Client API Service Adoption using OAuth 2.0 Protocol

OAuth is an open protocol that supports secure authorization in a simple, standard method and decouples authentication from authorization.

Customers who choose to adopt the OAuth protocol for authorization to access CME Group APIs can follow the adoption path outlined below.

API Service Adoption Steps:

Step 1

In CME Customer Center, create an OAuth API ID or Convert a Basic Auth API ID to an OAuth API ID.

Create an OAuth ID in CME Customer Center

1. If necessary, create a CME Group Login.
2. Log into CME Customer Center.
3. Follow the steps to Create an API ID.
    a. For the "Type," select **OAuth**.

> OAuth API IDs are case-sensitive.

Convert a Basic Auth ID to an OAuth ID in CME Customer Center

1. Log into CME Customer Center.
2. Follow the steps in API ID Management to convert the authentication type.
    a. Change the "Type" to **OAuth**.

> CME Group API IDs can only be used for OAuth or Basic Auth services. Once an API ID is converted to OAuth, it cannot be used to access Basic Auth services. OAuth API IDs are case-sensitive.

Step 2

Retrieve a Token

> Clients can use any API tool of their choice to create and retrieve a token.

Create a Post

Create a Post to retrieve an authentication token from the following URLs

Detail	New Release	Production
OAuth Token Endpoint	https://authnr.cmegroup.com/as/token.oauth2	https://auth.cmegroup.com/as/token.oauth2

The CME Group token retrieval uses the Client Credentials grant type to request an access token to access a client's own resources. Other grant types are not supported.

HTTPS Header

For customers using authorization header, the Base64 Encoding is required where secret is the “API ID:Password” (Base64 endcoded), as generated in Customer Center.

- client_id=CME Group OAuth API ID
- client_secret=<secret>

> For customers using url parameters Base 64 encoding is not required

Access Token Request Parameters

- **grant_type (required)**

  The grant_type parameter must be set to client_credentials.

- **Client Authorization (required)**

  Clients must send their CME Group OAuth API ID and password in the POST request, in client_id and client_secret fields respectively:

  client_id=CME Group OAuth API ID

  client_secret=<secret>

Example

The following is an example authorization code request.

```
POST /as/token.oauth2 HTTP/1.1
Host: auth.cmegroup.com
Content-Type: application/x-www-form-urlencoded
Authorization:Basic
YkVEMGJMaEFhb0pDamplbmFPVjNwMDZSeE9Eb2pyOUNFUzN1dldXcXUyeE9RYk9GeUE6WEZ0bmJIbXR3dXEwNVI1Yk91WmVOWHlqcW9RelNS
c21zUU5qelFOZUFZUlRIbmhHRGw=
grant_type=client_credentials
```

Responses

Successful Response

If the request for an access token is valid, the authorization server will generate an access token and send back to the client.

The response with an access token will contain the following properties:

- access_token - The access token string to use on requests to the RESTful API service.
- token_type - Defines the type of token, typically just the string “bearer”.
- expires_in - Defines the duration of time until the access token expires and a new token must be obtained.

The access token request will also include the additional Cache-Control: no-store and Pragma: no-cache HTTP headers to ensure clients do not cache this request.

For example, a successful token response may look like the following:

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache

{
  "access_token":"MTQ0NjJkZmQ5OTM2NDE1ZTZjNGZmZjI3",

  "token_type":"bearer",

  "expires_in":1799,

  }
```

Unsuccessful Response

If the access token request is invalid, such as the oAuth token endpoint UR Ididn't match the one used during authorization, then the server will return an error response.

Error responses are returned with an HTTP 400 or 401 status code, with error and error_description parameters. The error parameter will always be one of the values listed below.

- HTTP 400 errors
- invalid_request– The request is missing a parameter so the server can't proceed with the request. This may also be returned if the request includes an unsupported parameter or repeats a parameter.
- invalid_grant– The authorization code (or user's password for the password grant type) is invalid or expired, or the oAuth token endpoint URI given in the authorization grant does not match the oAuth token endpoint URI provided in this access token request.
- unauthorized_client– This client is not authorized to use the requested grant type.
- unsupported_grant_type– Sent if a grant type is requested that the authorization server doesn't recognize. Unknown grant types also use this specific error code rather than using the invalid_request
- HTTP 401 error
    - invalid_client – Client authentication failed, such as if the request contains an invalid client ID or secret.

CME Group supports two optional parameters when returning an error response, error_description and error_uri. These provide more information about the error.

The error_description parameter describes the circumstance of the error. The error_uri provides a link to the API documentation for information about how to correct the specific error that was encountered.

The entire error response is returned as a JSON string, similar to the successful response. Below are examples of a error responses.

HTTP 400 Error

```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
  "unsupported_grant_type"
}
```

HTTP 401 Error

```
HTTP/1.1 401 Unauthorized
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
  "error_description": "Invalid client or client credentials.",
    "error": "invalid_client"
}
```