OAuth API authorization

OAuth is an authorization protocol that secures API endpoints as part of machine-to-machine communication between API clients. Unlike SAML, which focuses on authentication of web clients, OAuth focuses on what actors have access to, not who the actor is. The OAuth 2.0 specification includes four actors: The Resource Owner (the user), the Client (an application or script that needs access to the Address Manager API), the Authorization Server (OAuth2 Server, Open ID Connect), and the Resource Server (Address Manager API). The authorization server issues access tokens (used to authenticate a request to an API endpoint) to the client and an authorization grant defines how the client obtains the access token. For more information on authorization grants, refer to https://tools.ietf.org/html/rfc6749.

How OAuth works with Address Manager

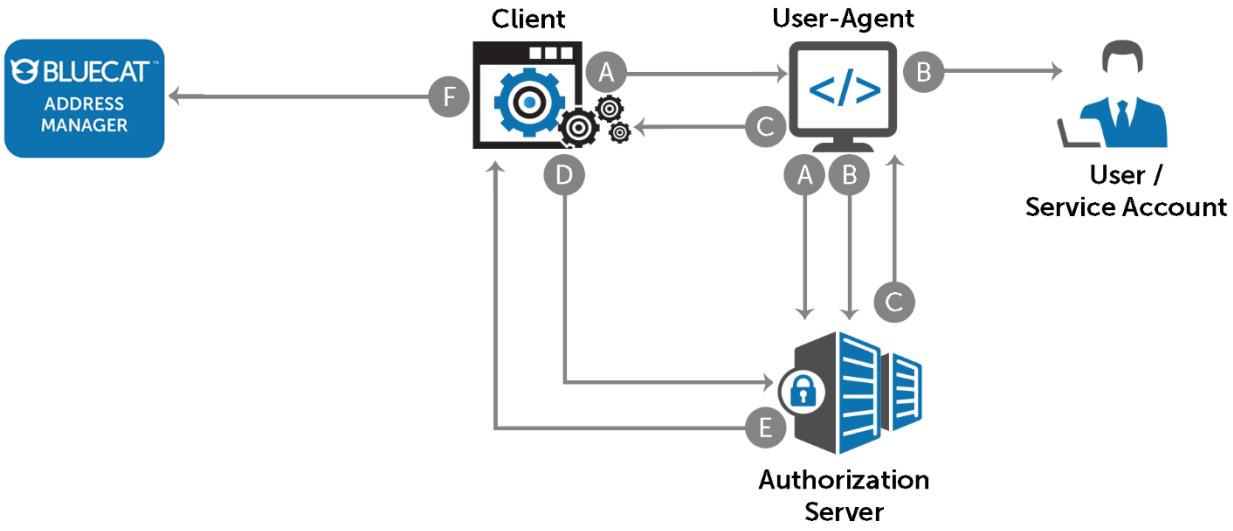
Address Manager allows the following authorization grants:

- Authorization Code Grant
- Implicit Grant
- Resource Owner Password Credentials Grant

Authorization Code Grant

In this authorization grant, the user is authenticated through a login page (the user-agent) hosted by the authorization server.

The following diagram explains the Authorization Code grant:



A. Client redirects user-agent to authorization server

B. Authorization server authenticates the user through the user-agent

C. If authentication of the user is successful and the user grants access to the requested resource, the authorization server returns an authorization code and redirects the user to the client

D. Client requests an access token from the authorization server by including authorization code

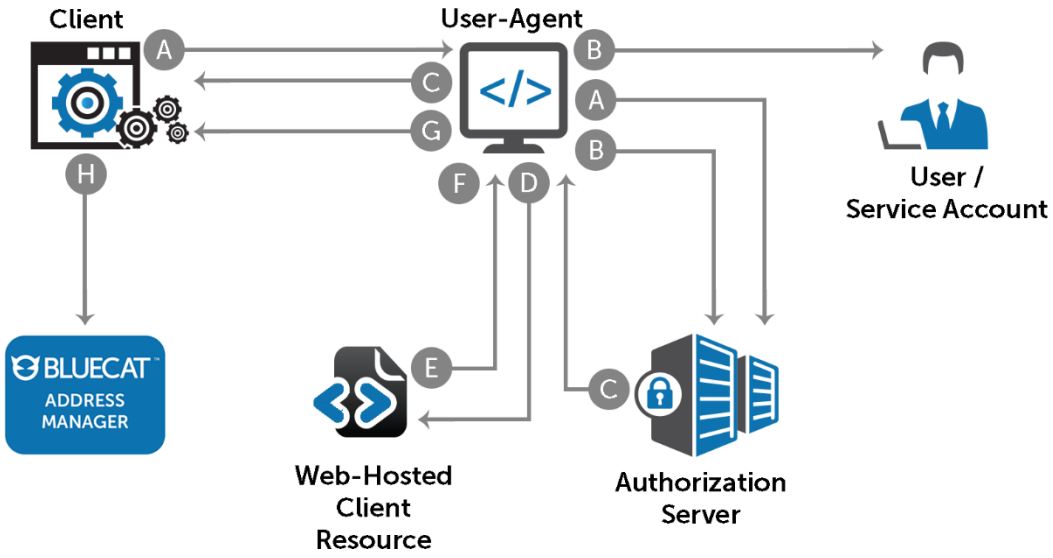
E. Authorization server authenticates client

F. Client uses access token to access the resource on the resource server

Implicit Grant

Similar to the Authorization Code grant, the user is authenticated through a login page (the user-agent) hosted by the authorization server, but instead of an authorization code, the access token is directly returned to the client.

The following diagram explains the Implicit grant:



A. Client redirects user-agent to authorization server

B. Authorization server authenticates the user through the user-agent

C. If authentication of the user is successful and the user grants access to the requested resource, the authorization server returns an access token in fragments and redirects the user to the client

D. User-agent makes a request to web-hosted client resource without the fragments

E. Web-hosted client returns a script to user-agent that can extract access token

F. User-agent executes script to extract access token

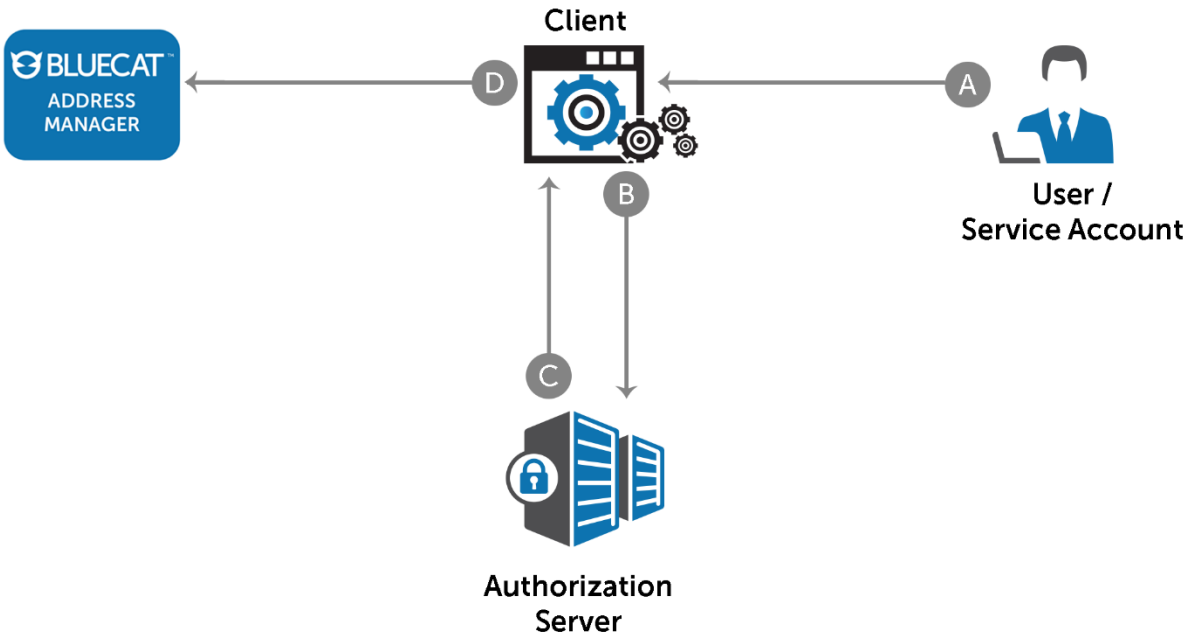
G. User-agent passes access token to the client

H. Client uses access token to access the resource on the resource server

Resource Owner Password Credentials Grant

In this authorization grant, the client requires credentials from the user—this grant does not involve a login page hosted by the authorization server.

The following diagram explains the Resource Owner Password Credentials grant:



A. User enters username and password in client application

B. Client forwards credentials to authorization server

C. Authorization server returns access token to client application

D. Client application calls Address Manager with access token

Enabling OAuth in Address Manager

Enabling OAuth secures the Address Manager API with access tokens issued by the authorization server. An access token represents the authorization of an API client to access the Address Manager API. Once you enable OAuth in Address Manager, you must also enable OAuth on the API client. For example, if you are using BlueCat Gateway, you must update its workflows and endpoints to use OAuth for access to the Address Manager API. Automated scripts must also be updated to use OAuth.

Prerequisites

Before you enable OAuth in Address Manager, you must perform the following:

- Ensure Address Manager can access the authorization server either on premises or cloud
- Register Address Manager as a resource server in the authorization server
- Register Address Manager as a client in the authorization server (OneLogin only)

What Address Manager needs from your Authorization Server

To enable OAuth authorization, obtain the following information from your authorization server:

- user claim name
- group claim name
- email claim name
- client ID
- client secret
- introspection endpoint

OR

- An XML file or URL to obtain the signing certificate. For more information, refer to Downloading the metadata XML file from ADFS.

Once you have completed the tasks in the prerequisites and obtained the required information from the authorization server, you can enable OAuth by configuring the authorization server in Address Manager.

Configuring the Authorization Server

Address Manager's API endpoints support the OAuth authorization protocol. This means an Address Manager API client can obtain an access token from the authorization server. The authorization server authenticates the resource owner (the user) and issues the access token for access to the resource server's protected resources (Address Manager API). To allow the issuance of access tokens by the authorization server to API clients of Address Manager, configure the authorization server in Address Manager.

> **Note:** Before performing the following steps, ensure that Address Manager is configured as the resource server with the authorization server.

1. In Address Manager, select the **Administration** tab.
2. Under **User Management**, select **Identity and Access Management**.
3. Select the **OAuth AS Configuration** tab.
4. Complete the **Authorization Server** section:
    a. **Name** (required): The name of the authorization server.
    b. **Description** (optional): A brief description of the authorization server.
    c. **OAuth** (required): Enables or disables OAuth. The default value is **Enable**.
5. In the **Signing Certificate** section, you can either upload the metadata file (XML file) by clicking **Choose File** in the **File** field or entering the metadata URL provided by the authorization server in the **URL** field. If you enter the metadata URL, you are directed to a trust page. On the trust page, click **Yes** to confirm the authorization server certificate.
6. Complete the **Token Validation** section:

a. **User Claim Name** (required): The user claim name of the authorization server

b. **Group Claim Name** (required): The group claim name of the authorization server.

c. **Email Claim Name** (required): The email claim name of the authorization server.

d. **Method** (required): Select **Local** if the token validation occurs in Address Manager. Select **Authorization Server** if the token validation occurs in the authorization server.

7. If you selected **Local** in the **Method** drop-down, complete the following fields:

    a. **Issuer** (required): The name of the token issuer – the IdP adds this to the token URL.

    b. **Audience** (required): The name of the BAM API string obtained from the authorization server.

8. If you selected **Authorization Server** in the **Method** drop-down, complete the following fields:

> **Note:** Once you register Address Manager as a resource server, you can obtain the information required for the fields below.

    a. **Client ID**: The public identifier of the application.

    b. **Client Secret**: The secret code known only to the application and the authorization server.

    c. **Introspection Endpoint**: Allows Address Manager to check the validity of access tokens.

> **Note:** Address Manager sends the client ID and the client secret to the introspection endpoint.

    d. **Authorization**: If you select **Basic**, Address Manager sends the Client ID and Client Secret as part of the header in the request. If you select **Post**, Address Manager sends the Client ID and Client Secret as part of the body in the request.

    e. **UserInfo Endpoint**: The information about the user—this includes the group membership information and user ID.

9. Click **Upload**.

The authorization server metadata populates in the **Signing Certificate** section.

10. Click **Update**.

> **Note:** Address Manager initiates a secure connection with both the introspection endpoint and userinfo endpoint. If the server is not CA-signed, a confirmation page about trusting the server may display.