Vendor OAuth2.0 Documentation

Version History

Date	Version
Friday, February 26, 2021	1.0
Tuesday, March 2, 2021	1.1
Friday, April 29, 2022	1.2
Thursday, September 1, 2022	1.3

This document describes authentication mechanics within the Kigo API platforms. The applicable parties are "Kigo", the "Vendor", and our shared customer, the property management company (PM). The systems involved are Kigo Authorization API (id.kigo.net), Kigo Pro APIs (kigoapis.com), and the Vendor application(s).

Setup/Account Linking

Before Vendor applications can retrieve PM data from Kigo Pro APIs, the PM must opt-in to the Vendor's product or service. This triggers a process which informs the Vendor application of the PM's intent to allow Kigo to share PM data and provides a mechanism for authentication.

- The moment a Kigo Property Manager (PM) opts-in to a vendor's services, their browser window will be redirected to a URL in the vendor's domain:

```
Example: https://www.testvendordomain.com/signin-oidc?
code=CB6627A2285B77A2C723190B88DE07347A2378BB889FAA3F3256EB5D6BD79E86&scope=pro.property
%_3Aget%20offline_access
```

- To connect the Vendor application with Kigo, the following steps must be executed:

    1. Authenticate the PM User within the Vendor application. The user must log in (or sign up) within the Vendor application, so that the following OAuth 2.0 Refresh Token can be associated with the correct PM Account within the Vendor application.

2. After the PM is authenticated against the Vendor application, a refresh token must be associated with the account within the Vendor application. The Kigo Authorization API must be called to exchange the **code and scope** provided in the above query string for a Refresh Token. This call is a grant type of *authorization_code* and utilizes the Vendor credentials (*client_id*, *client_secret*) which are provided to the Vendor by Kigo during initial integration.

```
POST /connect/token HTTP/1.1
Host: id.kigo.net
Content-Type: application/x-www-form-urlencoded Content-
Length: 432

client_id=testvendor.clients.pro.kigo.net
&client_secret=test-49C1A7E1-0C79-4A89-A3D6-A37998FB86B0
&grant_type=authorization_code
&code=CB6627A2285B77A2C723190B88DE07347A2378BB889FAA3F3256EB5D6BD79E86
&redirect_uri=https://www.somevendor.com/signin-oidc
```

3. The resulting Refresh Token provided by this call must be stored within in the Vendor application and associated with the PM account. Notice that the response will also provide an initial "access_token". This is only a convenience. The most important part here is to capture and store the "refresh_token" since that will be used in the future to issue new "access_tokens" as needed by the Vendor Application:


```
{
    "access_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IkU5RDU3OEQxQ0E2MzI2MkQ4OEQ0OUZFODUwM0Q5NDM2QzcyM
Tc3RDZSUzI1NiIsInR5cCI6ImF0K2p3dCIsIng1dCI6IjZkVjQwY3BqSmkySTFKX29VRDJVTnNjaGQ5WSJ9.eyJuYmYiOjE2MT
Q2MTc2MTIsImV4cCI6MTYxNDYyMTIxMiwiaXNzIjoiaHR0cHM6Ly9raWdvLWlkZW50aXR5c2VydmVyLWRldi1ldXMuYXp1cmV3
ZWJzaXRlcy5uZXQiLCJhdWQiOlsicHJvLmFwaSIsImh0dHBzOi8va2lnby1pZGVudGl0eXNlcnZlci1kZXYtZXVzLmF6dXJld2
Vic2l0ZXMubmV0L3Jlc291cmNlcyJdLCJjbGllbnRfaWQiOiJ0ZXN0dmVuZG9yLmNsaWVudHMucHJvLmtpZ28ubmV0Iiwic3Vi
IjoicHJvLmFjY291bnRpZF82MzAiLCJhdXRoX3RpbWUiOjYzNzUwMjE0NDAzMDAwMDAwMCwiaWRwIjoibG9jYWwiLCJwcm8uYW
Njb3VudGlkIjoiNjMwIiwianRpIjoiMUEwMkQyNDIwRjNFODk0MjVFRkYyMzdERDMyMTc1NjIiLCJpYXQiOjE2MTQ2MTc2MTIs
InNjb3BlIjpbInByby5wcm9wZXJ0eTpnZXQiLCJvZmZsaW5lX2FjY2VzcyJdfQ.d-
ChHaXp_BDCoWkJ3jmLEIra5SqX6ENFddOrfnYILR7jvgg1Krx4Y17eSA6DVCJTZoIrP5E9kaIB1-7KA8LQWsNNn3-
BQb2M76VeY67w2dflQLuFdAAIMO6QIQYN5gi2DYaxi6eG0VvgsQ_x_IRO3FtQTMiXZC5zu1lmxKMw3iArxKgSGNryhrHtQ9MvQ
GhVKpifdRlE6nbRF5tDehuylaE5PvfIt7YlLk_
20UMZkEJR1gPufym3pNjL99yP0n_-7iTl1vlItTg7UQ2wPqC1hxX0DiMbfAwsxSxfPshGOOr1WJICPB9EeD1S4sYqtTOWDfwa5
6zK6lsKYKfeTS15w",
    "expires_in": 3600,
    "token_type": "Bearer",
    "refresh_token": "38B7CEFEF7C59BC37B381E67F96C3DC99285BCF5ACD29DA188A25A14C5BC6A3F",
    "scope": "pro.property:get offline_access"
}
```


Accessing PM Data

Before accessing PM data within the Kigo Pro APIs the stored Refresh Token must be exchanged for a short-lived Access Token. On demand, the Vendor application will call the Kigo Authorization API to obtain this Access Token and utilize it for all subsequent requests to the Kigo Pro API during the active session.

1. Call the Kigo Authorization API using a grant_type of *refresh_token* and provide your *client_id*, and *client_secret*.

```
POST /connect/token HTTP/1.1
Host: id.kigo.net
Content-Type: application/x-www-form-urlencoded
Content-Length: 201

client_id=testvendor.clients.pro.kigo.net
&client_secret=test-49C1A7E1-0C79-4A89-A3D6-A37998FB86B0
&grant_type=refresh_token
&refresh_token=38B7CEFEF7C59BC37B381E67F96C3DC99285BCF5ACD29DA188A25A14C5BC6A3F
```

2. The response body will contain an *access_token* which should be stored for use in the current session:


```
{
    "access_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjVEQkM0RDdDMEQwODRERDZFRTU3NTM5QjY0Nzh
GOTE1QjM2NTk4NTdSUzI1NiIsInR5cCI6ImF0K2p3dCIsIng1dCI6IlhieE5mQTBJVGRidVYxT2JaSGo1RmJObG1
GYyJ9.eyJuYmYiOjE2NTEyMjg0MzUsImV4cCI6MTY1MTIzMjAzNSwiaXNzIjoiaHR0cHM6Ly9pZC5raWdvLm5ldC
IsImF1ZCI6WyJwcm8uYXBpIiwiaHR0cHM6Ly9pZC5raWdvLm5ldC9yZXNvdXJjZXMiXSwiY2xpZW50X2lkIjoidG
VzdHZlbmRvci5jbGllbnRzLnByby5raWdvLm5ldCIsInN1YiI6InByby5hY2NvdW50aWRfOTM3IiwiYXV0aF90aW
1lIjo2Mzc4NjgyNTA3ODAwMDAwMDAsImlkcCI6ImxvY2FsIiwicHJvLmFjY291bnRpZCI6IjkzNyIsImp0aSI6Ij
lGQzlFQzBBQzc4N0IyRTFGRDE1NkEyM0Y4MEY5NTQ1IiwiaWF0IjoxNjUxMjI4NDA1LCJzY29wZSI6WyJwcm8ucH
JvcGVydHk6Z2V0Iiwib2ZmbGluZV9hY2Nlc3MiXX0.pP2_fw7X_f5B2DVXEvSq2YKuAdYAqaIWU_7_sOicX2GupG
ce6QdId5hEoXmHs647ZQhhnGQghiVKMgJJws7IWdxk83TFd-
4k14pzac76Kg0FTgvCprh3Z7Rgni_SER1JJEypvv-1KASZ1TwoWR-
t4qbdRtyDAQKkiWO7mRenoNfukfhRfarOQJIItCLM_NCHwWG2_bDIgO56bhX9ELhNj4CYc5y5qpuBWtTqYY5v2kx
RmWDLpKsbLd-_oJQEilLxCZv_nIOF6GrrB-
kruqLF6J08Ji3uXpJDVfVF95MU30xEoSNniNEgPMTitTUqGBAj63ouFfjxfb0ecyk2hO8IYQ",
    "expires_in": 3600,
    "token_type": "Bearer",
    "refresh_token": "EB261E346DBE084A536412F960730FF3D19A51ADC91A5F4A70F336FE351E3637",
    "scope": "pro.property:get offline_access"
}
```


3. When calling Kigo Pro API endpoints, this Access Token must be included in the header of all requests: **Authentication: Bearer {access_token}**)

Expiration times

ITEM	EXPIRATION
Code grant	15 minutes
Access token	1 hour
Refresh token	It expires if it is not used for 60 consecutive days in a row