings > Customization > Phone Call Setting.
- **Email format:** The maximum number of allowed characters in the TLD section of an email address was increased from 9 to 15 characters.
- **Device manager:** The user interface for the device manager and device details pages was improved. The device manager page displays separate tabs for personal and mass devices. Devices on the device manager page can now be easily searched for, reordered, and edited. The number of users impacted by enabling or disabling a device is displayed. The process for adding a delivery gateway on device details pages was simplified.
- **Mobile Alert Settings page:** The Mobile Alert Settings page was updated to include a new tab for scheduled location access. For more information, see "[Configure mobile alert settings](#)" in the *BlackBerry AtHoc Manage Incoming Alerts from the Inbox User Guide*.
- **Mobile App gateway:** An option was added to the Mobile App gateway settings page to enable or disable showing the preferred language option in users' My Profile pages. The preferred locale option supports bilingual alerts. For more information, see "[Configure the mobile app gateway settings](#)" in the *BlackBerry AtHoc Mobile App Administrator Guide*.
- **Operator audit trail message:** The entry in the operator audit trail when a mobile user connects was improved. The "Additional Info" column now displays the following message: "Username (*userID*) connected using AtHoc Mobile app."
- **Operator import error message:** The error message that is displayed when double quotation marks ("") are missing in the userbase conditions during an operator import was updated for clarity.
- **Organization code:** The organization code in General Settings is auto-generated from the organization name with spaces replaced with hyphens. This field can be edited. The organization code is used in the URLs used to access Self Service and Single Sign-On. This field is mandatory.
- **Organization Code field:** Only System Administrators can edit the Organization Code field in General Settings. Previously, Enterprise Administrators and Organization Administrators could also edit this field.
- **Organization code replaces organization ID:** The organization ID is no longer used in Self Service and Single Sign-On URLs. The organization code is used instead.
- **Password reset link expiration timeout:** The reset password link provided in email as part of the forgot password flow is valid for 15 minutes by default. This value can now be adjusted by a System Administrator in the database. Previously, the timeout value was always 15 minutes.
- **Phone number validation for Ivory Coast:** Validation for phone numbers for the Ivory Coast were updated to accommodate a change in phone numbers from 8 to 10 digits.
- **Prevent end users from editing System Setup attributes:** Operators can restrict end users from editing the following system setup attributes: Username, First Name, Last Name, Mapping Id, and Display Name. For more information, see "[Prevent users from editing System Setup attributes](#)" in the *BlackBerry AtHoc Manage Users Guide*.
- **URL referrer whitelisting:** System Administrators can now add URLs for external domains or websites to enable users to access the BlackBerry AtHoc management system and Self Service from them. URLs must be in the HTTPS format. Separate URLs by commas, not spaces. The maximum number of characters allowed is 2000. For more information, see "[URL Referrer Whitelisting](#)" in the *BlackBerry AtHoc System Administrator Configuration Guide*.
- **User Details pop-up:** The User Details - Popup View settings screen was improved to enable operators to easily define which attributes, devices, and groups are displayed on the user details pop-up. The User Details -

Popup View can be configured in Settings > General Settings > Layouts. The user details pop-up can be viewed when targeting users in alerts and events, and on the map.

Distribution lists

- **Display:** By default, only enabled users are displayed when selecting members for a distribution list. Previously, all enabled and disabled users were displayed by default. When an operator's access to manage and/or publish distribution lists is restricted, the operator export displays the lists to which the operator has been restricted. If Restricted is selected under Publish or Manage, but no distribution lists are selected as the restricted values, then the value "Restricted" is displayed in the export. Previously, if no lists had been selected, the export displayed a blank field.
- **Export members of distribution lists:** End Users Managers can export the members of static and dynamic distribution lists. For more information, see the [BlackBerry AtHoc Manage Distribution Lists Guide](#).

Organizations

- **Organizational hierarchy import and export:** The ability to create a new organizational hierarchy or export an existing one using an import .csv file was added. For more information, see "[Import an organizational hierarchy](#)" and "[Export an organizational hierarchy](#)" in the [BlackBerry AtHoc Manage Users Guide](#).
- **Organization subscription:**
 - Operators can configure the organization subscriptions for their users in advance.
 - A mandatory Start Date field was added to the Subscribe Organization screen.
 - The number of organizations a user can be subscribed to was increased from 3 to 10.
 - If an operator subscribes a user to an organization and that organization is not enabled for subscription on that user's organization, the subscription is displayed on the user's profile in read-only mode in Self Service.
 - The names of subscribed organizations are now displayed fully in the Organization Subscriptions section in user profiles.

For more information, see "[Manage organization subscriptions](#)" in the [BlackBerry AtHoc Manage Users Guide](#).

Roles and permissions

- **Alert Publisher and Advanced Alert Manager:** The Alert Publisher and Advanced Alert Manager roles were updated to provide the correct permissions. Previously, the Alert Publisher role provided too many permissions, and the Advanced Alert Manager role provided too few. The Advanced Alert Publisher and Alert Manager roles were added. For more information, see the [BlackBerry AtHoc Operator Roles and Permissions Matrix](#).
- **Operator permission revocation:** The ability to select specific roles when automatically revoking operator permissions was added. For more information, see "[Revoke operator permissions](#)" in the [BlackBerry AtHoc System Administrator Configuration Guide](#).
- **Operator permission revocation in operator audit trail:** Operators whose permissions were revoked are displayed in the operator audit trail by username. The operator permissions that were revoked are displayed beside each operator. Previously, only the user ID was displayed.
- **Operator roles and permissions:** Operators cannot update their own roles and permissions. Administrators cannot assign or revoke permissions for a higher-level role than their role. For example, an Organization Administrator can grant Organization Administrator permissions to another operator, but cannot grant Enterprise Administrator permissions. For more information, see "[BlackBerry AtHoc roles](#)" in the [BlackBerry AtHoc Manage Operators and Administrators Guide](#).
- **Permission revocation:** The permission revocation job was improved by accounting for the creation date of the permission. This prevents an operator's permissions from being revoked before they can log in to the system. If the operator does not have a last login date, the revocation job uses the date that the operator's permissions

were granted on to calculate the revocation date. For more information, see "[Revoke operator permissions automatically](#)" in the *BlackBerry AtHoc Manage Operators and Administrators Guide*.

- **Report Manager:** Operators with the Report Manager role can no longer access the operator audit trail.
- **Role definitions in user interface:** A link to the *BlackBerry AtHoc Operator Roles and Permissions Matrix* was added to the Operator Permissions screen.
- **SDK User:** The SDK User role is no longer required for API-based user syncs. Operators instead need to have the required operator roles assigned to them in the BlackBerry AtHoc management system. For more information, see the *BlackBerry AtHoc Roles and Permissions Matrix*.
- **Show roles based on enabled features in the organization:** Roles associated with specific features in BlackBerry AtHoc are visible only when that feature is enabled for an organization when targeting users by role in alerts, creating distribution lists, and granting operator permissions. For more information, see "[BlackBerry AtHoc roles](#)" in the *BlackBerry AtHoc Manage Operators and Administrators Guide*.
- **Updated login error messages:** When an operator whose account has been disabled, deleted, locked, or has revoked permissions attempts to log in to the BlackBerry AtHoc management system, an error message is displayed. These error messages were updated for clarity. The updated error messages are logged in the operator audit trail.
- **Userbase restriction import:** The OR operator is now supported when importing userbase restrictions for an operator.

Search

- **Picklist smart search:** Smart search, where search results are presented as you type characters into a picklist search box, was added for searches in these areas:
 - User manager
 - Disabling or deleting users
 - Setting advanced criteria for alert publishing and targeting
 - Creating distribution lists
 - Setting operator restrictions
 - Selecting attribute values when editing a user profile in Self Service or in the user manager
 - Selecting organizations for user move in Self Service or in the user manager
 - Selecting organizations for organization subscription in Self Service or in the user manager
- **Support for AND and OR operators in advanced queries:** The AND and OR operators are now supported in the following areas that have an advanced query:
 - Alert targeting
 - Event targeting
 - User manager advanced search
 - Accountability events summary
 - Static distribution list advanced search
 - Dynamic distribution list advanced search
 - Automatic deletion and disabling of users by advanced query

Operators and administrators can create advanced queries using either AND or OR operators. For more information, see "[Search engine overview](#)" in the *BlackBerry AtHoc Manage Users Guide*.

- **User search:** The basic search engine was updated to support using quotes (" ") to search for an exact string. For more information, see "[Search engine overview](#)" in the *BlackBerry AtHoc Manage Users Guide*.

Users

- **Address display:** User addresses are displayed as physical addresses instead of latitude/longitude values in user detail pop-ups.
- **Bulk user update:** Concurrent calls for bulk update or creation of users are now handled properly.
- **CSV import:** Leading and trailing spaces in usernames are removed during a CSV user import. If a space is found in the middle of a username, an error is displayed.
- **Forgot password:** When a user clicks the reset password link in an email or SMS message, they must then enter their username on the Create/Reset Password screen.
- **Identify and delete unused mobile devices:** Operators and end users can view their mobile devices in the AtHoc Apps section of their user profile in the BlackBerry AtHoc management system or Self Service. Mobile devices are listed by recognizable names. Previously, mobile devices were identified only by UDID. Users can more easily identify and delete their unused devices. For more information, see "[Delete unused mobile devices from your profile](#)" in the *BlackBerry AtHoc Self Service User Guide*.
- **Operator import and export:** Enterprise Administrators can now import and export operators across all suborganizations from the enterprise organization. Include an Organization column in an operator import .csv file to import operators to different suborganizations across the enterprise organization. For more information, see "[Importing and exporting operators](#)" in the *BlackBerry AtHoc Manage Operators and Administrators Guide*.
- **Purged users:** Details about purged users are now removed from historical reports and from the operator audit trail. Deleted users are purged once a day by default. Purging deleted users ensures that the userbase is kept current and database performance is maximized. Do not disable purging deleted users unless your organization has a data retention requirement. You can change the purge interval. For more information, see "[Purge deleted users](#)" in the *BlackBerry AtHoc Manage Users Guide*.
- **Satellite phone provider support:** BlackBerry AtHoc now supports satellite phone prefixes in user profiles. Satellite providers are listed in the country list with a generic satellite phone icon. The satellite network is identified by its prefix. Satellite phone numbers are supported in all user sync scenarios, including from the user manager, Self Service, .csv import, User Sync Client, and API.
- **SMS support for Forgot Password and Forgot Username flows:** Users can choose to receive either an SMS message or email when resetting a forgotten password or username from Self Service or from the BlackBerry AtHoc management system.
- **User import:** When a user import includes location attributes, a partially processed count is displayed, regardless of whether the "Partial user import" option is enabled.
- **User move reporting:** Reporting was improved for user moves done by operators or users. User move information including the date the user was moved, who moved the user, and what organization the user was moved from are included in the User Activity section of user profiles. User move information is also displayed in the operator audit trail.

Maps

- **Map improvements:** The following improvements were made to the live and publisher maps:
 - The default map displayed in the Recently Received Alerts section on the BlackBerry AtHoc home page can now be configured in Settings > Basic > Map Settings.
 - User information is displayed in a redesigned pop-up window. A user's last known location and distribution list memberships are displayed. Additional user attributes, groups, and devices may also be displayed. The information displayed in the user details pop-up can be configured in Settings > General Settings > Layouts > User Details - Popup View.
 - Incoming mobile alerts are displayed with the relevant icons on the map. Map icons can be configured in Settings > Basic > Map Settings.
 - A user's last known location is displayed as a physical address and includes a timestamp.
 - On the publisher map, the list of targeted users or organizations can be exported to a .pdf or .csv file.

- Proper Report, Check-in, and Emergency icons are now displayed on the mini map on the BlackBerry AtHoc home page and in the Inbox.

Home page

- **Navigation bar changes:** New menu items were added for Plan and Collaborate. Organization information was updated to be more concise.

Single sign-on

- **Alternative authentication method:** When SSO authentication is selected as the authentication method for Self Service, username/password can be selected as an alternative authentication method. For more information, see "[Enable single sign-on for Self Service](#)" in the *BlackBerry AtHoc Single Sign-On Administrator Guide*.
- **Certificates:** Operators can upload Identity Provider (IDP) and Service Provider (SP) certificates from the BlackBerry AtHoc management system. Administrators can choose to use a BlackBerry-signed service provider certificate or upload and maintain their own custom certificate. For more information, see "[Configure Identity Provider settings](#)" and "[Configure Service Provider settings](#)" in the *BlackBerry AtHoc Single Sign-On Administrator Guide*.
- **Logout service:** In the SSO Service Provider settings, the Logout Service URL was renamed to "Custom Logout URL." The new Logout Service URL is read-only and is pre-populated with the URL of the service provider's endpoint that receives SAML log out messages. For more information, see "[Configure Service Provider settings](#)" in the *BlackBerry AtHoc Single Sign-On Administrator Guide*.

IPAWS

- **IPAWS WEA error codes:** Support was added for the following IPAWS WEA error codes:

Common name/delivery state	Status code	Delivery status code	Request type
message-not-disseminated-as-NWEM	5401	DLV-CAP-ERR-5401	MESSAGE ERROR
eventCode-valueName-does-not-contain-SAME-code	5428	DLV-CAP-ERR-5428	MESSAGE ERROR
message-not-disseminated-as-EAS	5501	DLV-CAP-ERR-5501	MESSAGE ERROR
message-not-disseminated-as-CMAS	5601	DLV-CAP-ERR-5601	MESSAGE ERROR
Accepted by IPAWS	5608	MSG-SENT-5608	MESSAGE SENT
system-error-has-occurred-CMAS-dissemination-service	5612	DLV-CAP-ERR-5612	MESSAGE ERROR

Common name/delivery state	Status code	Delivery status code	Request type
message-not-disseminated-as-non-EAS-public	5801	DLV-CAP-ERR-5801	MESSAGE ERROR

- **IPAWS WEA 3.0:** When sending an alert to an IPAWS WEA 3.0 mass device, the number of polygons and circles that can be selected is limited to 10 circles or polygons and 100 total points. One circle equals approximately 70 points.

Audit log

- **Audit log:** The payload type for old SDK calls is captured in the audit log.

Section 508 compliance

- **Home page:** The BlackBerry AtHoc management system home page is now section 508 compliant.
- **Alert publishing flow:** The following section 508 compliance items for operators in the alert publishing flow were made:
 - Keyboard access, focus, mouse-hover, tooltips, and help text
 - Improved color allocation and contrast
 - Detailed descriptions for web links and forms
 - Improved screen reader capability

SSA

- **Shared Situation Awareness:** All feature components related to SSA have been removed.

API

New APIs

- **GET /orgs/{orgCode}/AccountEvents/templates:** Returns the list of accountability templates.
- **GET /orgs/{orgCode}/AccountEvents/templates/{commonName}:** Returns accountability event template details.
- **GET /orgs/{orgCode}/AccountEvents:** Returns a list of published accountability events based on PageNo and PageSize.
- **POST /orgs/{orgCode}/AccountEvents:** Publishes an accountability event using a template.
- **GET /orgs/{orgCode}/AccountEvents/{eventId}/Officers:** Returns the accountability event officer list for the specified event ID.
- **GET /orgs/{orgCode}/attachments/{guid}:** Returns details about an attachment.
- **GET /orgs/{orgCode}/attributes/{commonName}/Values:** Returns all attribute values for the specified common name.
- **GET /orgs/{orgCode}/attributes/{commonName}/Values/{valueCommonName}:** Returns all attribute values for the specified common name.
- **DELETE /orgs/{orgCode}/attributes/{commonName}/values:** Deletes one or multiple values from a List type attribute.

- **POST /orgs/{orgCode}/attributes/{commonName}/values:** Adds new attribute values for an attribute.
- **PUT /orgs/{orgCode}/attributes/{commonName}/values:** Updates existing attribute values for an attribute.
- **PUT /orgs/{orgCode}/attributes/{commonName}/values/{valueCommonName}:** Updates the attribute value.
- **DELETE /orgs/{orgCode}/attributes/{commonName}/Values/{valueCommonName}/Users:** Deletes attribute values for the specified users.
- **PUT /orgs/{orgCode}/attributes/{commonName}/Values/{valueCommonName}/Users:** Adds attribute values for the specified users.
- **GET /orgs/{orgCode}/AuditLog:** Returns a list of operator audit logs based on RowOffset and Limit.
- **GET /orgs/{orgCode}/DeliveryTemplates:** Returns a list of delivery templates based on Offset and Limit.
- **POST /orgs/{orgCode}/DeliveryTemplates/Email/Preview/{DeliveryTemplateCommonName}:** Returns an HTML preview of the email delivery template.
- **POST /orgs/{orgCode}/DeliveryTemplates/Email/Preview:** Returns an HTML preview of the email delivery based on XSLT stylesheet.
- **POST /orgs/{orgCode}/DeliveryTemplates/DesktopPopup/Preview/{DeliveryTemplateCommonName}:** Returns an HTML preview of the desktop pop-up delivery template.
- **POST /orgs/{orgCode}/DeliveryTemplates/DesktopPopup/Preview:** Returns an HTML preview of the desktop pop-up delivery template based on XSLT stylesheet.
- **GET /orgs/{orgCode}/DeliveryTemplates/{DeliveryTemplateCommonName}:** Returns details about a delivery template based on common name.
- **POST /orgs/{orgCode}/EventLogs:** Creates an event log for the specified organization.
- **GET /orgs/{orgCode}/IncomingEvents:** Returns inbound external and user events. Inbound user events include check-ins, check-outs, reports, and emergencies.
- **GET /orgs/{orgCode}/IncomingEvents/{id}:** Returns details about a specific inbound external or user event.
- **GET /orgs/{orgCode}/operators:** Returns the list of operator details, including accessible organizations (enterprise and suborganization) and roles.
- **GET /orgs/{orgCode}/operators/{loginId}:** Returns the operator permissions, roles, and restrictions for the specified login ID.
- **GET /orgs/{orgCode}/users/search/basic:** Returns user details based on search criteria.
- **POST /orgs/{orgCode}/users/search/advanced:** Returns user details based on advanced search criteria.
- **GET /orgs/{orgCode}/users/{loginId}/profile:** Returns basic, distribution list, device, and attribute information for a specified user. Operators must have the correct user roles.
- **POST /orgs/{orgCode}/users/search/alert_users_targeted:** Returns the details of a specified user based on advanced search criteria.
- **POST /orgs/{orgCode}/users/search/alert_device_coverage:** Returns active alert device coverage based on advanced search criteria.
- **PUT /orgs/{orgCode}/alerts/{auld}:** Ends a live alert or updates an alert duration.
- **GET /orgs/{orgCode}/alerts/folders:** Returns all available folders for the specified organization.
- **GET /orgs/{orgCode}/alerts/{auld}/reports/listsummary:** Returns a Distribution List Summary report.
- **GET /orgs/{orgCode}/alerts/{auld}/report/alertresponsedetail:** Returns a Response Details Summary report.
- **GET /orgs/{orgCode}/alerts/{auld}/report/DetailsByUsers:** Returns a Response Details by User report.
- **GET /orgs/{orgCode}/alerts/{auld}/report/DetailsByUsersDevices:** Returns a Response Details by User Devices report.
- **GET /orgs/{orgCode}/Users/Roles:** Returns the user roles for the specified organization.
- **GET /SelfService/{orgCode}/OrgSubscriptions:** Returns the list of organizations that users can subscribe to.
- **GET /SelfService/{orgCode}/Devices:** Returns a list of all enabled devices in the organization.
- **GET /SelfService/{orgCode}/{loginId}/Profile:** Returns profile data for logged-in users.
- **PUT /SelfService/{orgCode}/{loginId}/Profile:** Updates profile data for logged-in users.
- **GET /SelfService/{orgCode}/{loginId}/OrgSubscriptions:** Returns the list of subscribed organizations by the user.

- **GET /SelfService/{orgCode}/Attributes:** Returns all attribute details for the specified common names.
- **POST /SelfService/{orgCode}/{loginId}/OrgSubscriptions/{addOrgCode}:** Adds or updates an organization subscription to your account.
- **DELETE /SelfService/{orgCode}/{loginId}/OrgSubscriptions/{deleteOrgCode}:** Deletes the selected organizations from user's organization subscription list.
- **GET /SelfService/{orgCode}/Lists/Static:** Returns a list of static distribution lists based on PageNo and PageSize.

Modified APIs

- **GET /orgs/{orgCode}/AccountEvents/{eventId}:**
 - Missing fields were added for Event Details.
 - The Reporting Summary was updated.
 - User Messages and Workflow are included in the event details.
- **No status common name:** The common name of the user status "no status" was changed to "SYS:NOSTATUS" for the following APIs:
 - GET /orgs/{orgCode}/AccountEvents/{eventId}
 - GET /orgs/{orgCode}/AccountEvents/{eventId}/StatusSummary
 - GET /orgs/{orgCode}/AccountEvents/{eventId}/EventUsers
 - GET /orgs/{orgCode}/AccountEvents/{eventId}/Users/{loginId}
 - PUT /orgs/{orgCode}/AccountEvents/{eventId}/EventUserStatus
- **GET: /orgs/{orgCode}/attributes and GET: /orgs/{orgCode}/attributes/{commonName}:** The Attributes APIs now contain the UseAsResponseOption and GroupTargeting fields. The UseAsResponseOption field indicates if this attribute can be used as a response option in the Publish Alert API. Valid values are True and False. The GroupTargeting field indicates if this attribute can be used in the Publish Alert API Group Targeting section. Valid values are True and False.
- **GET: /orgs and GET: /orgs/{orgCode}:** The DeliveryLocalesSupported field was added to the response payload. This field displays the list of delivery locales supported by the organization for alerting content. All valid users can use these APIs. Previously, only Organization Administrators, Enterprise Administrators, and Connect Agreement Managers could use them.
- **Distribution Lists:** The Distribution Lists APIs now returns only distribution lists that the user has permissions to manage or publish to by default. The AllowedToManage and AllowedToPublish fields were added to indicate the permissions. The following APIs are affected:
 - GET /orgs/{orgCode}/lists
 - GET /orgs/{orgCode}/lists/static
 - GET /orgs/{orgCode}/lists/dynamic
- **GET /orgs/{orgCode}/users:** Returns a list of users based on offset and limit. The default value is 1. The maximum value is 100.
- **GET /orgs/{orgCode}/attachments/{guid}:** If an alert or accountability event or template contains attachments, the response now contains the GUID for those attachments instead of the complete body as a Base64 string. The GUIDs can be queried using the following Attachments APIs:
 - GET /orgs/{orgCode}/alerttemplates
 - GET /orgs/{orgCode}/AccountEvents/{eventId}
 - GET /orgs/{orgCode}/alerttemplates/{templateCommonName}
- **GET /orgs/{orgCode}/Alerts:** New fields were added which are helpful for pagination and to enable Enterprise Administrators to see sent alerts from the suborganizations in their enterprise organization.
- **POST /orgs/{orgCode}/Alerts:** Support was added to override more template fields and sections such as Attachment, FillCountEscalation, and TargetUsers.

- **GET /orgs/{orgCode}/alerttemplates:** This API's response now includes the `IsAvailableForMobile` field.
- **GET /orgs/{orgCode}/alerttemplates/{templateCommonName}:** This API's response now includes the following fields: `IsAvailableForMobile`, `TargetCriteria`, `TargetDependents`, and `DeviceDeliveryPrefs`.
- **Operator access:** The following APIs were modified so that any operator with a valid access token can access them:
 - GET /orgs/{orgCode}/attributes
 - GET /orgs/{orgCode}/attributes/{commonName}
 - GET /devices
 - GET /devices/{deviceId}
 - GET /orgs/{orgCode}/devices
 - GET /orgs/{orgCode}/massdevices
 - GET /orgs/{orgCode}/lists
 - GET /orgs/{orgCode}/lists/static
 - GET /orgs/{orgCode}/lists/dynamic
 - GET /orgs/{orgCode}/lists/static/NestedLists
 - GET /orgs/{orgCode}/alert/Types
 - GET /orgs/{orgCode}/alert/Severity
- **Authentication flow:** The API authentication flow was updated so that when a user signs in and provides the organization code for an enterprise or suborganization, the authentication succeeds regardless of which organization (enterprise or suborganization) the user's profile exists in.
- **AtHoc Query Language (AQL):**
 - AQL functionality was introduced in the Publish Alert, Get Alert Details, and Get Alert Template Details APIs to support roles, geolocation, and additional datetime flows.
 - AQL functionality was introduced in the User Search APIs to support roles, geolocation, datetime special values, and CSV values in Organizational Hierarchy.

Deprecated APIs

- **POST /orgs/{orgCode}/users/SyncByDisplayNames:** The `SyncByDisplayNames` API is deprecated. Use the `SyncByCommonNames` API instead.

Attributes

- **Attributes as response options:** Operators can configure which user attributes can be used as response options in alerts and events. For more information, see "[Configure a response option as a user attribute](#)" in the *BlackBerry AtHoc Create and Publish Alerts User Guide*.
- **Attribute value import:** BlackBerry AtHoc now checks for dependencies before removing pick-list values when an operator selects to overwrite values in the attribute values import flow.
- **Custom attributes translation:** Users with an Organization Administrator, Enterprise Administrator, Advanced Alert Manager or System Administrator role can provide translations of custom attributes and their values in the following supported locales: Deutsch (Deutschland), English (UK), Español (España), Español (México), Français (Canada), Français (France), Italiano (Italia), and Nederlands (Nederland.) For more information, see "[Translate Custom Attributes](#)" in the *BlackBerry AtHoc Manage Users Guide*.
- **Export and import of user attribute values:** User attribute values can be exported and imported.
- **Last Known Location:** A timestamp was added to the Last Known Location attribute when displayed in the user details pop-up.
- **Last Known Location Updated:** The Last Known Location Updated user attribute is now visible on user profiles, in advanced searches, and is available for user exports and alert targeting. When a user checks in from the

BlackBerry AtHoc mobile app, a timestamp of the check-in is added to the Last Known Location field in their user profile.

- **Last Login Date:** The Last Login Date user attribute is now available in advanced queries and can be included in an operator export. Operators can use the Last Login Date user attribute to identify and send an alert to users who will be impacted by automatic revocation of their permissions due to inactivity.
- **Location attributes in .csv user import:** Location attributes can now be included when importing users with a .csv file. End users' physical locations no longer need to be converted to the latitude,longitude or POINT(longitude,latitude) format before being imported into BlackBerry AtHoc.
- **My Info Updated:** The My Info Updated attributes were added. The My Info Updated attributes are updated automatically when a user updates their profile in Self Service or on the BlackBerry AtHoc mobile app. The My Info Updated attributes are visible on user profiles, in advanced searches, and are available for user exports and in advanced reports. These are read-only attributes. End users cannot update them manually, and they cannot be edited by operators in the management system.
 - The My Info Updated By attribute displays the name of the person who last updated a user profile.
 - The My Info Updated On attribute displays the date and time a user profile was last updated.
 - The My Info Updated Source attribute displays the source of a user profile update. For example, Mobile.
- **Organization Subscription:** The organization subscription Start Date and End Date attributes can be included in CSV imports, User Sync Client, or API bulk user updates. The Start Date and End Date attributes can be imported and exported. Export and bulk update of the Start Date and End Date attributes are available on enterprise organizations and suborganizations. For more information, see "[Subscribe multiple users](#)" in the *BlackBerry AtHoc Manage Users Guide*.
- **Preferred Language:** The Preferred Language user attribute was added. This is an out of the box enterprise attribute with the common name "User-Preferred-Language." It is a single-select attribute that is searchable in advanced searches and can be exported and imported as part of a user import or export. Set the "User Can Update" option on the Preferred Language attribute to enable users to specify their preferred language in Self Service. This attribute cannot be used as a response option.
- **Subscribed Organizations:** The Subscribed Organizations user attribute is now visible in read-only mode on the User Attribute page. This enables operators to view the Common Name of the attribute for use in the User Sync Client and API.
- **User Last Updated:** The User Last Updated attributes were added. These attributes display user profile updates made by users, operators, and other sources. The User Last Updated attributes are visible on user profiles, in advanced searches, and are available for user exports and in advanced reports. These are read-only attributes. End users cannot update them manually, and they cannot be edited by operators in the management system.
 - The User Last Updated By attribute displays the name of the person who most recently updated a user profile.
 - The User Last Updated On time attribute displays the date and time a user profile was last updated.
 - The User Last Updated Source attribute displays the source of a user profile update. For example, Management System.

The User Last Updated attributes capture user profile updates from the following sources:

- A user updates their profile on the mobile app
- A users sends a report, check-in, check-out, or emergency from the mobile app
- A user enables tracking on the mobile app
- A user responds to an alert or event from a targeted device such as email, desktop app, mobile app, or SMS
- An operator updates a user profile in the management system
- An accountability officer responds to an event on behalf of a user
- A user profile is updated via the User Sync Client
- A user profile is updated via the API
- A user profile is updated via a CSV import

Authentication and validation

- **Desktop app session validation:** The performance of desktop app session validation was improved. The desktop app delivery protocol was updated to use the User ID and session ID to perform session validation checks.
- **Smart card authentication with a derived credential:** Smart card authentication is now supported on the BlackBerry AtHoc mobile app. Smart card users can derive their authentication credential from a certificate stored on the smart card to authenticate themselves while accessing privileged features like publishing alerts. For more information, see "[Enable smart card authentication for the mobile app](#)" in the *BlackBerry AtHoc Smart Card Authentication Configuration Guide*.
- **Mobile app authentication setting:** A new setting was added to allow operators to select smart card authentication for mobile operators. For more information, see "[Mobile app](#)" in the *BlackBerry AtHoc Manage Users Guide*.

Account

- **Accountability Officer search:** Advanced search capability was added to filter the list of Accountability Officers displayed on the Add Accountability Officers dialog. When adding Accountability Officers to accountability templates, any Accountability Officers who are targeted in the Affected Users section are preselected. If affected users are targeted by advanced query in the Affected Users section, the same search criteria are prepopulated in the Add Accountability Officers dialog. The number of rows displayed on the Add Accountability Officers dialog was increased to 15.
- **Recurring accountability events:** Operators can now set up recurring accountability events. For more information, see "[Set recurrence](#)" in the *BlackBerry AtHoc Account User Guide*.

Mobile device management

- **Device deletion:** BlackBerry AtHoc now notifies PSS when a user device is deleted.
- **Identify and delete unused mobile devices:** Operators and end users can view their mobile devices from their user profile in the management system or Self Service. Mobile devices are listed by recognizable names. Previously, mobile devices were identified only by UDID. Users can more easily identify and delete their unused devices. For more information, see "[Delete unused mobile devices from your profile](#)" in the *BlackBerry AtHoc Self Service User Guide*.

Situation Response

BlackBerry AtHoc Situation Response provides a centralized approach to critical event management to properly plan, manage, and remediate crises and improve business continuity.

- **Activity log:** Operators can now export the activity log to a .csv file.
- **Alert steps in incidents:** Alert steps in live incidents now have an **Edit/Publish** button instead of a **Run** button. Operators can edit any content in an alert in a live incident before publishing it. For more information, see "[Activate plan steps](#)" in the *BlackBerry AtHoc Situation Response User Guide*.
- **Attachments step type:** The Attachments step type can be added to a plan.
- **Step previews:** Plan Managers and Plan Incident Managers can now preview details about a step before adding the step to a plan or running the step during an incident.
- **Usability improvements:** Usability improvements for plan and incident management, including the ability to filter the change requests section by general requests, were made.

- **View active steps:** Plan Incident Managers can now view the details of an active step in a live incident.

Note: BlackBerry AtHoc Situation Response is not FedRAMP certified.

For more information, see the [BlackBerry AtHoc Situation Response User Guide](#).

Self Service

- **Default view:** The Acknowledge button on the Self Service disclaimer page is always displayed, regardless of the default view set on the user's device.
- **Display mobile devices in user profiles:** Mobile devices are displayed in the AtHoc Apps section of user profiles in Self Service. Unused mobile devices can be removed. For more information, see ["Delete unused mobile devices from your profile"](#) in the [BlackBerry AtHoc Self Service User Guide](#).
- **Multilingual support:** Self Service was updated to display all out-of-the-box system attributes in the language selected by the user. In addition, any custom attributes that have translations provided for them in the BlackBerry AtHoc management system are displayed in the language selected by the user.
- **Option to hide Organization Subscription and User Move:** Administrators can hide the "Move to organization" and "Organization subscription" options for users in Self Service. These options can be selected in Settings > General Settings in the BlackBerry AtHoc management system. For more information, see ["Enable user move"](#) and ["Select organizations for subscription"](#) in the [BlackBerry AtHoc System Administrator Configuration Guide](#).
- **Self registration:** Administrators can select the fields that appear on the registration screen for users to self register in Self Service. Up to 10 attributes and personal devices can be selected for inclusion on the self registration screen. Administrators can select that an email device be used as the username. Administrators can configure whether users must enter an email when they register for Self Service. For more information, see ["Self Service"](#) in the [BlackBerry AtHoc Manage Users Guide](#).
- **Self registration improvements:** End users may leave the Self Service registration process after they have completed the first screen, believing the registration is complete. They must proceed to the second screen in Self Service to complete the registration process. The following improvements were made to encourage users to complete the full Self Service registration process:
 - On the registration form, the "Register" button was changed to "Continue."
 - The Password Rules were removed from the registration page. They are displayed as a tool tip instead.
 - The AtHocIWSAlerts system name was removed from the registration page.
 - The BlackBerry AtHoc text and logo were removed from the bottom of the registration page.
 - In Self Service, the "Cancel" button was removed.
 - In Self Service, the "Save" button was renamed to "Submit."

For more information, see ["Register for Self Service"](#) in the [BlackBerry AtHoc Self Service User Guide](#).

- **Session timeout:** The Self Service session timeout was increased from 15 to 30 minutes.
- **Support for French locale:** Users with a French OS and locale now land on the French Self Service.
- **508 compliance improvements:** The following 508 compliance improvements were made:
 - Insufficient color contrast was improved.
 - The calendar and the date fields within the calendar can now be accessed by keyboard navigation.
 - In the Inbox, in the Advanced Search:
 - The Alert Type field name is read out by screen readers as "Select Alert types."
 - The Sent field is read out by screen readers as "Sent from. Enter date in mm/dd/yyyy format."
 - Screen resize up to 200% is supported.
 - Keyboard navigation is fully readable by screen readers.
 - Keyboard and mouse navigation to non-actionable labels was added.
 - Non-text content can be read by screen readers.

SMS opt-in

- SMS Opt-In enables operators to allow community members, visitors, event participants, or other users outside of their organization to subscribe to receive alerts by SMS. These outside users can subscribe to receive alerts by sending a text event code via SMS. Organization Administrators create event codes, and then share the event code and the short code with users. When a user opts-in by sending an SMS with the event code, they are added to the BlackBerry AtHoc management system. Administrators can then target them in alerts. For more information, see the [BlackBerry AtHoc SMS Opt-In User Guide](#).

User sync client

- **Bulk updates of users' physical addresses:** The BlackBerry AtHoc user sync client can be used to bulk-update your organization's users' physical addresses without the need to convert the addresses to the latitude,longitude or POINT(longitude latitude) format. The user sync client sends a query to the Bing geolocation API to calculate the longitude and latitude of the user's physical address provided in the input file. Only addresses that the Bing API returns with a match code of High Confidence or Good are processed and added to the database. The latitude,longitude and POINT(longitude latitude) formats are still supported. For more information, see "[How to bulk update users' physical location](#)" in the [BlackBerry AtHoc User Sync Client Guide](#).
- **Full sync attribute:** The default value of the <isFullSync> attribute is now "true" in the user sync client configuration file.

Cloud and delivery services

- **Pager release 2.9.20:** Support was added for Fax and Pager plug-ins.
- **TAS:** The following new locales were added:
 - Arabic
 - Greek
 - Polish
 - Russian
 - Swedish
 - Turkish

Mobile app

Mobile App 4.10 for iOS and Android

- **Mobile app registration:** Users can now register to use the BlackBerry AtHoc mobile app without having an existing user account in BlackBerry AtHoc. End users can register by providing only their email address. If the user account exists, the mobile app registration is complete. If no user account exists, one is created automatically using the provided email address as the username. If the "Email - Work" device is enabled on the organization, the user's email address is populated in their user profile as the "Email - Work" device. If the "Email - Work" device is not enabled in the organization, any enabled email device is used.

To enable this functionality, select the "Create New User if an Account is not Found" option in the BlackBerry AtHoc management system at **Settings > User Authentication > Assign Authentication Methods to Applications > Mobile App**.

- **Registration flow improvements:**
 - When a System Administrator has configured an organization to allow users to modify their user profiles via the mobile app, when a new user successfully registers, they are directed to the My Profile page so they can update their user profile immediately. The email address used during registration is populated in the user's profile automatically.
 - When a user enters their email address to register the mobile app, BlackBerry AtHoc checks for a mapped domain for the entered email. If one is found, the user can complete the registration without entering an organization code. If the entered email address does not match a mapped domain, the user is presented with a screen to enter their organization code.
 - When a user enters their email address to register the mobile app, BlackBerry AtHoc checks whether a user account already exists for the user. If no account is found, one is created automatically.
 - When a user updates their user profile on the mobile app and taps to save the changes, a "Changes have been saved" pop-up is displayed. Users can click OK on the pop-up to go to the Inbox.
- **Show Preferred Language:** The My Profile page was updated to include a Show Preferred Language option. Users can choose from these supported languages:
 - English (US)
 - English (UK)
 - Español
 - Español (Latinoamérica)
 - Français
 - Français (Canada)
 - Deutsch (German)
 - Italiano (Italian)
 - Nederlands (Dutch)
- **Deprecated Mobile App versions:** The following mobile app versions are deprecated: 3.5.x, 4.0, and 4.1.x.
- **OS support updates:**
 - Support was added for iOS 15.
 - Support was added for Android OS 12.
 - Apple iOS 13 and iOS 12 are no longer supported.
 - Android OS versions 8.0.x, 7.0.x and 7.1.x are no longer supported.

Mobile App 4.9.1 for iOS and Android

- **Supported Android OS versions:** Android OS versions 7.0.x and 7.1.x are no longer supported.
- **Supported iOS versions:** Apple iOS 12 is no longer supported.
- **Support for Samsung Knox Devices:** The Samsung Knox Galaxy XCover 5 device has an XCover (push-to-talk or PTT) key that can be mapped to perform a check-in or check-out on the BlackBerry AtHoc mobile app. Samsung Knox Galaxy XCover Pro devices also have a Top (emergency) key that can be mapped to send an emergency from the BlackBerry AtHoc mobile app. For unmanaged devices, end users can map the XCover and Top keys in the Advanced settings on their Samsung Knox devices. For managed devices, mobile administrators can map the XCover and Top keys using BlackBerry UEM or the Samsung Knox Manage Admin Portal and push them out to their users' managed devices. For more information, see "[Configure hardware key mapping for Samsung Knox devices](#)" in the *BlackBerry AtHoc Mobile App Administrator Guide*.
- **Critical alert notification support for iOS:** For iPhone 12 and above, users now receive consistent critical alert notifications. The BlackBerry AtHoc mobile app now always plays a sound for high severity alerts. Previously, the iPhone 12 did not play a sound for high severity alerts when it was set to Do Not Disturb or was muted or the mobile app was not running in the background.

- **Email verification:** During the registration process, when a user submits their email address, the mobile app displays a screen informing them that a confirmation email was sent. The confirmation screen presents a countdown timer while the mobile app checks the status of the email verification.
- **Admin log update:** The BlackBerry AtHoc mobile app admin log was updated to capture delays in sending out push notifications.

Mobile App 4.9 for iOS and Android

- **Organization subscription:** Mobile app users can subscribe to organizations from the mobile app. A new Subscriptions screen was added. To display the Subscriptions page, administrators must enable the My Profile Page setting in the Advanced Features settings for the mobile app. For more information, see ["Enable organization subscription"](#) in the *BlackBerry AtHoc Mobile App Administrator Guide* and ["Subscribe to organizations"](#) in the *BlackBerry AtHoc Mobile App User Guide*.
- **My Profile screen:** A new My Profile screen was added to the mobile app menu. The My Profile page enables end users to edit their user profile. For more information, see ["Update your user profile"](#) and ["Subscribe to organizations"](#) in the *BlackBerry AtHoc Mobile App User Guide*. To display the My Profile screen, administrators must enable the My Profile Page setting in the Advanced Features settings for the mobile app. For more information, see ["Role-based permissions for the mobile app"](#) section in the *BlackBerry AtHoc Mobile App Administrator Guide*.
- **My Profile error messages:** The following error messages were added when saving user profile details:

Error code	Error message
INVVAL1281	Invalid payload.
INVVAL1282	Invalid phone number.

- **Analytics for My Profile screen:** BlackBerry AtHoc collects data for analytics when a user accesses the My Profile screen, makes updates to their profile, or subscribes to or unsubscribes from an organization from the My Profile screen.
- **Alert template screen:** The template list and details screens were improved. The Edit icon in each template section was moved to prevent users from tapping the Publish button when attempting to edit the template. When a template title in the templates list is truncated, users can long press (Android) or 3D touch (iOS) to view the complete template title in a message box.
- **Branded logo on splash screen:** When the mobile app starts, it displays the BlackBerry AtHoc logo and then displays the logo for the latest connected organization on the splash screen. If the user disconnects from an organization and starts the mobile app, only the BlackBerry AtHoc logo is displayed on the splash screen.
- **Menu screen:** A larger logo for the connected organization is displayed on the Menu screen.

Mobile App 4.8 for iOS and Android

- **Smart card authentication with a derived credential:** Smart card authentication is now supported on the BlackBerry AtHoc mobile app. Smart card users can derive their authentication credentials from a certificate stored on the smart card to authenticate themselves while accessing privileged features like publishing alerts. For more information, see ["Enable smart card authentication for the mobile app"](#) in the *BlackBerry AtHoc Smart Card Authentication Configuration Guide*.
- **Mobile app badge counter improvement:** When a user receives a push notification on the mobile app, the badge counter now displays only the number of unread or new collaboration and alert messages.

Mobile App 4.7 for iOS and Android

- **Biometric authentication:** The mobile app now supports the use of Touch ID and Face ID to authenticate operator access to publish alerts and access the alert reporting summary. For more information, see "[Enable or disable biometric authentication](#)" in the *BlackBerry AtHoc Mobile App User Guide*.
- **Scheduled Location Access:** Operators can actively track a group of users for a selected interval. Scheduled location access enables operators to more accurately track where mobile personnel are without relying on end users to perform manual check-ins from the mobile app. When scheduled location access is enabled, users receive an alert on the mobile app that location access has started. For more information, see "[Configure scheduled location access](#)" in the *BlackBerry AtHoc Mobile Administrator Guide*.
- **OS support:** Android 6 and iOS 11 are no longer supported.
- **SSA Maps removed:** The Shared Situation Awareness (SSA) map is no longer supported. The Map option was removed from the menu.

Mobile App 4.6 for iOS and Android

- **Alert Responses:** The ability to view user details for alert responses on the mobile app was added.
- **Collaborate:** The mobile app integrates with the Situation Response Collaborate feature to enable users to send and receive messages.
- **New Logout option:** A new Logout option was added to the Mobile App menu.
- **User Device Identifier (UDID):** The User Device Identifier for end users is displayed in the mobile app.

Desktop app

Desktop app 7.3 (Windows)

- **Branding updates:** The following BlackBerry branding updates were made for the desktop app:
 - The desktop app is installed in the "BlackBerry" folder.
 - The Windows Start menu displays the desktop app as "BlackBerry AtHoc Desktop Notifier."
 - In C:\Program files\, the folder name is "BlackBerry AtHoc Desktop Notifier."
 - In C:\ProgramData\, the folder name is "BlackBerry AtHoc Desktop Notifier."
 - In Add/Remove Programs, the publisher is "BlackBerry."
 - When the desktop app is not connected, when hovering-over the icon, "BlackBerry AtHoc Desktop Notifier" is displayed.
 - When the desktop app is connected, when hovering-over the icon, "BlackBerry AtHoc Desktop Notifier - *organization-name*" is displayed.
- **Failover improvement:** The desktop app was updated so that failover URL values are returned to the desktop client as part of GetUpdate. Previously, updated failover URL values were downloaded to the client as part of the base URL call. If an operator updated the failover URL, the change was not downloaded to the client until a client machine was restarted, went offline and then back online, or a session became invalid.
- **Multiple browser sessions:** The desktop app no longer launches a new browser window in incognito mode. When multiple desktop app editions are running on the same computer, you must close the browser window for one edition before you can launch a browser window with a different desktop app edition.
- **Self Service menu items:** A new "Access My Profile" menu item was added. This menu item opens the My Profile page in Self Service in read-only mode. The "Access My Profile" menu item appears in the system tray by default.
- **508 compliance:** The About menu option screen was updated to improve screen reader capabilities on the About and System Information tabs.

Desktop app 7.2 (Windows)

- **Support for multiple certificates:** Support was added for multiple certificates for CAC authentication. This enables users in multiple-user environments to authenticate on a shared computer.
- **Support for multiple desktop client editions:** Support was added for multiple client editions on the same computer. When requesting a new desktop app, there are now multiple editions available for BlackBerry AtHoc and BlackBerry Alert. Multiple editions can run on the same computer and can point to different organizations on the same BlackBerry AtHoc system or on different systems. Multiple instances of the same edition on the same computer are not supported.

The following client editions are available:

- BlackBerry Alert: 0_BlackBerryAlert
- BlackBerry AtHoc: 1_BlackBerryAtHoc
- BlackBerry AtHoc Alt: 2_BlackBerryAtHocAlt
- BlackBerry AtHoc Aux: 3_BlackBerryAtHocAux

Desktop app 2.4.1 (Mac)

- **Packaging utility update:** The packaging utility for the Mac desktop client was updated to support Mac OS (Apple Silicon) and the latest macOS releases including macOS 12 Monterey, macOS 11 Big Sur, and macOS 10.15 Catalina.

Desktop app 2.4 (Mac)

- **Safari permissions:** Safari no longer requests permission to access web pages when the URLs are launched from the desktop app menu.

Desktop app 7.1 (Windows)

- **Internet Explorer dependency removed:** The desktop app 7.1 for Windows is no longer restricted to using only Internet Explorer and can now also be used with Chrome, Microsoft Edge, and Firefox. The desktop app now uses the user-defined system default browser when:
 - Self Service or any other URL is launched from the desktop app menu.
 - A desktop alert is delivered to a browser. Deep links in a desktop alert to Self Service or to the live map also open in the user's system default browser.

Desktop app 7.0 (Windows)

- **New desktop app 7.0 version:** Desktop app version 7.0 is a new desktop app, not an update to the 6.2.x.X desktop app.
- **Registration process:** After installing the Windows desktop app, if the Defer to Self Service authentication method is configured, users are redirected to Self Service to generate a registration code to complete the registration process and connect. For more information, see "[Register the desktop app \(Windows only\)](#)" in the *BlackBerry AtHoc Desktop App User Guide*.
- **Desktop app system tray:** For new desktop app deployments, the BlackBerry AtHoc Management System menu item in the desktop app system tray menu is no longer included by default. Enterprise Administrators and Organization Administrators can add the BlackBerry AtHoc Management System menu item in the System Tray Menu XML. If the menu item is added, all operators connected to the desktop app will see the menu item after the next get update (GU) call.

For existing desktop app deployments, the BlackBerry AtHoc Management System menu item will be removed from the desktop system tray menu when:

- An Enterprise Administrator or Organization Administrator makes any update to the system tray menu XML.
- The desktop app gateway is saved.
- The desktop app completes a GU call to retrieve new System Tray Menu XML for the organization.

Only users with operator permissions will see the BlackBerry AtHoc Management System menu item.

- **Localization:** The About screen and its tabs are fully localized.
- **C++ client migrated to C#:** The desktop client was updated from using C++ technology to using the C# language. This update enables support for .net framework 4.5 and later releases and simplifies creating the desktop client MSI.
- **Client config and CSI service:** The desktop client configuration and CSI services were updated to use asp.net core.
- **508 compliance:** 508 compliance improvements were made in the following areas:
 - Screen readers (for delivered alert content, response options, and desktop app contents)
 - Color contrast ratio
 - Mouse navigation
 - Keyboard navigation

Desktop app 2.3 (Mac)

- **Source code and build modifications:** The BlackBerry AtHoc desktop app was updated to use a different source code management system and to support updated branding.

Desktop app 2.2 (Mac)

- **Smart card authentication:** The following changes were made to address smart card authentication issues with macOS:
 - The BlackBerry AtHoc desktop app supports external PIV/CAC cards to connect users to the BlackBerry AtHoc management system. The desktop app can now read and use the certificates in a physical PIV/CAC card to obtain user information and use that information to authenticate with BlackBerry AtHoc. When the authentication type is set to Smart Card Authentication, user certificates do not need to be available in the macOS device keychain. The desktop app can read the certificates when a PIV/CAC card is inserted in a physical laptop.
 - The desktop app can now read certificates without a private key installed in the keychain for smart card authentication.

Desktop app 2.1 (Mac)

- **Section 508 compliance:** The following section 508 compliance improvements were made:
 - Keyboard navigation
 - Color contrast
 - Screen reader capabilities

Desktop App 2.0 (Mac)

- **Apple Notarization:** Support for the Apple Notarization service was added. The Apple notarization service automatically scans the desktop software for malicious content or components.

- **macOS Catalina:** Support for macOS 10.15 Catalina was added.

IIM

- **6.0.0.x:**
 - **Migration to .NET:** The IIM is made of the following modules: Relay input card, text-to-speech, serial port, interface to BlackBerry AtHoc, encoders, logging, UI, license manager, and watch dog. Each of these modules were translated into .NET from JAVA. During the migration from Java version to .NET version, the design and architecture of all IIM modules and interfaces were not modified. The features and functionality are unchanged in the .NET version of the IIM from the Java version. IIM was migrated from a Java to a .NET code base on Windows 2012 and 2016 for the following integrations:
 - American Signal (AmSig)
 - ATI
 - Federal Signal (FedSig)
 - IPBS
 - Whelen
 - **API retry:** API retry enhancement was added.
 - **API v2:** The SDK API was upgraded to API v2.
 - **Relay indicator:** The following relay indicators were added:
 - Push button
 - Success alert publish
 - Alert publish failure
 - Strobe Activation
 - Network Failure/Silent test
 - **IIM FIPS 140-2 compliance:** IIM was made FIPS 140-2 compliant by removing the Md5.cs library and replacing the SharpZip library with a secure FIPS 140-2-compliant library.

Security

- **.NET Core Runtime version:** To install the latest security enhancements, update the .NET Core Runtime version to 3.1.25 after upgrading to BlackBerry AtHoc release 7.15.

SDK specification

- **SDK Specification Guidelines:** The BlackBerry AtHoc SDK specification guidelines were removed from docs.blackberry.com.

Behavior changes

Behavior changes are changes in existing functionality that you need to be aware of when upgrading to BlackBerry AtHoc release 7.15. These changes require that you re-learn existing functionality.

- **Default SMS device option:** SMS text alert body is limited to 350 characters by default. SMS is designed to handle short messages from 150 to 350 characters. The new default option was introduced because numerous countries' SMS regulating bodies have recently increased their enforcement of SMS length regulations. As a result of the increased enforcement, sending a long-form alert using SMS jeopardizes the delivery assurance of the message, making your system less effective. Sending a long-form alert using SMS also impacts our compliance with carrier regulations. For that reason, we have introduced a default option that limits the alert body to 350 characters. The 350 character limit does not include the title and response options. When including response options, the alert creator must ensure there is sufficient information in the first 350 characters of the alert content to allow end-users to select a proper response.
- **Device delivery preference:** When device delivery preference is enabled and the operator selects Organization-defined in the alert template, setting the priority of phone devices from the UI is not available.
- **Distributions Lists API:** The Distributions Lists API now returns only distribution lists that the user has permissions to manage or publish by default.
- **Last Known Location attribute:** For location-based targeting, users with any geolocation attribute and users whose Last Known Location attribute has been updated within the last 4 hours are targeted. When an operator adds a location to an alert, the following message is displayed below the map: "Locations selected here will target all user geolocation attributes, plus Last Known Location Updated within the past 4 hours."
- **Legacy desktop templates support:** In BlackBerry AtHoc release 7.6, support for the following legacy desktop delivery templates were removed:
 - Amber Desktop Popup
 - Gray Desktop Popup
 - Green Desktop Popup
 - Red Desktop Popup
 - Yellow Desktop Popup
 - Black Desktop Popup
 - White Desktop Popup
 - Tan (Brown) Desktop Popup
 - Blue Desktop Popup
 - Orange Desktop Popup

In BlackBerry AtHoc release 7.15, support was reinstated for these desktop delivery templates, with the exception of the Weather Template. After migration to 7.15, any custom alert template that uses the Weather Template will be updated to use the default severity template instead of the custom template. These reinstated desktop delivery templates do not support attachments or including a map in 7.15.

- **Live map support for IE:** The live map is not supported on the Internet Explorer browser.
- **Mass device name update:** (For users on the alerts5 system only.) The following mass device names were updated:

Previous mass device name	Updated mass device name
American Signal Giant Voice	Sirens
CAP Exchange	COG to COG
Community Warning System Feeds V2	Community warning system

Previous mass device name	Updated mass device name
Industrial strobe beacon	Strobe
IPAWS-EAS	EAS
IPAWS-NWS	NWS
IPAWS-NWEM	NWEM
IPAWS-WEA	WEA
RSS Feeds	RSS

- **Mass device targeting:** The Select All option was removed when targeting mass devices to prevent multiple alerts from being sent on Giant Voice speakers.
- **Migration from BlackBerry AtHoc release 7.9 to 7.15:** When migrating from BlackBerry AtHoc release 7.9 to 7.15, live alerts and accountability events are not automatically ended.
- **Mobile app check-in button:** When a user taps the check-in button (📍), the check-out button (📶) is displayed. Users must tap the check-out button before they can check in again.
- **Next Occurrence timestamp:** The Next Occurrence timestamp in alert and event templates was a static field. Now, this field changes automatically when Daylight Savings Time (DST) occurs.
- **Operator audit trail:** The operator audit trail now retains data for up to six months. A purge job runs once a month to remove data older than six months. If you need to retain data in the operator audit trail for longer than six months, you can use the API or export functionality to export and archive the data locally.
- **Operator role display:** If a feature is not enabled for an organization, then operator roles associated with those features are no longer displayed.
- **Organization Administrator access on the System Health page:** Organization Administrators can view health monitors on the System Health page. Organization Administrators cannot access modified or created health monitors, or add, delete, or edit health monitors. Ownership of any existing health monitors created by an Organization Administrator will be transferred to the Enterprise Administrator and System Administrator.
- **Organization code:** The organization code in General Settings is auto-generated from the organization name and is now a required field.
- **Placeholders in draft alerts:** Placeholder values for draft alerts are now resolved on the Review and Publish page. This enables alert publishers to view the final content of the message before publishing the alert.
- **Recorded response options:** Recorded response options are now played when an alert is delivered to an end user's phone.
- **Response option attributes:** The "Use as a Response Option" setting must be enabled for a user attribute to be available as a response option. Select this option in Settings > User Attributes.
- **Response option values:** User attributes with more than 9 values cannot be used as response options.
- **Roles:** The Advanced Alert Publisher and Alert Manager roles were added. The Advanced Alert Manager and Alert Publisher roles were modified. For more information, see "[BlackBerry AtHoc roles](#)" in the *BlackBerry AtHoc Manage Operators and Administrators Guide* and the *BlackBerry AtHoc Operator Roles and Permissions Matrix*.
- **Self Service My Info Updated On:** The "Self Service My Info Updated On" attribute was renamed to "My Info Updated On." This attribute is updated when an end user manually updates their user profile through Self Service or the mobile app. The My Info Updated On attribute is searchable in advanced queries and is displayed on user profiles in the BlackBerry AtHoc management system.
- **Single Sign On logout service:** In the SSO Service Provider settings, the Logout Service URL was renamed to "Custom Logout URL." The new Logout Service URL is read-only and is pre-populated with the URL of the service provider's endpoint that receives SAML log out messages. For more information, see "[Configure Service Provider settings](#)" in the *BlackBerry AtHoc Single Sign-On Administrator Guide*.

- **SMS link:** When an operator sends an alert to SMS devices that exceeds the 1,250 character limit for title and body, the message may be delivered as multiple messages depending on target user's mobile service provider. If the title and body exceed the 1,250 character limit, the title and body are truncated and a link is provided for the user to view the complete message so that users can view the complete message without piecing together multiple messages. This link now appears before any response options that are included in the alert.
- **SMS URL domain name change:** The number of characters for the SMS URL was reduced, so that more characters are available for SMS messages and the number of additional SMS pages is reduced. The SMS URL is included in SMS alerts to view the entire alert content and reply. The URL was updated from d1.athoc.com and d2.athoc.com to athoc.io.
- **SSO:** A password is required to upload an SP certificate for SSO.
- **Suborganization user move:** Operators who are End Users Managers, Organization Administrators, Alert Managers, or Advanced Alert Managers in a suborganization can move and subscribe users from their suborganization to other suborganizations. For more information, see "[Enable user move](#)" in the *BlackBerry AtHoc System Administrator Configuration Guide*.
- **Support for IDP-initiated SSO:** Support was added for IDP-initiated SSO. Previously, only the SP-initiated SSO authentication flow was supported.
- **Text Messaging option:** The Alert Title and Body option was removed from the Personal Device Options settings for text messaging.
- **Two-factor authentication:** When two-factor authentication is enabled and the "User must change password at next login" option is selected, users are prompted to select a delivery method for receiving an activation code, then use the code to change their password.
- **Updated help text:** The SMS targeting help text and warning messages were updated.
- **User export:** The number of users that can be exported to a .csv file is limited to 25,000. When exporting more than 25,000 users to a .csv file, select a grouping of 25,000 users to export.
- **WEA 2.0 device option changes:** The Mass Device options for WEA 2.0 now include options for "English" and "English and Spanish." A text box was added for messages with a 90-character limit. Both 90-character and 360-character limit custom text boxes display the character count.

Breaking changes

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

- **Alert templates:** The New Alert Template was renamed to ~*** New Alert Template - Configuration Use ***~. The New Template was renamed to ~*** New Template - Configuration Use *** ~. These changes were made to prevent operators from accidentally overwriting the system alert templates when creating a new alert template.
- **API Get Alert Template, Get Event Template, and Alert Details APIs:** The following APIs return AttachmentIds instead of Base64Attachment:
 - GET /orgs/{orgCode}/alerts/{auld}
 - GET /orgs/{orgCode}/alerttemplates/{templateCommonName}
 - GET /orgs/{orgCode}/AccountEvents/templates/{commonName}

To download an attachment, use the AttachmentId with the Attachment GET API:

- GET /orgs/{orgCode}/attachments/{guid}
- **Organization ID and provider ID disallowed in externally-facing URLs:** The organization ID must be replaced with the organization code in any bookmarked Self Service and Single Sign-On URLs. The Provider ID must be replaced with the organization code in the identity mapping file in the SSO configuration.
- **SSO URL:** If a secondary authentication method is selected for Self Service, /SSO is appended to the SSO URL.
- **User base operator import:** When importing user base restrictions, each operator (such as "less than" or "equal to") must be enclosed in double quotation marks ("").

Breaking changes (7.15 FE-11)

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

- **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 7.15, most existing weather alert rules 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.

Resolved issues

The following issues were resolved in BlackBerry AtHoc release 7.15 (OnPrem.)

Jira ID	Description
IWS-14632	Browse - Play does not work the first time the user uploads the audio if the file is not fully uploaded.
IWS-45839	The Event Duration list does not load properly on an accountability event template.
IWS-46310	When viewing Self Service on a tablet device, the Status details sometimes appear under the Display Name column.
IWS-46360	The CentrAlert and Cooper-WAVES gateways were removed from BlackBerry AtHoc. The CentrAlert and Cooper-WAVES output formats were removed from all applicable devices. The default value for the Eaton gateway was updated to "Eaton Waves" instead of "Standard."
IWS-46613	In Self Service with responsive mode on, the Date and DateTime fields from the date selector are not saved.
IWS-46697	If a value of 2147483600 or more is entered in the Offset field of the GET Accountability Event Users List API, the following error is displayed: "An internal error occurred while processing the request."
IWS-46708	Two-factor authentication email delivery does not work for the sparkpost (delivery3.athoc.com) gateway.
IWS-46880	A File Not Found (404) error is displayed when the Export to Excel button is clicked on the placeholder dependency pop-up window.
IWS-46887	The online help link navigates to the wrong release.
IWS-46932	On the Disable End User confirmation window, an incorrect "This action cannot be reversed" message appears.
IWS-47010	An error is displayed when the Export to Excel button on the Delete Attribute dialog is clicked.
IWS-47027	In Self Service, the Clear All button does not work through the keyboard.
IWS-47090	The operator is returned to the previous Delivery Template page after attempting to upload a blank image.
IWS-47124	The Online Users and Messages charts on the Home page are not displayed when using Firefox.
IWS-47125	Data is not displayed in the correct columns after exporting an event summary to a PDF.

Jira ID	Description
IWS-47301	In Internet Explorer, the dependency dialog is displayed even when there are no dependent draft alerts on the Sent Alert or Alert Template pages.
IWS-47348	A configured geolocation for a user is not displayed correctly in Self Service.
IWS-47394	Operator export does not work as expected if you deselect some operators from the list.
IWS-47424	Minor error in the error message when enabling fill count on an alert template.
IWS-47449	On the New Dependent page, the date picker does not work if you save the page without selecting a date.
IWS-47512	Placeholder text is trimmed if you navigate away from the page.
IWS-47731	508 compliance on the Self Service Inbox event details page.
IWS-48387	<p>The following APIs do not reach the expected limit of 800 per minute with a benchmark of 30% CPU consumption:</p> <ul style="list-style-type: none"> • OrgUsers > Get Users List • Publishing > Get Alert List • Publishing > Get Alert Types • Publishing > GetTemplateDetails • Publishing > GetAlertDetails • Publishing > PublishAlert • Reporting > GetHierarchySummaryReport
IWS-48393	Health monitors create a schedule with an automatic expiration of 10 years.
IWS-48394	User attributes are not displayed in a user profile in Self Service.
IWS-48634	A session timeout leads to an error on the Edit Profile dialog in Self Service.
IWS-48861	In Self Service, an operator's user base restrictions are incorrectly applied to the operator's profile, preventing them from editing their profile.
IWS-49084	The Organization Subscriptions section was removed from dependent user profiles in Self Service. The organization subscription feature is not available for dependents.
IWS-49150	The Disable and Delete Users window does not show users in suborganizations.

Jira ID	Description
IWS-49292	The Collaborate page takes a minute to load. If you send a message while the page is loading, you will see the sent message but not previous messages in the collaboration. If you attempt to end a collaboration before the Collaborate page loads, the following error message is displayed: "[2006] The collaboration could not be accessed."
IWS-49502	After changing the locale in Self Service from the language selection drop-down menu in the footer, an error message is displayed in the base locale instead of in the locale selected in the drop-down menu.
IWS-50528	Importing a large number of users with a disabled status results in event viewer errors.
IWS-50617	When logging off from BlackBerry AtHoc and Self Service, an error is displayed.
IWS-50754	Moving a large number of users with status attributes using a .csv file results in event viewer errors.
IWS-50889	Email alert responses are not recorded in the Alert Summary after 8 hours.
IWS-51021	When multiple single sign-on sessions are opened in different browsers, a logout error appears.
IWS-51046	Non-English characters cannot be added to desktop app menu items.
IWS-51099	A "maximum number of sessions has been reached" error occurs for all operators as soon as concurrent session limits is enabled, regardless of the number of allowed concurrent sessions.
IWS-51416	Scheduled alerts are getting stuck in the "Publishing" status.
IWS-51478	When an event template with a 100-character name is added to a plan and an incident is created from it, the event is published but only the initial email is received. Follow-up and end event emails are not received. Placeholder errors are also displayed.
IWS-51744	Import via a .csv file fails when an organizational hierarchy attribute with a Dutch character "ë" is replaced with a question mark (?).
IWS-51757	The "Roles in other organizations" link on the distribution list manager page is no longer a link.
IWS-51775	Importing date values does not work when upgrading from ADSync 1.2.7 to USC 1.1.11.
IWS-51785	When a picklist attribute with duplicate values is imported via a .csv file, errors are displayed when synchronizing users or saving from the BlackBerry AtHoc management system.

Jira ID	Description
IWS-52049	An error is displayed when an SDK publishing payload includes a location.
IWS-52491	In the Organization Subscriptions section of a user's profile, the warning message when trying to set an end date that is earlier than the start date was updated to "earlier" instead of "smaller."
IWS-52583	Inconsistencies in the username field in the operator audit trail.
IWS-52922	Unable to create an organization hierarchy node if multiple nodes are created and one node is deleted before the nodes are saved.
IWS-53028	Subscription user import takes an extra 9 seconds for large organizations.
IWS-53330	Importing user attributes fails when an organization name contains a forward slash (/).
IWS-53434	Text on the Prioritize Personal Devices pop-up is not correctly aligned in the French locale.
IWS-53552	Some Self Service menu item links have the incorrect URL.
IWS-53618	If a user is idle in Self Service for more than 30 minutes on the My Profile edit page and then clicks the Save button, or makes other edits to the page and clicks Save, the user is not logged out or redirected to the session timeout page.
IWS-54173	An OR operator that is generated from comma separated or multi picklist values is not translated in German.
IWS-54240	When modifying the user base restrictions for a user, the list of organizations is not in alphabetical order.
IWS-54294	Importing operators with the "User base manage/publish" attribute set to "Organization" results in empty values.
IWS-54354	EVT_CATEGORY_TAB is empty after an upgrade from 6.1.8.85 to 7.9, causing Connect to fail.
IWS-54402	An API call fails with the following error: "Object reference not set to an instance of an object."
IWS-54403	When an operator with restricted permissions attempts to edit and save a user, a SQL timeout error is displayed.
IWS-54474	An API user sync fails and displays the following error: "Object reference not set to an instance of an object."

Jira ID	Description
IWS-54543	Support was added for non-English conditional operators (AND/OR) in operator roles import.
IWS-54571	User move does not work as expected when using the advanced user search in the user manager.
IWS-54589	The user search API does not work with the OR condition after an upgrade to release 7.11.
IWS-54693	A user's last known location is not displayed on the map when a dynamic distribution list is created using a "Mobile app equals Active" condition.
IWS-54847	The UAP Health Test monitor is missing in BlackBerry AtHoc release 7.11.
IWS-54934	508 Compliance: Tab navigation on Self Service pages does not scroll down.
IWS-55090	Operator export does not work as expected from an enterprise organization.
IWS-56067	Sorting with Updated On column on the API Applications page does not work as expected.
IWS-56591	An operator's user base restriction with an OR condition prevents tracking reports from showing all targeted users.
IWS-56687	User move displays a 404 error when using some conditions.
IWS-56712/IWS-56713	Importing operators with "User base manage/publish" set to use organization attributes results in empty values.
IWS-56868	The User Manager and Advanced Query sections report incorrect user counts for criteria with mobile app device.
IWS-56970	"Export Full Report" links are not working in Personnel Reports.
IWS-57501	The "Exempt redirections for users with username containing" option in System Settings > Redirection Settings > Redirection Rules does not work.
IWS-57724	If an operator has restricted permissions to access a specific alert folder and that folder is deleted, an export of that operator still contains the deleted alert folder.
IWS-57905	The following actions appear in the Operator Audit Trail with an Object ID of 0 instead of the user ID: <ul style="list-style-type: none"> • Operator permissions revoked • Operator permissions granted • Password changed

Jira ID	Description
IWS-57906	Publishing is unavailable using the publisher map when large layers are selected.
IWS-58093	A different Target Users count appears when drawing a shape that is the same size and location of a Predefined Location.
IWS-58128	Using unsupported desktop delivery templates can cause the following issues: <ul style="list-style-type: none"> • "More Info" and "View Location" links open in Microsoft Internet Explorer instead of in the user-defined default browser. • Desktop app users receive alerts, but do not see any maps in the alert. • Responses are not recorded and a white screen with the following message is displayed: close67393ADC22204452BD24EF1E9C0586EF
IWS-58611	When using an SSO login URL, the disclaimer pop-up is off-center and partially off the screen.
IWS-58760	Desktop app clients version 7.x.x.x and above fail when loading the Self Service Inbox or My Info pages.
IWS-58817	If a deleted operator attempts to use CAC to log in to BlackBerry AtHoc, the following error message is displayed: "CryptographicException: m_safeCertContext is an invalid handle."
IWS-59055	Published alerts do not appear in the Operator Audit Trail for some time zones.
IWS-59468	On the Self Service My Profile page, the drop-down menu does not work for single or multi-select picklist user attributes that are the maximum character length.
IWS-59781	When signing on to the desktop app, LDAP authentication falls back to domain\username authentication when the LDAP value is empty.
IWS-59783	The Distribution List Report page does not render correctly for an accountability alert that targets a large number of distribution lists.
IWS-60112	The Personnel Report summary does not work as expected for large single picklists.
INT-1928	Some IPAWS alerts show as sent even though they are not sent.
ISEC-1116	Desktop client executes JavaScript in localhost domain.
CLD-1056	Inconsistencies in the text-to-speech playback for the date format were fixed.

Jira ID	Description
CLD-1393	The SMS link webpage should have the copyright string footer at the bottom of the page.
CLD-1404	Fixed split SMS response links in multi-page messages.
CLD-1409	SMS string resources missing strings for a few locales.
CLD-1426	The TAS call flow was optimized to fix a performance degradation issue with TTS.

Known issues

This section lists known issues in BlackBerry AtHoc releases.

7.15

- There are no additional known issues in release 7.15.

7.14

Jira ID	Problem	Workaround
Alerting		
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.	—
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.

7.13.1

- There are no additional known issues in release 7.13.1.

7.13

- There are no additional known issues in release 7.13.

7.12

- There are no additional known issues in release 7.12.

7.11

- There are no additional known issues in release 7.11.

7.10

Jira ID	Description	Workaround
Collaborate		
IWS-51450	After a mobile user is disabled or deleted, they are still able to send messages and attachments in collaborations.	Manually remove the disabled or deleted user from the collaboration.

7.9

Jira ID	Description	Workaround
Alerting		
IWS-61042	In a Basic organization, saving a draft alert more than one time causes an error.	—

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

©2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

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

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

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

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

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

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

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at <https://www.blackberry.com/us/en/legal/third-party-software>

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