



# **BlackBerry AtHoc**

## **API Quick Start**

7.15



# Contents

- What is the BlackBerry AtHoc API?.....4**
  - Key differences between API Version 1 and API Version 2..... 4
  - System level guidelines..... 5
- Set up your environment.....6**
  - Create a user account with operator permissions..... 6
  - Provision an application that can call the web API.....6
  - Set up an organization code in the BlackBerry AtHoc system..... 6
- Authentication.....7**
  - Password grant.....7
  - Authorization code grant..... 8
  - Implicit grant..... 9
  - Change organization grant..... 10
  - Refresh tokens.....11
  - Authentication errors..... 12
  - Reset the client secret..... 13
- Call the API.....15**
  - Resolve response codes.....15
- Code samples..... 16**
- Required roles for API access.....17**
- MTLS service error codes..... 36**
- BlackBerry AtHoc Customer Support Portal..... 38**
- Documentation feedback.....39**
- Legal notice..... 40**

# What is the BlackBerry AtHoc API?

**Note:** This document does not contain a full list of the available API endpoints. This list, including detailed definitions of each endpoint, is available in the interactive documentation installed with BlackBerry AtHoc and can be accessed at `[server-address]/api/v2/docs`.

BlackBerry® AtHoc® integrates with existing systems and investments to create a comprehensive end-to-end crisis communication system. A common integration use case is to synchronize all user contact details between an authoritative source and BlackBerry AtHoc. This integration is possible thanks to an extensible set of web APIs. The APIs are designed to integrate a BlackBerry AtHoc system with other systems to make alerting more successful.

BlackBerry has incremented the web-based API to include new REST endpoints. The new REST-based web APIs are referred to as the BlackBerry AtHoc API V2.

This document describes how to get started using the BlackBerry AtHoc API V2. This document assumes that the reader is familiar with the BlackBerry AtHoc product, the end-user interaction, and the use of the management system. Familiarity with API V1 is helpful but not required.

This document also assumes that the reader has a customer relationship with BlackBerry or is working as a developer for a BlackBerry customer.

## Key differences between API Version 1 and API Version 2

The BlackBerry AtHoc API V2 makes establishing new integrations easier for developers. It follows the popular REST pattern with HTTP methods and JSON-formatted payloads. The authentication and authorization are OpenID Connect and OAuth 2.

The following table summarizes the differences between the API V1 and V2:

|                                    | API Version 1   | API Version 2   |
|------------------------------------|---|---|
| <b>Payload format</b>              | XML over HTTP   | JSON over HTTP  |
| <b>Authorization</b>               | Inline username and password  | OpenID Connect with OAuth2 JWT Access Tokens  |
| <b>Calling pattern</b>             | HTTP POST of Custom XML Payload Definitions   | REST with HTTP methods GET, PUT, POST, DELETE   |
| <b>Scenarios covered</b>           | <ul style="list-style-type: none"><li>• User Sync</li><li>• Distribution List</li><li>• Sync Alert</li><li>• Publishing Get Content</li></ul> | <ul style="list-style-type: none"><li>• User Sync</li><li>• Distribution List Sync</li><li>• Get Content</li><li>• Accountability Officer</li></ul> |
| <b>Unique identifier for users</b> | MID (mapping ID)  | LOGIN_ID (username)   |

# System level guidelines

## Throttling limits

- There are throttling limits in place when calling the API. Try to optimize the workflow of calls to the API to achieve the maximum work within the number of allowed calls.
- Your calls may be blocked if they exceed the defined limits of your system or organization.

## Dates and times

- Dates and times will be in the organization time zone unless otherwise specified.

## User synchronization

- Use batches to update multiple users in one request instead of single-user updates in each call.
- Do not exceed more than 1000 users in each call because the SyncBy endpoints are in real-time. If you need to synchronize more than 1000 users in a call, use the background job CSV import endpoint.
- Don't store UserIDs inside your application. The identifier for the user is username or mapping ID.

## Attributes

- The API GET method does not retrieve CommonName attributes when they contain the following special characters : + @ #
- Common names may be optional in the user interface.
- The following APIs do not support attributes whose common name {commonName} or attribute value common name {valueCommonName} contains the forward slash (/) character:

| HTTP type | URL  |
|-----------|--|
| GET       | /orgs/{orgCode}/attributes/{commonName}                                |
| GET       | /orgs/{orgCode}/attributes/{commonName}/Values                         |
| GET       | /orgs/{orgCode}/attributes/{commonName}/Values/{valueCommonName}       |
| DELETE    | /orgs/{orgCode}/attributes/{commonName}/values                         |
| POST      | /orgs/{orgCode}/attributes/{commonName}/values                         |
| PUT       | /orgs/{orgCode}/attributes/{commonName}/values                         |
| PUT       | /orgs/{orgCode}/attributes/{commonName}/values/{ValueCommonName}       |
| DELETE    | /orgs/{orgCode}/attributes/{commonName}/Values/{valueCommonName}/Users |
| PUT       | /orgs/{orgCode}/attributes/{commonName}/Values/{valueCommonName}/Users |

# Set up your environment


## Create a user account with operator permissions

To use the BlackBerry AtHoc API, you must create a user account with operator permissions. The user must have the SDK User role and permissions to access the specific API module. For example, you must have the User Manager role to access the User Sync API.

## Provision an application that can call the web API

To provision a new API integration with the BlackBerry AtHoc management system, you must have organization administrator, enterprise administrator, or system administrator permissions. You must have system administrator permissions to enable a provisioned application.

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

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

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

## Set up an organization code in the BlackBerry AtHoc system

Complete the following task to set up an organization code for your specific organization in the BlackBerry AtHoc management system. This organization code is not propagated to PSS, so if you already have an organization code in PSS, use that one to complete this task.

This task is not required if an organization code for your organization has already been provided to you.

1. Log in to the BlackBerry AtHoc management system as a system administrator.
2. Switch to the specific organization.
3. Go to **Settings > General Settings**.
4. In the **Organization Details** section, enter the organization code. Do not use spaces.

# Authentication

The BlackBerry AtHoc API V2 uses OAuth2-compliant authentication and authorization. To call the API, the client must first obtain an access token. Each organization has one access token. You will need to request an access token for every individual organization that you are calling against. The authentication step returns an access token which will be used when it calls the APIs.

The access token is only useful if the user has an operator role required to access the specific API module. For example, the User Manager role is required for User Sync. For more information, see [Required roles for API access](#).

The parameter `acr_values` should contain the organization code in a key value pair with the `Key=tenant` (for example, `acr_values=tenant:<OrgCode>`) where `<OrgCode>` is the organization code of the organization that you want to access the API for.

Scope should be a space-delimited string of the resources that you want to access. If you also need long-term access to the API, you can request a Refresh Token with the `offline_access` scope. For example, `openid profile athoc.iws.web.api offline_access`.

Depending on your application and security requirements, you can obtain an access token from any of the following supported grant types:

- Password Grant
- Authorization Code Grant
- Implicit Grant
- Change Org Grant
- Refresh Token Grant

## Password grant

The resource owner password grant type allows requesting tokens on behalf of a user by sending the user's name and password to the token endpoint. This is "non-interactive" authentication and is generally not recommended. There may be instances in certain legacy or first-party integration scenarios where the password grant type is useful, but the general recommendation is to use an interactive flow like implicit or auth code for user authentication.

The following is a Postman request for an Access and a Refresh Token using the Password Grant:





```
response_type=code
&client_id=<client_id>
&redirect_uri=<your_app_callback_url>
&scope=openid profile athoc.iws.web.api offline_access
&state=<guid>&acr_values=tenant:<org_code>
&code_challenge=<ClientGenerated_CodeChallenge>
&code_challenge_method=S256
```

**state** This is an opaque value that the application adds to the initial request. During authentication, the application sends this parameter in the authorization request, and the authorization server returns this parameter unchanged in the response. This value must be used by the application to prevent cross-site request forgery (CSRF) attacks. This value can also be used by the application to restore the previous state of the application.

For more information about the state parameter, see:

<https://auth0.com/docs/api-auth/tutorials/authorization-code-grant>

<https://auth0.com/docs/protocols/oauth2/oauth-state>

**code\_challenge:** The code\_challenge is a Base64-URL-encoded string of the SHA256 hash of the code\_verifier. Your application saves the code\_verifier for later and sends the code\_challenge with the authorization request to your authorization server's authorization URL.

For more information about the code\_challenge parameter, see

<https://developer.okta.com/authentication-guide/implementing-authentication/auth-code-pkce>

### Step 2: The browser redirects the user to the login screen.

The browser redirects the user to the login screen. Upon entering login credentials, if the credentials are valid, the browser has the authentication code in the URL. If the credentials or organization code are invalid, the browser displays HTTP status code 400 "Bad Request."

### Step 3: The client requests the access\_token based on the authentication code in step 2.

```
POST https://<Server>/AuthServices/Auth/connect/token
{
  "grant_type": "authorization_code",
  "code": "<code>" //code returned in browser from 2nd Step
  "redirect_uri": "<your_app_callback_url>",
  "client_id": "<client_id>",
  "code_verifier": "<ClientGenerated_CodeVerifier>"
}
```

### Step 4: The authentication server sends the access token response.

```
{
  "expires_in": 3600,
  "token_type": "Bearer",
  "refresh_token": "ljiweoriwoer...",
  "access_token": "okljhgfdsignijuhdfgdkljhgdfkkgjlkjdlfkkgj..."
}
```

## Implicit grant

The implicit grant type is optimized for browser-based applications. The implicit grant type is used for user authentication-only (both server-side and JavaScript applications), or for authentication and access token

requests (JavaScript applications). In the implicit flow, all tokens are transmitted through the browser. Advanced features such as refresh tokens are not allowed as the security of the tokens cannot be guaranteed.

The implicit grant flow has the following steps:

1. Your application directs the browser to the authentication server sign-in page, where the user authenticates.
2. The authentication server redirects the browser to the specified redirect URI, and includes the access and ID tokens as a hash fragment in the URI.
3. Your application extracts the tokens from the URI.
4. Your application can now use these tokens to call the resource server (for example, an API) on behalf of the user.

Starting this flow is very similar to the authorization code flow except that the `response_type` is `token` or `id_token` instead of `code`.

**Step 1: Your browser makes a request to authorize the endpoint of the authorization server.**

```
GET https://<server>/AuthServices/Auth/connect/authorize?
response_type=token
&client_id=<client_id>
&redirect_uri=<your_app_callback_url>
&scope=openid profile athoc.iws.web.api offline_access
&state=<guid>
&acr_values=tenant:<org_code>
```

**Step 2: The user logs in.**

If the user does not have an existing session, this will open the authentication server sign-in page. After authenticating, or if the user has an existing session, the user arrives at the specified `redirect_uri` with a token as a hash fragment.

**Step 3: The authentication server sends a redirect response.**

```
https://localhost:8080/#
access_token=eyJhbkjughfs...
&token_type=Bearer&expires_in=3600
&scope=openid
&state=<state>
```

Your application must now extract the tokens from the URI and store them.

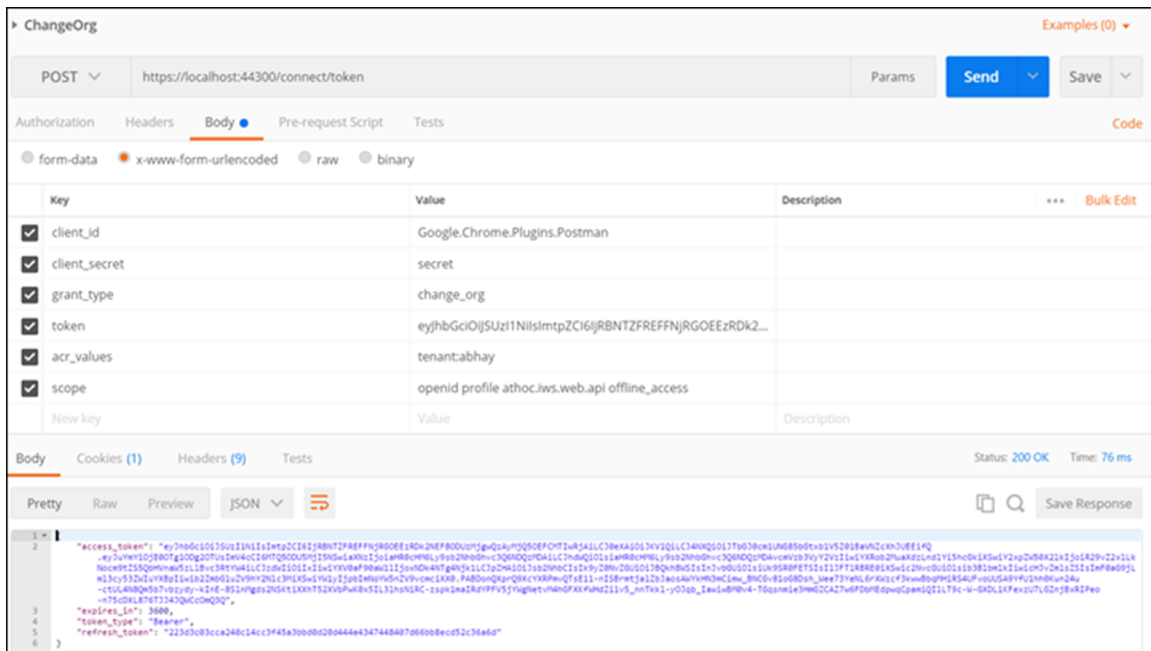
## Change organization grant

The change organization grant has been specifically designed for external applications that allow their users to switch between multiple organizations.

When the application has received an access token based on user credentials, the same access token can be used as the user's identity to get new access tokens for organizations that the user has access to.

The response of this call is a new Access (and Refresh) token based on the user's permissions within the new organization. If the user is not authorized in this organization, an error is returned.

The following is a Postman request and response for the `change_org` grant:



**Note:** The change organization grant type must be requested from BlackBerry AtHoc Customer Support for the provisioned application. The change organization grant is an add-on grant that can be added to any provisioned application using the implicit, authentication code, and password grants.

**URL:** `https://<server>/AuthServices/Auth/connect/token`

**HTTP Verb:** POST

**Parameters:**

- **client\_id:** <client\_id>
- **client\_secret:** <secret>
- **grant\_type:** change\_org
- **scope:** openid profile athoc.iws.web.api
- **acr\_values:** tenant:<org\_code>
- **token:** <current valid access token>

**API Error Response:** If the user is not authorized for the given tenant (organization), the following error code is returned:

401: Unauthorized

## Refresh tokens

Refresh tokens enable granting long-term access to APIs. You should keep the lifetime of access tokens as short as possible. However, you want to avoid forcing the user to perform repeated front-channel round trips to the authentication server to request new access tokens.

Refresh tokens allow new access tokens to be requested without user interaction. Every time the client refreshes a token, it needs to make an authenticated back-channel call to the authentication server. This call allows verifying if the refresh token is still valid or has been revoked.

Refresh tokens expire after 30 days. Refresh tokens have a sliding lifetime window of 15 days. The lifetime of a refresh token is renewed by the amount of time specified in the `SlidingRefreshTokenLifetime` parameter. After 30 days, the client must reauthenticate, regardless of the validity period of the most recent refresh token acquired by the application.

**URL:** https://<server>/AuthServices/Auth/connect/token

### Parameters:

- **client\_id** <client\_id>
- **client\_secret**: <secret>
- **grant\_type**: refresh\_token
- **refresh\_token**: <current valid refresh token>

[illegible]

This topic describes the error codes you may see when authentication of an API client fails. When authentication fails because the client is disabled or not present, a 400 error code is displayed. The following table explains the errors:


| Error code             | Cause  | Action to correct  |
|------------------------|--|--|
| invalid_client         | The client name does not exist or is incorrect, or the client secret is invalid. | Check that the client is provisioned in the API application page and that it is in the Enabled state.<br><br>Reset the client secret and use the new one.  |
| unsupported_grant_type | The grant type is invalid.   | The Grant type cannot be empty. Check that the Grant type is populated with one of the following supported grant type values: Implicit, authorization_code, Password, Change_org.  |
| invalid_grant          | The username or password is invalid, or the tenant code is invalid.              | Make sure that the user credentials are valid and the correct organization code is passed.   |
| invalid_scope          | The scope is invalid.  | The Scope cannot be empty.<br><br>The mandatory Scope value is <b>openid profile athoc.iws.web.api. offline_access</b> .<br><br>The offline_access scope value is an optional value that is required only when requesting a refresh token. |

If you received an error, verify the following items:

1. Your client is properly provisioned and your client\_id and secret are valid.
2. Your client has the password grant configured and allowed.
3. Your username and password fields are correct.
4. The user exists in the organization defined in the acr\_values tenant:<org\_code>.
5. The operator account is not locked.

## Reset the client secret

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

1. Log in to the BlackBerry AtHoc management system.
2. In the navigation bar, click .
3. In the System Setup section, click **API Applications**. The API Applications window opens.

4. Optionally, enter a name in the search box to filter the list of applications.
5. Optionally, select **Enabled Applications** or **Disabled Applications** from the All Applications list to filter the list of applications.
6. Click the application that you want to modify.
7. Click **Reset Client Secret**. A confirmation window opens.

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

# Call the API

You can call the BlackBerry AtHoc web API through a URL in your browser.

To access the BlackBerry AtHoc API, complete the following steps:

1. Log in to the BlackBerry AtHoc management system as an SDK User.
2. In the address bar of your browser, replace "athoc-iws" with "api/v2/docs" . The web API page opens.
3. Enter your organization ID in the **Authorize** field.
4. Click **Authorize**. The Available authorizations window opens.
5. Select the scope option.
6. Click **Authorize**. You are directed to a login page.
7. Enter your username and password.
8. Click **Log In**.

## Resolve response codes

The following table lists response codes and how to resolve them:

| Response code | Description           | Steps to resolve  |
|---------------|-----------------------|---|
| 400           | Bad Request           | Check that the payload and its format are correct. Check for validation errors and take necessary actions to correct the payload.   |
| 401           | Unauthorized          | Make sure that the access token is present, correct, and not expired.   |
| 403           | Forbidden             | <ul style="list-style-type: none"><li>• The operator does not have sufficient operator permissions to execute the request. Log in to the BlackBerry AtHoc management system to modify the roles for the operator.</li><li>• The password used is changed or expired. Generate a new authentication token.</li></ul> |
| 404           | Not Found             | The resources you are trying to find are not present in the system. Pass valid parameters.  |
| 429           | Too Many Requests     | There is a restriction on the number of API calls allowed. Try the service again. If you continue to see this response code, contact your administrator and request that the API throttling limit be increased to allow the client to perform more requests.  |
| 500           | Internal Server Error | Report this error to BlackBerry AtHoc customer support at athocsupport@blackberry.com.  |
| 503           | Service Unavailable   | The server is currently unable to handle the request due to a temporary overload or scheduled maintenance. Wait and try again.  |

# Code samples

BlackBerry AtHoc has created a set of code written in C# that can be used as a template to call the APIs. This code handles authentication and allows you to use the .Net methods and functions instead of calling the REST endpoints directly.

Contact your implementation engineer or BlackBerry AtHoc Customer Support for the .zip file that contains these code files. You can also access code samples by clicking the **API Development Kit** link at [\[server-address\]/api/v2/docs/apiguide.html](#).



# Required roles for API access

The following table lists the operator roles that are required to access API calls. You must have at least one required role to access each API.

| API                 | Required role   |
|---------------------|---|
| GetOperatorAuditLog | <ul style="list-style-type: none"><li>• Alert Manager</li><li>• Advanced Alert Manager</li><li>• Enterprise Administrator</li><li>• Organization Administrator</li><li>• System Administrator</li></ul>   |
| GetAllDevices       | <ul style="list-style-type: none"><li>• Accountability Manager</li><li>• Accountability Officer</li><li>• Activity Log Manager</li><li>• Activity Log Viewer</li><li>• Alert Manager</li><li>• Advanced Alert Manager</li><li>• Alert Publisher</li><li>• Advanced Alert Publisher</li><li>• Collaboration Manager</li><li>• Connect Agreement Manager</li><li>• Draft Alert Creator</li><li>• End Users Manager</li><li>• Enterprise Administrator</li><li>• Organization Administrator</li><li>• Plan Incident Manager</li><li>• Plan Manager</li><li>• Report Manager</li><li>• SDK User</li><li>• System Administrator</li><li>• Basic Administrator</li><li>• Basic Operator</li></ul> |

| API           | Required role   |
|---------------|---|
| GetDevice     | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| GetOrgDevices | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |

| API               | Required role  |
|-------------------|--|
| GetOrgMassDevices | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul>                                      |
| GetOrganizations  | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Distribution List Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |

| API               | Required role  |
|-------------------|--|
| GetOrganization   | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Distribution List Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| SyncByCommonNames | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>  |
| GetUsers          | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>  |
| GetUserProfile    | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>  |

| API                | Required role  |
|--------------------|--|
| UserSearchBasic    | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>  |
| UserSearchAdvanced | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>  |
| AlertUsersTargeted | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| AlertDeviceCoverge | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |

| API                              | Required role   |
|----------------------------------|---|
| GetEvent                         | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Enterprise Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> </ul> |
| GetEventStatusSummary            | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Enterprise Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> </ul> |
| GetEventDetailsWithStatus        | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Enterprise Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> </ul> |
| GetUserEventStatusHistory        | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Enterprise Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> </ul> |
| UpdateUserStatus                 | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Enterprise Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> </ul> |
| GetAccountabilityTemplates       | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Enterprise Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> </ul> |
| GetAccountabilityTemplateDetails | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Enterprise Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> </ul> |
| PublishEvent                     | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Enterprise Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> </ul>                                   |

| API                            | Required role   |
|--------------------------------|---|
| GetEvents                      | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Enterprise Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> </ul>   |
| GetAccountabilityEventOfficers | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Enterprise Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> </ul>   |
| GetOrgAllApiClient             | <ul style="list-style-type: none"> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• System Administrator</li> </ul>  |
| GetApiClientDetails            | <ul style="list-style-type: none"> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• System Administrator</li> </ul>  |
| SaveApiClient                  | <ul style="list-style-type: none"> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• System Administrator</li> </ul>  |
| ResetApiClientSecret           | <ul style="list-style-type: none"> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• System Administrator</li> </ul>  |
| GetAttachmentDetails           | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Draft Alert Creator</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |

| API              | Required role   |
|------------------|---|
| GetAllAttributes | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| GetAttribute     | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |



| API                      | Required role   |
|--------------------------|---|
| UpdateAttribute          | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• System Administrator</li> </ul> |
| GetAttributeValues       | <ul style="list-style-type: none"> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>                                |
| GetAttributeValue        | <ul style="list-style-type: none"> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>                                |
| AddAttributeValues       | <ul style="list-style-type: none"> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>                                |
| UpdateAttributeValues    | <ul style="list-style-type: none"> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>                                |
| UpdateAttributeValue     | <ul style="list-style-type: none"> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>                                |
| DeleteAttributeValues    | <ul style="list-style-type: none"> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>                                |
| UpdateUserAttributeValue | <ul style="list-style-type: none"> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>                                |
| DeleteUserAttributeValue | <ul style="list-style-type: none"> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>                                |

| API                                    | Required role  |
|--|--|
| GetDeliveryTemplates                   | <ul style="list-style-type: none"> <li>• Advanced Alert Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• System Administrator</li> </ul>  |
| GetEmailDeliveryTemplatePreview        | <ul style="list-style-type: none"> <li>• Advanced Alert Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• System Administrator</li> </ul>  |
| GetDesktopPopupDeliveryTemplatePreview | <ul style="list-style-type: none"> <li>• Advanced Alert Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• System Administrator</li> </ul>  |
| GetDeliveryTemplateDetails             | <ul style="list-style-type: none"> <li>• Advanced Alert Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• System Administrator</li> </ul>  |
| PostEventLog                           | <ul style="list-style-type: none"> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• System Administrator</li> </ul>   |
| GetInboundAndExternalEvents            | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Connect Agreement Management</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |

| API                        | Required role   |
|----------------------------|---|
| GetInboundAndExternalEvent | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Connect Agreement Management</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul>  |
| GetAllLists                | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |

| API                | Required role   |
|--------------------|---|
| GetAllStaticLists  | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| GetAllDynamicLists | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |

| API                           | Required role   |
|-------------------------------|---|
| SyncStaticLists               | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>  |
| DeleteStaticLists             | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>  |
| GetStaticListRelations        | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| SetStaticListRelations        | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>  |
| PostStaticDistributionMembers | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Basic Administrator</li> </ul>  |

| API                          | Required role   |
|------------------------------|---|
| GetOperatorsPermission       | <ul style="list-style-type: none"> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• System Administrator</li> <li>• Basic Administrator</li> </ul>   |
| GetOperatorPermissionDetails | <ul style="list-style-type: none"> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• System Administrator</li> <li>• Basic Administrator</li> </ul>   |
| PublishAlert                 | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Draft Alert Creator</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| UpdateAlert                  | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Draft Alert Creator</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| GetAlertTemplates            | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Draft Alert Creator</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |

| API              | Required role   |
|------------------|---|
| GetAlertTemplate | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Draft Alert Creator</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul>   |
| GetAlertTypes    | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |

| API                | Required role   |
|--------------------|---|
| GetAlertSeverities | <ul style="list-style-type: none"> <li>• Accountability Manager</li> <li>• Accountability Officer</li> <li>• Activity Log Manager</li> <li>• Activity Log Viewer</li> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Collaboration Manager</li> <li>• Connect Agreement Manager</li> <li>• Draft Alert Creator</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• SDK User</li> <li>• System Administrator</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| GetAlerts          | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Draft Alert Creator</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul>   |



| API                            | Required role   |
|--------------------------------|---|
| GetAlertDetails                | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Alert Publisher</li> <li>• Advanced Alert Publisher</li> <li>• Draft Alert Creator</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| GetAlertFolders                | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Advanced Alert Publisher</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Plan Incident Manager</li> <li>• Plan Manager</li> <li>• System Administrator</li> </ul>  |
| GetAlertSummaryReport          | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Advanced Alert Publisher</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul>   |
| GetAlertHierarchySummaryReport | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Advanced Alert Publisher</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul>   |

| API                                   | Required role   |
|---------------------------------------|---|
| GetAlertDeviceSummaryReport           | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Advanced Alert Publisher</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| GetAlertDistributionListSummaryReport | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Advanced Alert Publisher</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| GetAlertResponseDetail                | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Advanced Alert Publisher</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| GetAlertDetailsByUser                 | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Advanced Alert Publisher</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |

| API                           | Required role   |
|-------------------------------|---|
| GetAlertDetailsByUsersDevices | <ul style="list-style-type: none"> <li>• Alert Manager</li> <li>• Advanced Alert Manager</li> <li>• Advanced Alert Publisher</li> <li>• End Users Manager</li> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• Report Manager</li> <li>• Basic Administrator</li> <li>• Basic Operator</li> </ul> |
| GetRolesController            | <ul style="list-style-type: none"> <li>• Enterprise Administrator</li> <li>• Organization Administrator</li> <li>• System Administrator</li> <li>• Basic Administrator</li> </ul>   |

# MTLS service error codes

The BlackBerry AtHoc MTLS service returns error codes in the form of a JSON file in the following format:

```
{
  "errors" : [
    {
      "code" : "<error-code-1>",
      "field" : "<field-name>",
      "message" : "<error-message>"
    },
    {
      "code" : "<error-code-2>",
      "field" : "<field-name>",
      "message" : "<error-message>"
    }
  ]
}
```

| Error code | Handler                   | Error message  |
|------------|---------------------------|--|
| HTTP 403   | IIS                       | The user certificate is invalid or unable to contact the Certificate Authority (CA.)                             |
| HTTP 401   | IIS                       | The user certificate is expired or blacklisted.  |
| HTTP 500   | IIS                       | Other (internal server error.)   |
| 1020       | Mobile MTLS Token Service | The request contains an invalid RedirectUri. The parameter exists in the query string and is not an empty value. |
| 1030       | Mobile MTLS Token Service | The request contains an invalid organization code.   |
| 2010       | Mobile MTLS Token Service | MTLS authentication is not configured for the organization (based on the organization code and Client ID.        |
| 2020       | Mobile MTLS Token Service | The primary regex (CAC/PIV) is not defined for the organization.   |
| 2030       | Mobile MTLS Token Service | The mapping ID cannot be extracted from the certificate. The regex is invalid or the mapping ID is empty.        |

| Error code | Handler                   | Error message  |
|------------|---------------------------|--|
| 3010       | Mobile MTLS Token Service | The user could not be found in BlackBerry AtHoc. The mapping ID is not set for the user. |
| 3020       | Mobile MTLS Token Service | The user is disabled or deleted in BlackBerry AtHoc.                                     |

# BlackBerry AtHoc Customer Support Portal

BlackBerry AtHoc customers can obtain more information about BlackBerry AtHoc products or get answers to questions about their BlackBerry AtHoc systems through the Customer Support Portal:

<https://www.blackberry.com/us/en/support/enterpriseapps/athoc>

The BlackBerry AtHoc Customer Support Portal also provides support via computer-based training, operator checklists, best practice resources, reference manuals, and user guides.

# Documentation feedback

The BlackBerry AtHoc documentation team strives to provide accurate, useful, and up-to-date technical documentation. If you have any feedback or comments about BlackBerry AtHoc documentation, email [athocdocfeedback@blackberry.com](mailto:athocdocfeedback@blackberry.com). Please include the name and version number of the document in your email.

To view additional BlackBerry AtHoc documentation, visit <https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc>. To view the BlackBerry AtHoc Quick Action Guides, see <https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc/Quick-action-guides/latest>.

For more information about BlackBerry AtHoc products or if you need answers to questions about your BlackBerry AtHoc system, visit the Customer Support Portal at <https://www.blackberry.com/us/en/support/enterpriseapps/athoc>.

# Legal notice

©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 <http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp>.

BlackBerry Limited  
2200 University Avenue East  
Waterloo, Ontario  
Canada N2K 0A7

BlackBerry UK Limited  
Ground Floor, The Pearce Building, West Street,  
Maidenhead, Berkshire SL6 1RL  
United Kingdom

Published in Canada