FXCM Global Services, LLC

FXCM RestAPI 3rd Party OAUTH

User Guide

**Date: 11/02/2020**

**Author: Matthew Schwartz**

**Revised by:**

**Revision: 1**

Contents

[1 Introduction 2](#_Toc39165189)

[2 Grant Type: auth\_code 3](#_Toc39165190)

[3 Grant Type: implicit 4](#_Toc39165203)

[4 FXCM Sample Application 5](#_Toc39165211)

[5 Revision History 6](#_Toc39165222)

# Introduction

The purpose of this document is to describe the functionality and workflow of FXCM’s 3rd Party OAUTH authentication.

FXCM’s RESTAPI requires an access\_token to be passed in order to authenticate an end user and establish a trading session. Prior to the OAUTH authentication solution, an end user would have to log in to FXCM’s Trading Station Web platform with their username and password and subsequently generate an access token. This model is sufficient for the end user who will be integrating with the API directly.

When 3rd parties build applications to be consumed by the end user and utilize the RestAPI, the end user must supply the application with their access token. This process is cumbersome to the end user, as they must access two applications.

The 3rd party OAUTH authentication model solves this problem by allowing the 3rd party application to direct the end user to FXCM’s authentication page. Upon successful authentication, FXCM will redirect back to the 3rd party application and provide the token. This model follows standard OAUTH2 protocol and requires each 3rd party to register their callback URL with FXCM and get issued a client\_id and client\_secret.

This document outlines the steps a 3rd party should take in order to integrate with the OAUTH authentication model, as well as provide instructions to access and run sample a sample front end application.

# Grant Type: authorization\_code

The *authorization\_code* grant type allows for the token exchange to occur in the back channel and is completely hidden to the end user.

**OAUTH 2.0 RFC:** <https://tools.ietf.org/html/rfc6749>

## 3rd Party application must launch FXCM’s login page

### https://{fxcm\_domain}/oauth/authenticate?client\_id={client\_id}&response\_type=token&redirect\_uri={redirect\_uri}

#### fxcm\_domain is environment specific

##### Production:

###### General: tradingstation.fxcm.com

###### China: tradingstation.fuhuisupport.com

###### Indonesia: tradingstation.trade-fxcm.com

###### \*Demo and Real can be chosen on the page by the end user

##### UAT: titanx.fxcorporate.com

###### End user must choose Real

#### client\_id: string value provided by FXCM and must match exactly

#### response\_type: always ‘code’

#### redirect\_uri: must be agreed between FXCM and 3rd party and must match exactly

##### Multiple redirect\_uri are available upon request

## The end user must enter their FXCM login credentials

## The user will be prompted to and must subsequently approve the request

## FXCM Auth Server will redirect back to {redirect\_uri} with the query parameter: code

## 3rd party application will receive response with header.location: {redirect\_uri}?code={code}

## 3rd party application must submit a POST as follows:

### https://{fxcm\_domain}/oauth/token

#### fxcm\_domain must match from step 2.1

### POST BODY must contain:

#### code: value from ‘code’ query parameter in step 2.5

#### grant\_type: ‘authorization\_code’

### POST AUTHORIZATION HEADER must contain:

#### base64 encoded client\_id:client\_secret

##### client\_id: string value provided by FXCM

##### client\_secret: string value provided by FXCM

## Client receives JSON response: {access\_token: *access\_token,* token\_type: ‘Bearer’, conn: *env*}

### access\_token: the API access token to be used to create a RESTAPI session

### conn: the environment, demo or real, to identify which RESTAPI environment URL to target

# Grant Type: authorization\_code (PKCE)

This grant type allows the token exchange to occur in the front channel (single-page apps).

**PKCE RFC:** <https://tools.ietf.org/html/rfc7636>

3rd Party application must launch FXCM’s login page

### <https://{fxcm_domain}/oauth/authenticate?client_id={client_id}&response_type=code&redirect_uri={redirect_uri}>&code\_challenge={code\_challenge}&code\_challenge\_method=S256

#### fxcm\_domain is environment specific

##### Production: tradingstation.fxcm.com

###### Demo and Real can be chose on the page by the end user)

##### UAT: titanx.fxcorporate.com

###### End user must choose Real

#### client\_id: string value provided by FXCM and must match exactly

#### response\_type: always ‘code’

#### redirect\_uri: must be agreed between FXCM and 3rd party and must match exactly

##### Multiple redirect\_uri are available upon request

#### code\_challenge: base64 url encoded, SHA256 hash of **code\_verifier**

3.7.1.6 code\_challenge\_method: **S256**

## The end user must enter their FXCM login credentials

## The user will be prompted to and must subsequently approve the request

## FXCM Auth Server will redirect back to {redirect\_uri} with the query parameter: code

## 3rd party application must submit a POST as follows:

### https://{fxcm\_domain}/oauth/token

#### fxcm\_domain must match from step 2.1

### POST BODY must contain:

#### code: value from ‘code’ query parameter in step 2.5

#### grant\_type: ‘authorization\_code’

3.11.2.3 code\_verifier: randomized string used to generate code\_challenge

## Client receives JSON response: {access\_token: *access\_token,* token\_type: ‘Bearer’, conn: *env*}

### access\_token: the API access token to be used to create a RESTAPI session

### conn: the environment, demo or real, to identify which RESTAPI environment URL to target

# FXCM Sample Application

## Visit FXCM’s Github page

### <https://github.com/FXCM/3rd-party-oauth>

## Clone the master branch of the project:

### Note the client\_id, client\_secret, and redirect\_urls in the sample are not configured in the test environment. Please reach out to FXCM customer support to request Demo and Real environment access.

## Navigate to the cloned repository and run the command: ‘npm install’

## Run the command: ‘node server’

### Note that node version should be at least v10.16.0

## Visit localhost:[port] on a browser

### Port is set in config.json

## The browser page will display options to verify authorization\_code and authorization\_code (PKCE) grant type workflows

### Run the browser network tab to view inbound and outbound network requests.

### Log in to FXCM using credentials:

#### Connection: REAL

#### Username: oauth\_user

#### Password: fxcm1234

# Revision History

| Version | Date Revised | Revised By | Description |
| --- | --- | --- | --- |
| 1.0 | 05/01/2020 | Matthew Schwartz | Document Creation |
| 1.1 | 11/2/2020 | Matthew Schwartz | Added alternate production URLs  Added support for ‘conn’ parameter in JSON response |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |