Syncplicity Authenticate a Connector

Last Modified on 03/16/2020 10:10 pm EDT

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

Syncplicity offers two types of authentication: Oauth2 and custom.

Authenticate Through the UI

Authenticate Through the UI Using OAuth2

Because you authenticate with Syncplicity via OAuth 2.0, all you need to do is add a name for the instance, as well as your Syncplicity user email. After you create the instance, you'll log in to Syncplicity 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 the UI Using Custom Authentication

When authenticating with Syncplicity using custom authentication, you need to provide a name for the instance as well as the user email and app token noted in Syncplicity API Provider Setup. For more information about authenticating a connector instance, see Authenticate a Connector Instance (UI).

Authenticating Through the UI for Users in the EU

To avoid authentication errors, SAP Cloud Platform Open Connectors users in the EU must provide an API key and secret in order to authenticate a Syncplicity instance. To do so while authenticating through the UI, click **Show Optional Fields** and enter the values, which you

generated and recorded in Syncplicity API Provider Setup, into the **Syncplicity OAuth API Key** and **Syncplicity OAuth API Secret** fields.

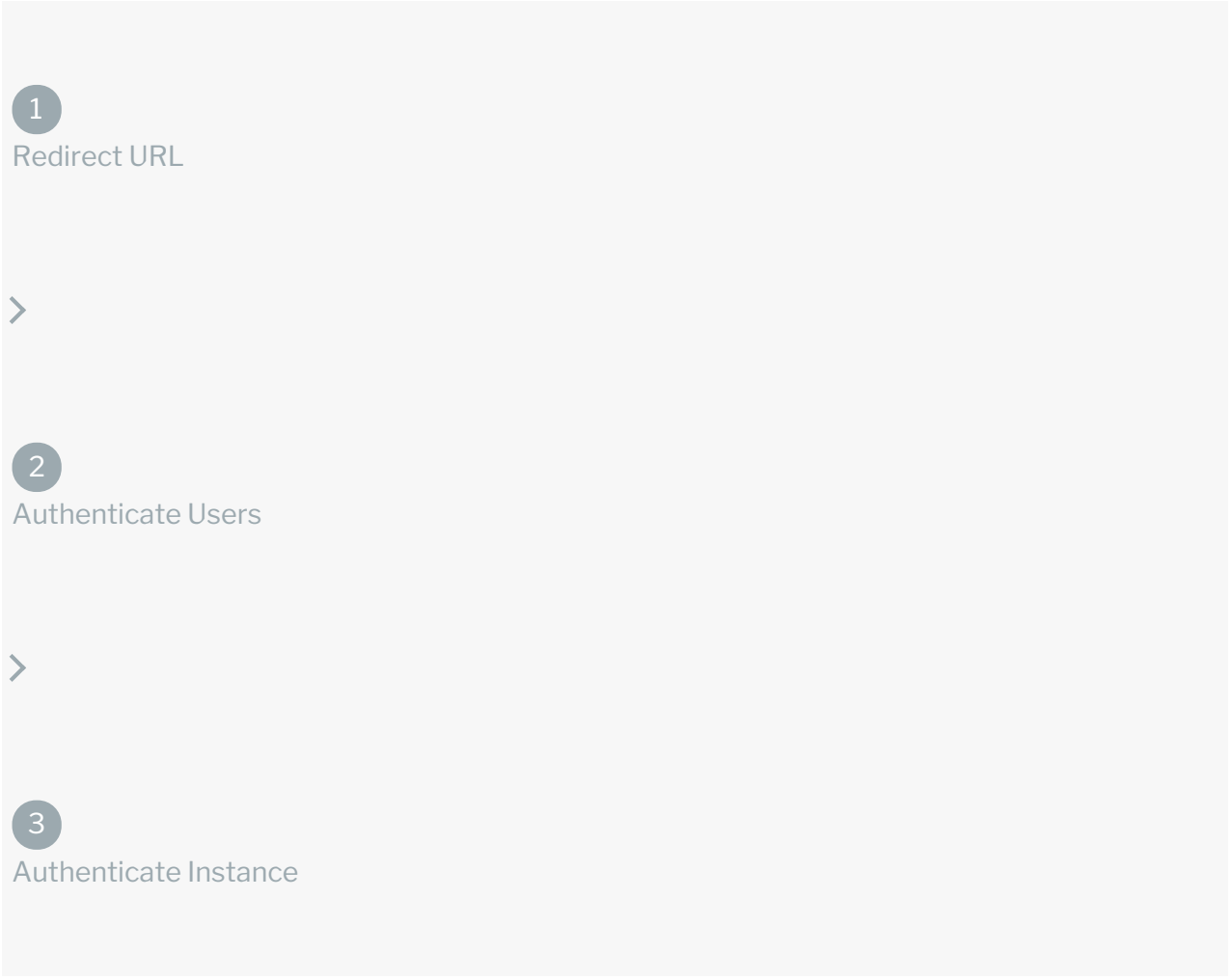
Authenticate Through API

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**.

You can authenticate using either OAuth 2.0 or custom authentication.

OAuth 2.0 Authentication through API

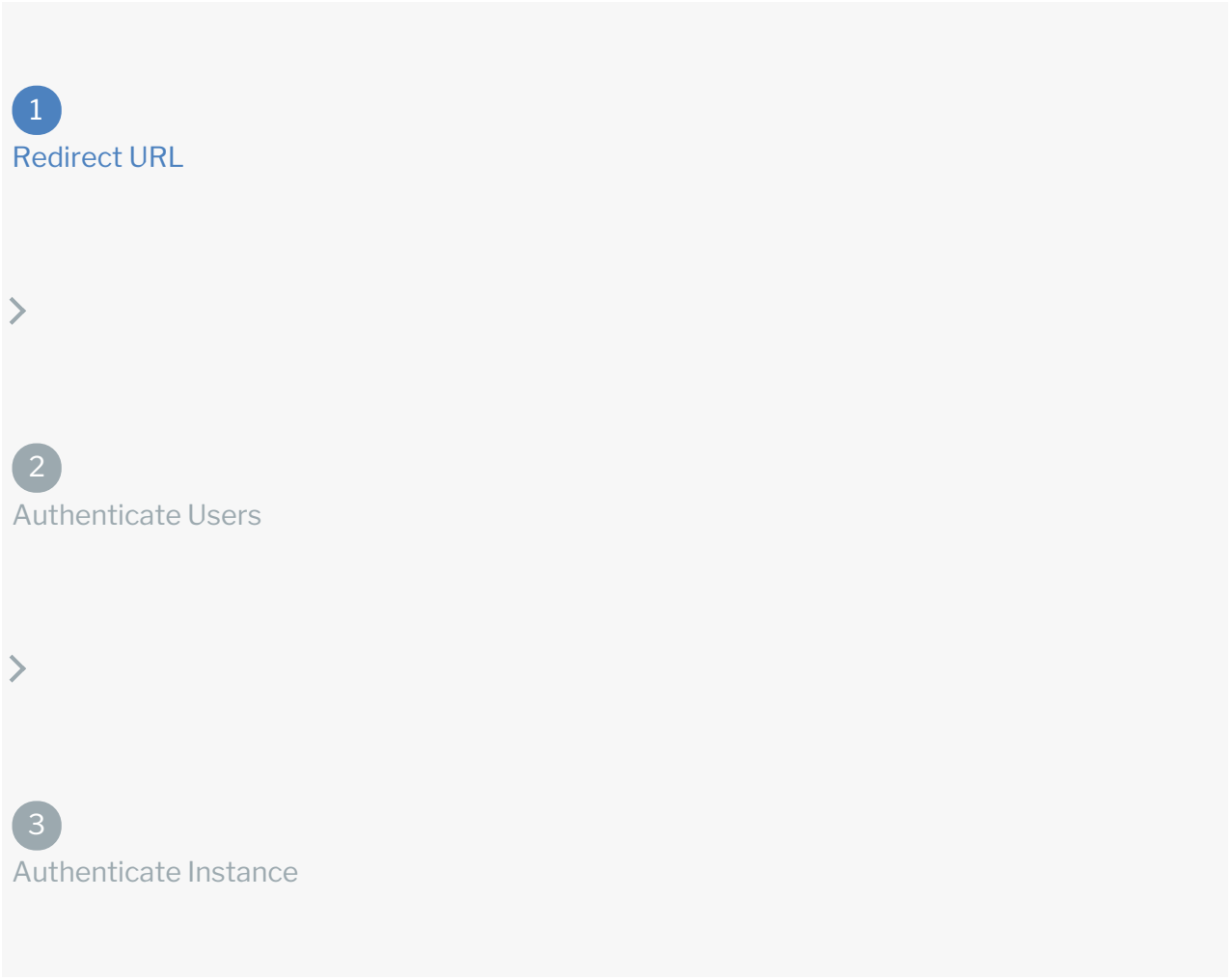
Using OAuth 2.0 to authenticate through API follows a multi-step process that involves:



- 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 callback 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 API provider. Replace `{keyOrId}` with the connector key, `syncplicity`.

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

Query Parameters

Query Parameter	Description
apiKey	The API key obtained from registering your app with the provider. This is the API key that you recorded in the API Provider Setup section.

Query Parameter	Description
apiSecret	The API secret obtained from registering your app with the API provider. This is the API secret that you recorded in the API Provider Setup section.
callbackUrl	The URL that the API provider returns a user to after they authorize access. This is `https://auth.cloudelements.io/oauth`, the redirect URL specified in the API Provider Setup section.

Example cURL

```
curl -X GET
-H 'Content-Type: application/json'
'https://api.openconnectors.us2.ext.hana.ondemand.com/elements/api-v2/elements/syncplicity/oauth/url?apiKey=&apiSecret=&callbackUrl='
```

Example Response

Use the `oauthUrl` in the response to allow users to authenticate with the vendor.

```
{
    "secret": "3BK0GSFI85TZRKBFK5SZG8Q43",
    "token": "syncplicityOK7EW7S0X1KGEMT21L2BEBJL62CS2EXBF3F0THIPIZF44WCRPKV1JWYZSRYVZ5M6ZTPY94ZLMLQ0MNO2"
}
```

Authenticating Users and Receiving the Authorization Grant Code

1 Redirect URL

2 Authenticate Users

3
Authenticate Instance

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

- code
- state

Response Parameter	Description
code	The Authorization Grant Code required by SAP Cloud Platform Open Connectors to retrieve the OAuth access and refresh tokens from the endpoint.
state	A customizable identifier, typically the connector key (`syncplicity`) .

> **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

1
Redirect URL

2
Authenticate Users

3 Authenticate Instance

Use the `/instances` endpoint to authenticate with Syncplicity and create a connector instance.

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

To create a connector instance:

1. Construct a JSON body as shown below (see OAuth2 Parameters):

```
{
  "element": {
    "key": "syncplicity"
  },
  "providerData": {
    "code": ""
  },
  "configuration": {
    "authentication.type": "oauth2",
    "oauth.api.key": "",
    "oauth.api.secret": "",
    "oauth.callback.url": "",
    "syncplicity.user.email": ""
  },
  "tags": [
    ""
  ],
  "name": ""
}
```

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

```
POST /instances
```

> **Note:** Make sure that you include the User and Organization keys in the

> header. For more information, see Authorization Headers, Organization Secret, and User Secret.

3. Note the **Token** and **ID** and save them for all future requests using the connector instance.

OAuth2 Example cURL

```
curl -X POST \
  https://api.openconnectors.us2.ext.hana.ondemand.com/elements/api-v2/instances \
  -H 'authorization: User , Organization ' \
  -H 'content-type: application/json' \
  -d '{
    "element": {
      "key": "syncplicity"
    },
    "providerData": {
      "code": "8aa74ff8ae16ba3ca19d12cbdea83aff16bddcd7"
    },
    "configuration": {
      "authentication.type": "oauth2",
      "oauth.api.key": "xxxxxxxxxxxxxxxxx",
      "oauth.api.secret": "xxxxxxxxxxxxxxxxxxxxx",
      "oauth.callback.url": "https://mycoolapp.com",
      "syncplicity.user.email": "fgrimes@springfield.power"
    },
    "tags": [
      "Test"
    ],
    "name": "SyncplicityInstance"
  }'
```

OAuth 2.0 Parameters

API parameters not shown in SAP Cloud Platform Open Connectors are in `code formatting`.

Parameter	Description	Data Type
`key`	The connector key. syncplicity	string
	The authorization grant code returned from the API provider in an OAuth 2.0 authentication workflow.	

Parameter	Description	Data Type
`code`	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
Authentication Type `authentication.type`	Optional. Identifies the type of authentication used in the request. Use `oauth2`.	string
Syncplicity User Email `syncplicity.user.email`	The user email address associated with your Syncplicity account.	string
`oauth.api.key`	The API key or client ID obtained from registering your app with the provider. This is the App Key that you recorded in the API Provider Setup section.	string
`oauth.api.secret`	The client secret obtained from registering your app with the API provider. This is the App Seret that you recorded in the API Provider Setup section.	string
`oauth.callback.url`	The URL that the API provider returns a user to after they authorize access. This is the redirect URI (`https://auth.cloudelements.io/oauth)` you entered in the API Provider Setup section.	
`tags`	*Optional.* User-defined tags to further identify the instance.	string

Example Response for an Authenticated Connector Instance

The following example response is the payload received when authenticating through OAuth 2.0.

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.


```
{
  "id": 12345,
  "name": "API Instance",
  "createdDate": "2017-08-07T18:46:38Z",
  "token": "ABC/Dxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
  "element": {
    "id": 361,
    "name": "Syncplicity",
```

```
    "hookName": "syncplicity",
    "key": "syncplicity",
    "description": "Add a Syncplicity Instance to connect your existing Syn
cplicity account to the documents Hub, allowing you to share and manage doc
uments, files, and more across multiple connectors. You will need your Sync
plicity account information to add an instance.",
    "image": "elements/provider_syncplicity.png",
    "active": true,
    "deleted": false,
    "typeOauth": true,
    "trialAccount": false,
    "configDescription": "Syncplicity",
    "defaultTransformations": [  ],
    "transformationsEnabled": true,
    "bulkDownloadEnabled": false,
    "bulkUploadEnabled": false,
    "cloneable": false,
    "extendable": false,
    "beta": false,
    "authentication": {
        "type": "custom"
    },
    "extended": false,
    "hub": "documents",
    "protocolType": "http",
    "parameters": [   ],
    "private": false    },
    "elementId": 361,
    "tags": [
      "Docs"
      ],
    "provisionInteractions": [],
    "valid": true,
    "disabled": false,
    "maxCacheSize": 0,
    "cacheTimeToLive": 0,
    "configuration": {    },
    "eventsEnabled": false,
    "traceLoggingEnabled": false,
    "cachingEnabled": false,
    "externalAuthentication": "none",
    "user": {
        "id": 12345
      }
}
```


Custom Authentication

Use the `/instances` endpoint to authenticate with Syncplicity and create a connector instance.

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

To create a connector instance:

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

```
{
  "element": {
    "key": "syncplicity"
  },
  "configuration": {
    "authentication.type": "custom",
    "oauth.api.secret": "******",
    "syncplicity.app.token": "******",
    "oauth.api.key": "******",
    "syncplicity.user.email": "address@your.email"
  },
  "tags": [
    ""
  ],
  "name": ""
}
```

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

```
POST /instances
```

> **Note:** Make sure that you include the User and Organization keys in the header. For more information, see Authorization Headers, Organization Secret, and User Secret.

3. Note the **Token** and **ID** and save them for all future requests using the connector instance.

Custom Authentication Example cURL

```
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": "syncplicity"
    },
    "configuration": {
      "authentication.type": "custom",
      "oauth.api.secret": "******",
      "syncplicity.app.token": "******",
      "oauth.api.key": "******"


      "syncplicity.user.email": "address@your.email"



    },
    "tags": [
      "Test"
    ],
    "name": ""
  }'
```

Custom Parameters

API parameters not shown in SAP Cloud Platform Open Connectors are in `code formatting`.

Parameter	Description	Data Type
Key `key`	The connector key. syncplicity	string
Name `name`	The name of the connector instance created during authentication.	string
Authentication Type `authentication.type`	Optional. Identifies the type of authentication used in the request. Use `custom`.	string
API Secret `oauth.api.secret`	The API Secret you identified in API Provider Setup.	string
Syncplicity App Token		

Parameter	Description	Data Type
`user.password`	The app token you identified in API Provider Setup.	string
API Key `oauth.api.key`	The API Key you identified in API Provider Setup.	string
Syncplicity User Email `syncplicity.user.email`	The user email address associated with your Syncplicity account.	string
`tags`	Optional. User-defined tags to further identify the instance.	string