

Con Edison/Orange & Rockland Green Button Connect

Third-Party Technical Onboarding Document



conEdison



Orange & Rockland

Document Version	4.3
------------------	-----

Creation Date	3/14/2018
---------------	-----------

Last Update Date	9/5/2024
------------------	-----------------

INTERNAL

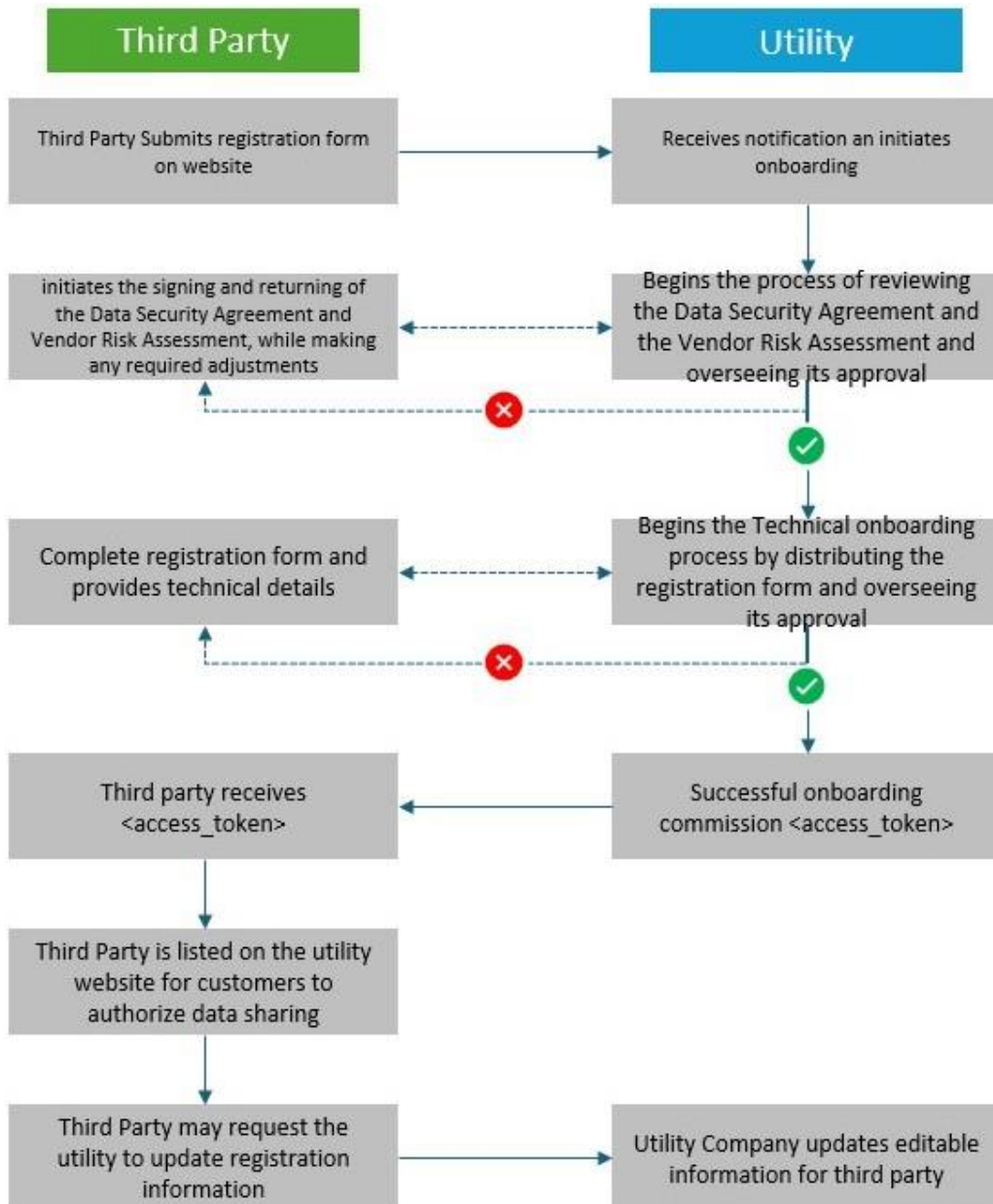
CONTENTS

- 1. Objectives..... 3
- 2. Overview 4
- 3. Technical onboarding PROCESS 7
 - Historic Usage Data.....19
 - Real-Time Usage Data.....20
- 4. Post onboarding 21
- 5. Key Responsibilities – Third Party..... 22
- 6. Document References..... 23

1. OBJECTIVES

The purpose of this document is to describe Con Edison/Orange & Rockland for the Green Button Connect My Data program and the Technical Onboarding process to be followed by a Third-Party to register with this program.

The below diagram provides a high-level overview of the process:



2. OVERVIEW

2.1 Green Button Connect

- Download My Data
 - This document is intended to detail the Green Button Connect feature; it is important to distinguish this from Green Button Download. The Green Button Download feature is accessible through a user-friendly interface on the Con Edison website. By logging in and visiting the energy usage section users can review and analyze up to one year of their energy consumption data presented in an easy-to-understand spreadsheet format. Additionally, users have the option to download detailed energy usage information, as recorded by their smart meter, in either CSV or XML formats.

Learn more [Download Your Energy Data | Con Edison](#)

- Connect My Data

Green Button Connect My Data (CMD), the commonly known name for the component of the North American Energy Standards Board's (NAESB) **REQ.21 - Energy Services Provider Interface Model Business Practices** for the authorized sharing of usage data, is the energy-industry standard for enabling easy access to, and secure sharing of, utility-customer energy data.

 - Machine to Machine data exchange
 - Requires customer authorization for sharing data.
 - High level overview of scopes and types of data exchanges (EUI/PII)

Learn more [Green Button Connect My Data® \(CMD\) - Green Button Alliance](#)

2.2 Connect My Data Overview

2.2.1 Third Party Registration

Upon successful completion of Data security agreement, the Con Edison GBC technical onboarding team will electronically send the Technical Onboarding welcome package to the third-party vendor. This package consists of the following:

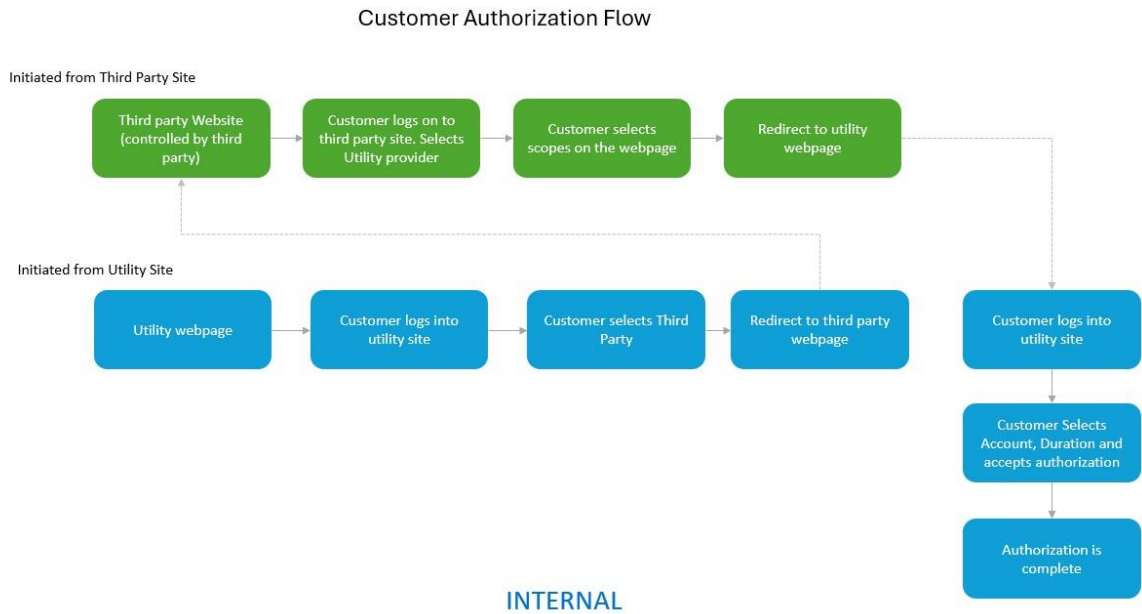
- GBC onboarding technical documentation
- Registration form
- Endpoint checklist (API's list)

To utilize the GBC API, it's necessary to first acquire customer authorization. We expect third-party vendors to create their own websites for managing customer authorizations and storing responses from the GBC application.

To proceed with the technical onboarding process, the third party must share all relevant technical details with Con Edison's GBC technical onboarding team. This team, comprised of technical specialists, serves as a point of contact for third-party vendors to address any issues they may encounter during the onboarding process.

2.2.2 GBC Customer Authorization flow

The following diagram displays the customer authorization flow:



Customers have the option to commence data authorization from either the third-party vendor's portal or the utility's website. Should the process initiate on the utility's site, the customer will be redirected back to the third-party's platform to initiate the scope selection. The flow of this information exchange is further elaborated in the following sections.

2.2.3 GBC APIs

2.3.1 APIs to access Third Party Registration Information

2.3.2 APIs to access data for a specific customer authorization.

2.3.3 APIs to access data for all customer authorization to the third party.

3. TECHNICAL ONBOARDING PROCESS

3.1 Technical Onboarding Process Overview

Stages of technical onboarding

1. Third Party Registration in Test Environment

- Registration Form fields

A third-party vendor must send the completed registration form with details of their test environment to Con Edison GBC Technical onboarding team to start the onboarding process using this [registration form](#).

- After the third-party supplies the registration form, the Con Edison GBC technical onboarding team will set up the third-party on the GBC Share My Data platform .The onboarding team will share registration access token and application information id via email. Third party can retrieve client id and client secret using Application information Api.
- The third-party must notify Con Edison GBC technical onboarding team when they are ready to start the customer authorization testing. (Currently third-party vendors cannot access the GBC test environment. The Con Edison GBC technical onboarding team will assist in this process).
- The third-party must notify Con Edison whenever there is a change to the registration information that was provided to Con Edison by emailing the updated registration form.

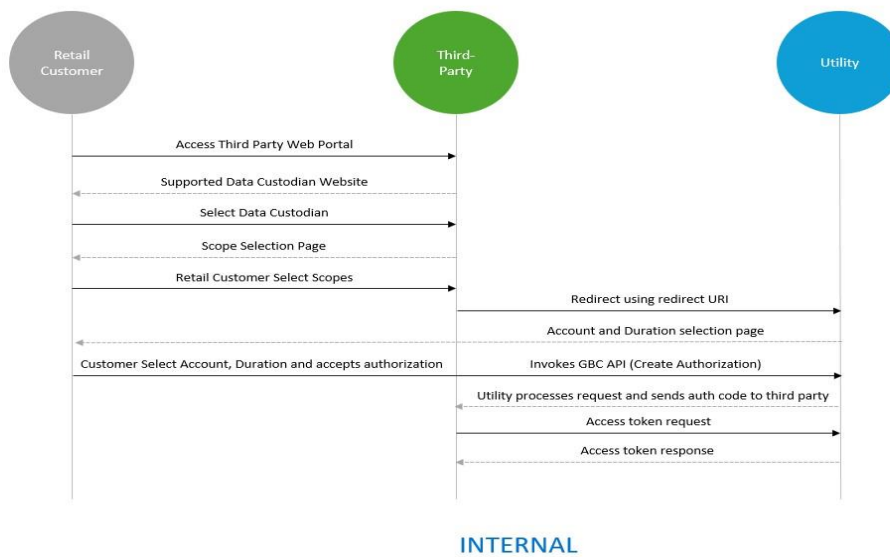
Note : Email Address - (dlsharemydatatech@coned.com)

- **Note:** Third-party vendors can request a mock customer authorization application code via an email (dlsharemydatatech@coned.com) to the Con Edison GBC technical onboarding team if needed.
- All URLs need to be accessible from ConEd network and should support TLS 1.2 or higher version.

- Successful onboarding response details:
Upon successful onboarding Third party is expected to send below 2 items :
1) Application Information Id
2) Registration Token

2. Customer Authorization Flow Testing in Test Environment

- Customer Initiates Authorization from Third Party Portal



- **Customer Login** : The process begins with the customer logging into the third party website, where they will choose their utility provider and select the types of data they consent to share.
- **Select Utility** : The customer selects their Utility provider (CECONY or ORU).
- **Scope Selection WebPage** : The retail customer begins the authorization process on the third-party portal where they can select one or more scopes to share.
- **Note** : Third-Parties have the option to predefine these scopes. Here are two options:
 - i. Let the customer see and choose the scope.
 - ii. Send a predefined scope each time which will be used for authorization.

The customer is then redirected to Con Edison's website. The Url used for this redirection will contain parameters related to scope, client Id , callback URI, state and response Type.

- **Redirection to Authorization server** : The customer is redirected to the authorization server.

Url used for redirection will be :

```
{{base_url}}/oauth/Authorize?scope=FB=1_3_4_5_7_10_15_16_35_51_53_56_57_58_60_67;IntervalDuration=Monthly;BlockDuration=Monthly;HistoryLength=63072000_86400;&client_id=<<client_id>>&redirect_uri=<callbackURI>&state=<state>&response_type=<response_type>
```

i. On Con Edison's site, the customer will be presented with the following options:

- Verify and/or edit (only removal of selected scopes is permitted) the preselected scopes from the third-party portal.
- Select their account number.
- Select the duration of the authorization for their account.
- Accept the authorization.
- Once the customer makes their selections, the GBC API will be invoked to create the authorization.

After user selects account and duration it will invoke the GBC api to create authorization.

- **TAccess token generation** : The third party uses this authorization code to make a request to the token endpoint , which will finalize the authorization process and activate the authorization record .
 - **Request/Response for access token generation** :

Request : The third – party vendors required to generate access token during authorization process :

API : https://webapi-test.coned.com/gbc/espi/1_1/oauth/token

Body :

```
{  
  "grantType":"authorization_code",  
  "clientId" : "<<Third-Party Client ID>>",  
  "clientSecret" : "<<Third-Party Client Secret>>",  
  "redirectUri" : "<<Third-Party registered redirect URI>>",
```

```
        "oauthCode": "<<code parameter you receive in link from
coned>>"
    }
```

Header :

Content -type	application/json
---------------	------------------

Note : Production Url :

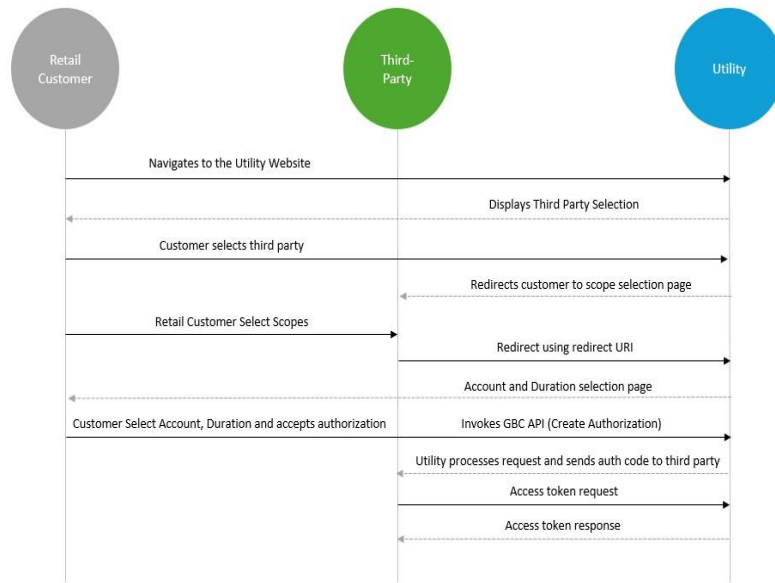
https://api.coned.com/gbc/espi/1_1/oauth/Token

Response :

```
{
    "access_token": "<<Access token for data exchange
which will be valid for 1 hour from the time it is generated>>"
    "refresh_token": "<<token used to generate new access
token once it is expired>>",
    "token_type": "Bearer",
    "expires_in": 3600,
    "scope": "<<Customer selected scope string>>",
    "resourceURI":
    "https://api.coned.com/gbc/v1/resource/Batch/Subscription/",
    "authorizationURI":
    "https://api.coned.com/gbc/v1/resource/Authorization/"
    "customerResourceURI": "<<customerResourceUri>>"
}
```

- **Customer Initiates Authorization from ConEd/ORU Portal**

The following diagram outlines the steps that needed to be followed when the customer authorization begins at the utility's website.



INTERNAL

- **Customer Login :** Customer logs into the Utility's website .
- **Third-Party Selection:** Customer navigates to the Share My Data page, server gives list of third parties. Customer then selects the authorized third party.
- **Redirection to Third-Party:** Customer is redirected to the third-party's Scope selection URI :
 - Utility will redirect customer to Third-Party Scope Selection Screen URI .
 - Customer logs onto Third-Party website.
- **Scope selection Webpage at Third Party website :** A customer can select one or more scopes from the scope selection screen and confirm authorization in the third party website .
 - The scope selection screen will list all the available scope strings for a retail customer to give access to a third party.

Please find below Functional Blocks and its description:

[FB_01]	Usage Data common
[FB_03]	Usage Data Connect My Data
[FB_04]	Interval Reading

[FB_05]	Electricity Interval Meeting
[FB_07]	Net Electricity Meeting
[FB_10]	Natural Gas Interval Meeting
[FB_15]	Usage Summary
[FB_16]	Usage Summary with cost
[FB_35]	Usage Data Bulk
[FB_51]	Retail Customer Common
[FB_53]	Retail Customer Connect My Data
[FB_56]	Retail Customer Billing Information
[FB_57]	Retail Customer Account-Agreement Information
[FB_58]	Retail Customer Service-location Information
[FB_60]	Retail Customer Meter Information
[FB_67]	Retail Customer Bulk

- Here's the sample image of webpage:



Below is the sample representation of scopes on a third-party portal :

Scope Name	Scope Value
------------	-------------

Consumption Electric Scope	<u>FB=1_3_4_5;IntervalDuration=Monthly_3600_900_300;BlockDuration=Monthly_Daily;HistoryLength=63072000_86400;</u>
Consumption Electric Net Scope	<u>FB=1_3_4_7;IntervalDuration=Monthly_3600_900_300;BlockDuration=Monthly_Daily;HistoryLength=63072000_86400;</u>
Consumption Gas Scope	FB=1_3_4_10;IntervalDuration=Monthly_3600_900_300;BlockDuration=Monthly_Daily;HistoryLength=63072000_86400;
Billing Information Without Cost Scope	FB=1_3_15;IntervalDuration=Monthly;BlockDuration=Monthly;HistoryLength=63072000;
Billing Information With Cost Scope	FB=1_3_15_16;IntervalDuration=Monthly;BlockDuration=Monthly;HistoryLength=63072000;
Retail Customer	FB=51_53_56_57_58_60;
Customer	Customer can select custom scopes

Note :

- Third-Party should pass selected scopes separated by a ‘|’ pipe symbol to the Utility after the customer has selected which scopes, they want to share with the third-party. For example: scope= <selected scope 1> | <selected scope 2> | <selected scope 3>.
- If a third party does not pass valid scope values , the authorization process will fail.

- Redirect to Utility : After selection of scope redirect using oauth url to utility with user selected scope string as mentioned below :

	Test	Production
CECONY	https://uat10.coned.com/oauth/authorize?clientId=abc&scope=FB=1_3_4_5_7_10_13_28_31_35_37_39_41_44;IntervalDuration=Monthly_3600_900_300;BlockDuration=Monthly_Daily;HistoryLength=63072000_86400;&state=123	https://api.coned.com/oauth/authorize?clientId=abc&scope=FB=1_3_4_5_7_10_13_28_31_35_37_39_41_44;IntervalDuration=Monthly_3600_900_300;BlockDuration=Monthly_Daily;HistoryLength=63072000_86400;&state=123
ORU	https://uat10.oru.com/oauth/authorize?clientId=abc&scope=FB=1_3_4_5_7_10_13_28_31_35_37_39_41_44;IntervalDuration=Monthly_3600_900_300;BlockDuration=Monthly_Daily;HistoryLength=63072000_86400;&state=123	https://api.oru.com/oauth/authorize?clientId=abc&scope=FB=1_3_4_5_7_10_13_28_31_35_37_39_41_44;IntervalDuration=Monthly_3600_900_300;BlockDuration=Monthly_Daily;HistoryLength=63072000_86400;&state=123

- **Manage Third Party authorization** : A selection web page is displayed where the following fields are present:
 - Account Number selection
 - Select the duration for their chosen account.
 - Accept or deny authorization.

After user selects account, duration and accepts or denies authorization it will invoke the GBC api to create authorization.

Url :

```

{{base_url}}/oauth/Authorize?scope=<scope>;IntervalDuration=<duration>;BlockDuration=Monthly_Daily;HistoryLength=63113904;|FB=1_3_6_10_13_14_15_16_28_32_33_35_37_38_41_44;IntervalDuration=Monthly;BlockDuration=Monthly;HistoryLength=63113904;|FB=1_3_4_5_7_13_14_18_32_33_35_37_38_41_44;IntervalDuration=900_300;BlockDuration=Daily;HistoryLength=86400;&clientId=<client_id>&redirectUri=<callbackURI>&MAID=<maid>&accountNumber=<acct>&startDate=<start>&endDate=<end>

```

- Authorization Code generation at Utility : Upon receiving the above request, the Utility will generate a one-time authorization code and redirect to the Third Party's registered redirect URI. During the authorization process, it is crucial to use the authorization code as soon as possible before it expires (5-minute expiry).
- There is sample image below :

If the request is accepted, the server responds with an OAuth 2.0 Authorization Code Grant response.

HTTP/1.1 302 Found Location: https://naesb.thirdpary.com/esp/1_1/OAuthCallback?code=DusXAVksa7edJEbzm16wg2Q9xdKSaCf5Kz516NsZ3H3KDFErPasVYmnNUteXkRaM&state=ee148ec2-9892-466e-a013-4dedf1eb3018
--

- **Access token generation** : he third party uses this authorization code to make a request to the Token endpoint, which will finalize the authorization process and activate the authorization record, refer to the Third-Party exposed API's list and sample request below :

- **Request / Response for access token generation:**

Request : The third-party vendors are required to generate the Third- party User Token (i.e., Access Token) during the authorization process.

API : https://webapi-test.coned.com/gbc/esp/1_1/oauth/Token

Body:

```
{
  "grantType":"authorization_code",
  "clientId":"<<Third-Party Client ID>>",
  "clientSecret":"<<Third-Party Client Secret>>",
  "redirectUri":"<<Third-Party registered redirect URI>>",
  "authCode": "<< code parameter you receive in the link from coned >>"
}
```

Header

Content -type	application/json
---------------	------------------

Note : Production Url :

https://api.coned.com/gbc/espi/1_1/oauth/Token

Response :

```
{  
  "access_token": "<<Access token for data exchange which will be  
  valid for 1 hour from the time it is generated>>",  
  "refresh_token": "<<token used to generate new access token  
  once it is expired>>",  
  "token_type": "Bearer",  
  "expires_in": 3600,  
  "scope": "<<Customer selected scope string>>",  
  "resourceURI":  
  "https://api.coned.com/gbc/v1/resource/Batch/Subscription/<<su  
  bscription id used for data exchange>>",  
  "authorizationURI":  
  "https://api.coned.com/gbc/v1/resource/Authorization/<<authoriza  
  tion id used for viewing or updating authorization details>>  
  "customerResourceURI":<< customerResourceURI >>  
}
```

Note :

- Processing and storing the response will be controlled by the third-party.
- The access token will be active for 1 hour from the time of its creation. The Third-Party will have to invoke the token API along with the refresh token, their client credentials and scope to generate a new access token.
- Third-party should cache the access token and reuse the access token for subsequent API calls until the access token expires. Access token will be active for 1 hour.

3. GBC API Testing in Test Environment

- Swagger Documentation

<https://dcx-downloads-prod.azureedge.net/gbc-api-defintions/swagger-cert.json?sp=r&st=2024-08-29T02:55:48Z&se=2031-08-29T10:55:48Z&spr=https&sv=2022-11-02&sr=b&sig=WAVltmTKe4OKqZW05je%2FUMTZSB5%2BdMk8FbgNHR%2FkCU%3D>

You can download the above definitions and render/upload in your choice of swagger viewer/editor. <https://editor.swagger.io> is commonly used. Below is an example of .JSON uploaded.

- After successful customer authorization in Phase 1 , the Third Party can proceed to test APIs. Third parties can import postman and environment collection available here for testing the api's:
<https://www.coned.com/-/media/files/coned/documents/accountandbilling/share-my-data/onboarding-doc-files/postman-collection.json>
<https://www.coned.com/-/media/files/coned/documents/accountandbilling/share-my-data/onboarding-doc-files/postman-environment.json>
- Third Parties are required to send the completed status of API testing to the Con Edison GBC technical onboarding team for review.
- Synchronous vs Batch APIs
 - a. Upon receiving the BatchList of Resource URLs, the ThirdParty looks up the Authorization associated with each Resource URL and uses the access_token in conjunction with the entire Resource URL from the BatchList to make the GET request to retrieve the data. Note that this BatchList may include URLs for Bulk Resources and/or individual ones.
 - b. Depending on the structure of the Data Custodian, data requested may not be available. It is possible Subscriptions and Bulk Green Button ESPI implementation API requests may have large data responses that require time to assemble.
 - c. The HTTP response code 202 signifies to the Third Party a Data Custodian has accepted the request and will require some time to assemble the response. When the Data Custodian has completed assembling the data, it MUST issue a notification to the Third Party's notification endpoint with the URI the Third Party will use to retrieve the assembled data.
 - d. TPs should avoid sending duplicate batch requests while one is still pending. The GBC platform will reject duplicate requests, and sending duplicates will not reduce the wait time for the initial request.

4. Third Party Registration in Production Environment

Upon successful completion of all testing stages, third-party vendors can progress to the production stage.

NOTE: Third-party vendors are required to fill in the registration form with the production data.

- Production Registration Form
- Note that we will not be doing any customer authorization testing in production.

3.2 ConEd and ORU Data Custodian

The registration process for Con Edison (ConEd) and Orange & Rockland Utilities (ORU) is identical. However, the Third Party authorization needs to be directed to different utilities based on the specific account they intend to authorize. This means that depending on the account they're authorizing, the Third Party needs to route their authorization to the appropriate utility.

3.3 Additional Details regarding Coned GBC Program

a. Access Token expiry, Token Caching

All access Token expire in 60 mins and we recommend third parties to cache the access token and reuse them for subsequent calls for the same subscription within the expiration period.

Since the access token expires in 1 hour, we recommend that TPs store a timestamp in their system. This will help identify expired tokens, preventing unauthorized responses. Always obtain a new access token before making a new call if the current one has expired.

b. Rate Limits for APIs

Rate limiting is in place for the token endpoint and it will only allow 50 token API calls within one minute. For all other endpoints, no rate limit is in place currently.

c. Batch API response times

Batch notification time can vary depending on the batch processing queue size. Typically notifications are sent within one hour but when the system is under heavy load, batch responses can take up to 24 hours.

d. Refresh token expiry

If a refresh tokens is not used to acquire a new access token, refresh token will expire after one year. If the refresh token expires, third party needs to contact the customer to revoke the old authorization and re-authorize the account to get a new refresh token.

e. Real time APIs

f. Latency of data for real time and historic data

- For commissioned and communicating, historical meters Interval data availability is
 - 1) 80-90% within 24 hours
 - 2) 99% within 3 days
 - 3) 99.8% within 7 days
- For real time data, Meter Readings are available for last 24 hours. For Electricity data, data latency will be 45 minutes from the request processing time.

g. Data quality of real time and historical data

- Historical interval data represents finalized and validated information, while real-time data is considered provisional and unvalidated. A QualityOfReading value of 17 signifies good and validated data.
- Real time interval data are not billing quality data

h. Reading types for commercial, residential, and solar accounts

[Historic Usage Data](#)

Meter Readings are displayed per mentioned intervals for an Electricity or Gas account. The requested intervals should be within last 2 years of range from current date.

Customer Category	Usage Data Available
Electric Commercial Customers with AMI Meters	5-minute intervals
Electric Residential Customers with AMI Meters	15-minute intervals
Electric Customers with Legacy Interval Meters	15-minute intervals
All Gas Customers with AMI Meters	1-hour intervals
All customers with Non-Interval Meters	Monthly

[Real-Time Usage Data](#)

Meter Readings are from last 24 hours, only for Electricity data, with a latency of 45 minutes from the request processing time.

Customer Category	Usage Data Available
Electric Commercial Customers with AMI Meters	5-minute intervals
Electric Residential Customers with AMI Meters	15-minute intervals
Electric Customers with Legacy Interval Meters	15-minute intervals

- i. Batch response - file chunking
- j. Bulk chunking - TBD

3.4 Timeline expectation for finishing technical onboarding.

The anticipated timeline for completing the onboarding process is between 30 to 60 minutes. This includes all necessary steps and procedures involved in getting fully set up and ready to proceed.

3.5 Onboarding Team Support

- Onboarding overview meeting
- Support DL

4. POST ONBOARDING

4.1 Registration Information Updates

In the event a third party need to update any fields associated to their registered information in a registration form , they need to update those fields and resend the completed registration form with updated fields.

4.2 Client Name change requirements

1) Third Party Client Access token [CAT]

- a. The Third-Party can generate this token following the successful completion of the onboarding process.
- b. This token can be used to retrieve data for all the customers who are actively authorized with the Third-Party. The type of data could be Usage, Billing, and Account Details based on the scope of authorization granted to the Third-Party.

- c. Sample Request Body :

```
{  
  "grant_type":"{{client_credentials}}",  
  "scope": "FB=35_67"  
}
```

2. Third Party User Access Token

- a. This token can be used to retrieve a specific customer's Usage / Billing / Real-Time / Retail Customer data based on the scope provided during authorization. This token cannot be shared across multiple authorizations.

- b. Sample Request Body :

```
{"redirect_uri": "{{redirect_uri}}",  
  "refresh_token": "{{refresh_token}}",  
  "grant_type":"refresh_token",  
  "scope": "FB=1_3_4_5_7_10_15_16_51_53_56_57_58_60" }
```

4.3 Reporting production issues

5. KEY RESPONSIBILITIES – THIRD PARTY

The following are the Key responsibilities to be taken care of by the Third-Party during the Technical Onboarding process:

#	Key Responsibilities
1	The Third-Party will receive a Notification from the Utility to provide the required registration details.
2	The Third-Party will be responsible for: Ensuring the registration form contains the correct details and their website is set up as per the process mentioned above in this document Notifying the Utility representative with the completed registration form
3	The Third-Party Client Access Token and access tokens are active only for 1 hour. The Third party should cache the token value for an hour and reuse it. After an hour, the Third-Party will have to request a new token by providing the refresh token, once the Client credentials and Subscription ID are received after successful authorization.
4	The Retail Customer API provides Account ID information (Account number, Address – street, city, state, town, postal code) for the corresponding subscription ID. The Third-Party is required to map and maintain the Account ID for its usage data.
5	The Third-Party will always receive up to the last two years of historical usage / billing data. They can apply a date filter to select the time range for requesting any customer's data within a 2 year time frame. Real-Time data only corresponds to electricity usage data for the last 24 hours with a latency of 45 minutes from the request processing time.
6	The Third-Party, upon data exchange requests, will be provided with "NET" consumption data for Solar accounts and only "consumption" data for Non-Solar accounts.
7	ESCO charges, if applicable for the customer, will be included in the BillLastPeriod displayed in the billing information.
8	The Third-Party, as part of Data exchange for NYPA customer(s) can access historical and real-time consumption data.
9	Unit of measurement for gas consumption is (CCF).
10	Real time api's not applicable for gas services.

6. DOCUMENT REFERENCES

#	Document	Document link / Reference ID
1	REQ.21 – Energy Services Provider Interface	http://www.naesb.org/ESPI_Standards.asp
2	The OAuth 2.0 Authorization Framework, RFC 6749	http://www.ietf.org/rfc/rfc6749.txt
3	The OAuth 2.0 Authorization Framework: Bearer Token Usage, RFC 6750	http://www.ietf.org/rfc/rfc6750.txt