

Technical Specifications – IBM COS Connector

IBM COS Connector is a utility to connect IBM Cloud Object Storage from Salesforce and upload/download large files. It's a Lightning Web Component which can be added to any page in portal and community. Its setup is very simple and there is NO file size restriction.

Setup and Configuration

Once you install IBM COS Connector to your Salesforce Org, it will add following components,

Lightning Web Component

- cosUpload – It's the main LWC which you can add to any page using Lightning Builder.

Apex Classes

- GetIAMToken – This apex class has the method to get IAM Authorization Token. This token is used to authorize HTTP requests to IBM Cloud Object Storage.
- GetIAMTokenTest – This is test class for GetIAMToken.
- GetIAMTokenHttpCalloutMock – This class is used to mock HTTP Callout request for testing.

Named Credentials

- COSToken – This Named Credential contains the IAM Token endpoint url and API Key as password. Please create new Named Credential with the same name i.e COSToken after installing this package and add your IAM API Key as password. *Package will add this Named Credentials, but make sure to add new one with the same configuration.*

Custom Metadata

- COS_Endpoint__mdt – This custom metadata stores the url of IBM Cloud Object Storage bucket. Please update this with your bucket url.

Remote Site Settings

Add "IAM Token endpoint" and "IBM Cloud Object Storage" endpoints in Remote Site Settings of your org.

CSP Trusted Site

Add "IAM Token endpoint" and "IBM Cloud Object Storage" endpoints in CSP Trusted Site Settings of your org.

Add CORS setting to IBM Cloud Object Storage bucket (IMPORTANT**)**

Once you create IBM Cloud Object Storage instance and add bucket to it, by default it will not add any CORS settings for that bucket. To allow HTTP requests from salesforce, you must add CORS rules to your COS bucket.

You can add CORSRules to COS Bucket using IBM Cloud CLI.

- Login to IBM Cloud CLI
- Create a json file that contains the CORSRules as shown below.
- Upload this file to the root file directory of IBM Cloud.
- Run this command

Command: `ibmcloud cos bucket-cors-put --bucket <BUCKET-NAME> --cors-configuration file:///<CORS-JSON-STRUCTURE> --region <REGION>`

Where,

BUCKET-NAME – IBM COS bucket name

CORS-JSON-STRUCTURE – It's the JSON structure of CORS rules

```
{
  "CORSRules": [
    {
      "AllowedOrigins": ["*"],
      "AllowedMethods": ["GET", "HEAD", "POST", "PUT", "DELETE"],
      "AllowedHeaders": ["*"]
    }
  ]
}
```

REGION – IBM COS Bucket Region

You can add the same using S3 API as well. You need to generate base64 encoded Content-MD5 (echo -n '<CORSConfiguration>' | openssl dgst -md5 -binary | openssl enc -base64) and pass it in the header of the PUT request.

```
echo -n '{
  "CORSRules": [
    {
      "AllowedOrigins": ["*"],
      "AllowedHeaders": ["authorization", "content-type"],
      "AllowedMethods": ["GET", "HEAD", "POST", "PUT", "DELETE"]
    }
  ]
}' | openssl dgst -md5 -binary | openssl enc -base64
```