# Microsoft Graph Authenticate a Connector

Last Modified on 03/19/2020 7:06 pm EDT

You can authenticate with Microsoft to create your own instance of the Microsoft Graph connector through the UI or through APIs. Once authenticated, you can use the connector instance to access the different functionality offered by the Microsoft platform.

## Authenticate Through the UI

Use the UI to authenticate with Microsoft and create a connector instance. Because you authenticate with Microsoft via OAuth 2.0, all you need to do is add a name for the instance. In OAuth Scope, leave the default scopes unless you extended the connector. If so, add the required scopes for any resources that you add. After you create the instance, you'll log in to Microsoft to authorize SAP Cloud Platform Open Connectors access to your account. For more information about authenticating a connector instance, see Authenticate a Connector Instance (UI).

After successfully authenticating, we give you several options for next steps. Make requests using the API docs associated with the instance, map the instance to a common resource, or use it in a formula template.

## Authenticate Through API

Authenticating through API is similar to authenticating via the UI. Instead of clicking and typing through a series of buttons, text boxes, and menus, you will instead send a request to our /instances endpoint. The end result is the same, though: an authenticated connector instance with a **token** and **id**.

Authenticating through API follows a multi-step OAuth 2.0 process that involves:





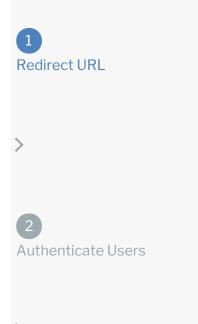


>

3 Authenticate Instance

- Getting a redirect URL. This URL sends users to the vendor to log in to their account.
- Authenticating users and receiving the authorization grant code. After the user logs in, the vendor makes a call back to the specified url with an authorization grant code.
- Authenticating the connector instance. Using the authorization code from the vendor, authenticate with the vendor to create a connector instance at SAP Cloud Platform Open Connectors.

## Getting a Redirect URL





Use the following API call to request a redirect URL where the user can authenticate with the service provider. Replace {keyOrId} with the connector key, microsoftgraph.

curl -X GET /elements/{keyOrId}/oauth/url?apiKey=&apiSecret= &callbackUrl=

#### **Query Parameters**

Query Parameter	Description
apiKey	The API key or client ID obtained from registering your app with the provider. This is the <b>Application Id</b> that you recorded in API Provider Setup.
apiSecret	The client secret obtained from registering your app with the API provider. This is the <b>Password/PublicKey</b> that you recorded in API Provider Setup.
callbackUrl	The URL that the API provider returns a user to after they authorize access. This is the <b>Redirect URL</b> that you recorded in API Provider Setup.

#### **Example Request**

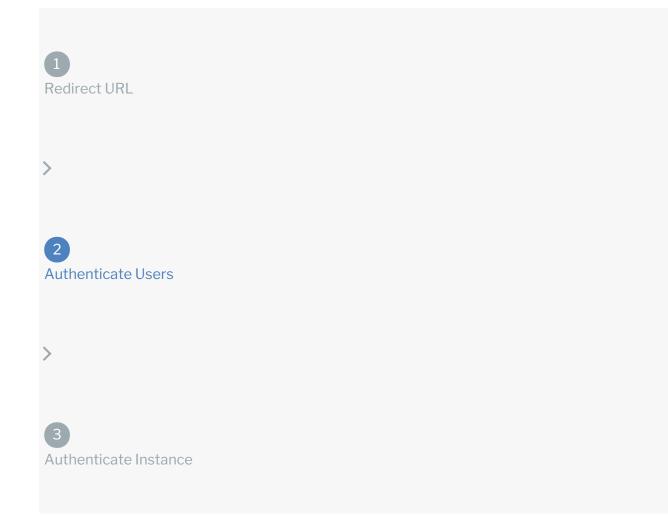
curl -X GET \
'https://api.openconnectors.us2.ext.hana.ondemand.com/elements/api-v2/eleme
nts/microsoftgraph/oauth/url?apiKey=RandOMAP1-key&apiSecret=fak3AP1-s3Cr3t&
callbackUrl=https:%3A%2F%2Fwww.mycoolapp.com%2auth' \

#### Example Response

Use the <code>oauthUrl</code> in the response to allow users to authenticate with the vendor.

{
 "oauthUrl": "https://login.microsoftonline.com/common/oauth2/v2.0/authorize
 ?scope=Calendars.Read+Calendars.ReadWrite+offline\_access&response\_type=code
 &redirect\_uri=https%3A%2F%2Fwww.mycoolapp.com%2auth&state=microsoftgraph&cl
 ient\_id=RandOMAP1-key",
 "element": "microsoftgraph"
}

## Authenticating Users and Receiving the Authorization Grant Code



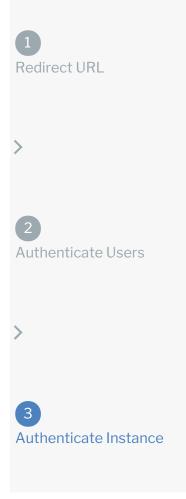
Provide the oauthUrl in the response from the previous step to the users. After users authenticate, Microsoft provides the following information in the response:

- code
- state

Response Parameter	Description
code	The authorization grant code returned from the API provider in an OAuth 2.0 authentication workflow. SAP Cloud Platform Open Connectors uses the code to retrieve the OAuth access and refresh tokens from the endpoint.
state	A customizable identifier, typically the connector key ( microsoftgraph ).

**()** Note: If the user denies authentication and/or authorization, there will be a query string parameter called error instead of the code parameter. In this case, your application can handle the error gracefully.

## Authenticating the Connector Instance



Use the <u>code</u> from the previous step and the <u>/instances</u> endpoint to authenticate with Microsoft and create a connector instance. If you are configuring events, see the <u>Events</u> section.

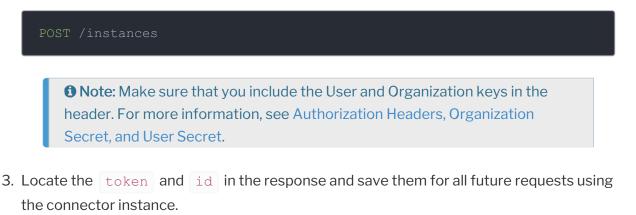
• Note: The endpoint returns a connector instance token and id upon successful completion. Retain the token and id for all subsequent requests involving this connector instance.

To authenticate a connector instance:

1. Construct a JSON body as shown below (see Parameters):



2. Call the following, including the JSON body you constructed in the previous step:



#### **Example Request**

```
curl -X POST \
    https://api.openconnectors.us2.ext.hana.ondemand.com/elements/api-v2/inst
ances \
    -H 'authorization: User , Organization ' \
    -H 'content-type: application/json' \
    -d '{
    "element": {
        "key": "microsoftgraph"
    },
    "providerData": {
        "code": "xxxxxxxxxxxxxxxxxx"
    },
    "configuration": {
        "oauth.api.key": "RandOMAP1-key",
        "oauth.callback.url": "https://mycoolapp.com",
        "oauth.scope": "Calendars.Read Calendars.ReadWrite offline_access"
    },
    "tags": [
        "Docs"
    ],
    "name": "API Instance"
}/
```

### **Authentication Parameters**

API parameters in the UI are **bold**, while parameters available in the instances API are in code formatting.

**1** Note: Event related parameters are described in Events.

Parameter	Description	Data Type
key	The connector key. microsoftgraph	string
code	The authorization grant code returned from the API provider in an OAuth 2.0 authentication workflow. SAP Cloud Platform Open Connectors uses the code to retrieve the OAuth access and refresh tokens from the endpoint.	string
Name name	The name of the connector instance created during authentication.	string

QAuth API Key Parameter oauth.api.key	The API key or client ID obtained from registering your app <b>Description</b> vider. This is the <b>Application Id</b> that you noted in API Provider Setup.	Data string Type
OAuth API Secret oauth.api.secret	The client secret obtained from registering your app with the API provider. This is the <b>Password/PublicKey</b> that you noted in API Provider Setup.	string
oauth.callback.url	The URL that the API provider returns a user to after they authorize access. This is the <b>Redirect URL</b> that you noted in API Provider Setup.	string
OAuth Scope	The permissions required to access resources set up on the connector.	string
Tags tags	<i>Optional.</i> User-defined tags to further identify the instance.	string

## **Example Response for an Authenticated Connector Instance**

In this example, the instance ID is 12345 and the instance token starts with "ABC/D...". The actual values returned to you will be unique: make sure you save them for future requests to this new instance.