Cross River | Docs

Get started

Welcome to Cross River documentation

Discover, explore and start integrating our products with ease

[Quickstart] [Explore all products]

Get started

Set up and start your journey using Cross River APIs

Concepts

Discover how Cross River solutions can transform your fintech journey

APIs

Develop using the Cross River banking platform and robust API sets

Tutorials

Learn how to use Cross River APIs step by step

2. **Quickstart**

Step 1 — **Get API credentials**
Step 2 — Get Access Token
Step 3 — Use Access Token
Step 4 — Build a Sample App
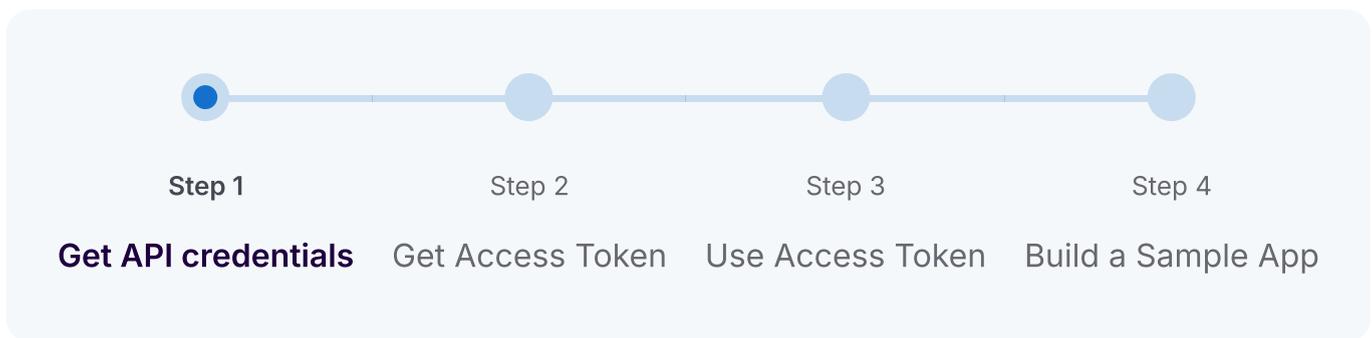
Get API credentials: Your first step to working with Cross River APIs is to register for API credentials.

Get access token: Once you've received your API credentials and before you can use our APIs, you must get an access token using the `client_id` and `client_secret` you received when you registered.

Use access token: Once you've successfully authenticated, an `access_token` is returned to you. Include this token in the header of your API calls.

Webhooks: Webhooks are an important component of any integration with Cross River. While APIs let you request data on demand, webhooks push real-time updates directly to your system—eliminating the need for constant polling and reducing latency.

Sandbox environments: The sandbox is a completely isolated environment, so feel free to experiment.

Swagger links: Links to all our swagger environments.

Get API credentials

Step 1	Step 2	Step 3	Step 4
Get API credentials	Get Access Token	Use Access Token	Build a Sample App
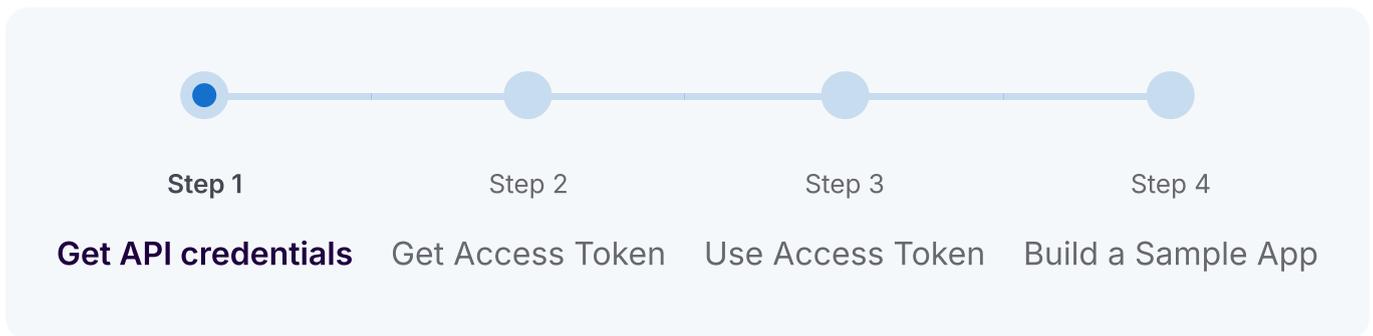
Your first step to working with Cross River APIs is to register for API credentials. With these credentials you can request and receive an access token to use for sending APIs in our sandbox environment.

> **IMPORTANT**
>
> Your IP address, which must be public and static, has to be on our allowlist. Your internal IT department should be able to provide you with this IP. Learn more about **static IPs**.

Sandbox Access

Submit a request for sandbox access, to receive API credentials.

Once your static IP is added to our allowlist, we will send you 2 encrypted emails with your credentials:

- One email contains your `client_id`, `partner_id` and other information you'll need depending on what you have requested.
- The second email, which is encrypted, contains your `client_secret` and `webhook_secret`. You'll need these for authentication and for working in the sandbox.

NOTE

If you asked for access to Card Payments, you'll receive an additional set of credentials including a second `client_id` and `client_secret`

2.2. Get access token
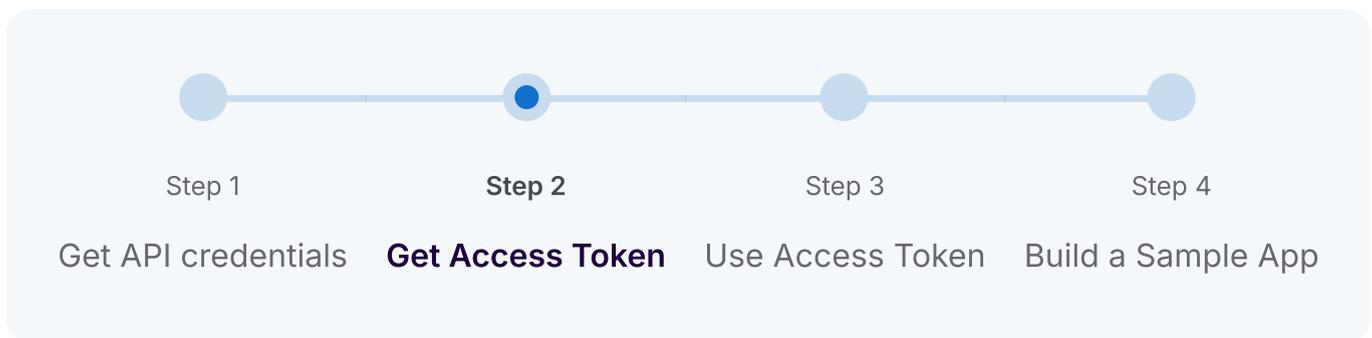
Cross River uses OAuth 2.0 for authentication and authorization. This controls entry to our system and ensures that only authorized entities can access our APIs and other protected resources. The information you enter into our authentication system is confidential and can never be accessed from any other Cross River applications.

Once you've received your **API credentials**, and before you can use our APIs, you must get an access token using the `client_id` and `client_secret` you received when you registered. This access token allows you to send information securely as a JSON object for use in our APIs. You must include this token in the header of each API request.

There are several ways to request and receive an access token:

- Use Command Line Interface (CLI) with cURL or any other language
- Use Postman or any other API testing tool

> Once obtained, copy the access token to your clipboard. Make sure you save it.

Command Line Interface

To request a token send a `POST connect/token` command containing the `client_id` and `client_secret` and `grant_type` to the **authentication server** (auth server) of the appropriate sandbox, as shown in the sample below.

Refer to the **HTTP components table** for an explanation of these tags.

The following example uses cURL to request a token from one of the auth servers.

📦 **Sample request in cURL for COS**

```
curl --location --request 'POST https://idptest.crbcos.com/connect/token' \
  --header 'Content-Type: application/x-www-form-urlencoded' \
   --data-urlencode 'client_id=[your id here]' \
  --data-urlencode 'client_secret=[your secret here]' \
  --data-urlencode 'grant_type=client_credentials' \
  --data-urlencode 'audience=https://api.crbcos.com/'
```

📦 **Sample response from cURL request**

```
{ "access_token": "contains many characters", \
    "expires_in": 86400, \
    "token_type": "Bearer" }
```

Postman

To request a token using Postman, send a `POST connect/token` command to the **auth server** of the appropriate sandbox. Add the `grant_type`, `scope (optional)`, `client_id` and `client_secret` to the call.

Refer to the **HTTP components table** for an explanation of these tags.
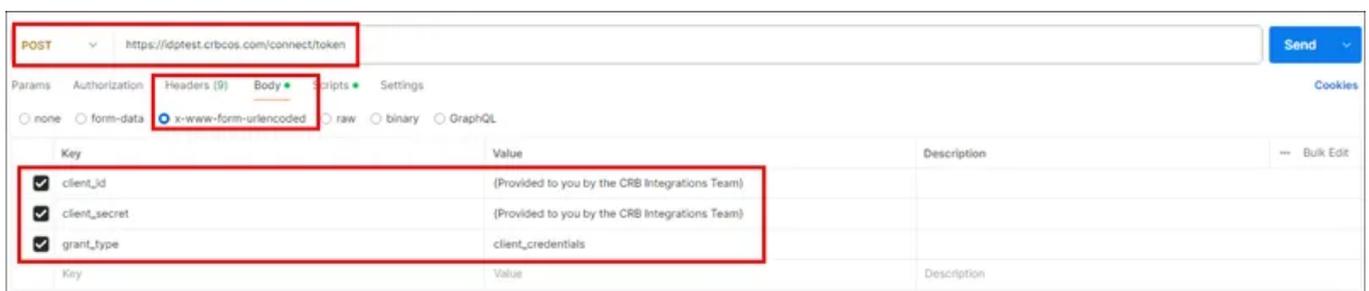
If the authentication is successful, the status code is 200 (OK).

```
1  {
2      "access_token":{xxxxxxxx}
       "expires_in": 3600,
       "token_type": "Bearer",
       "scope":  "relevant_scope"
   }
```

COS Explorer

In **COS Explorer**, click the down arrow next your login and click **Copy Access Token**.

The access token is copied to your clipboard, ready for use in the **Sandbox**.
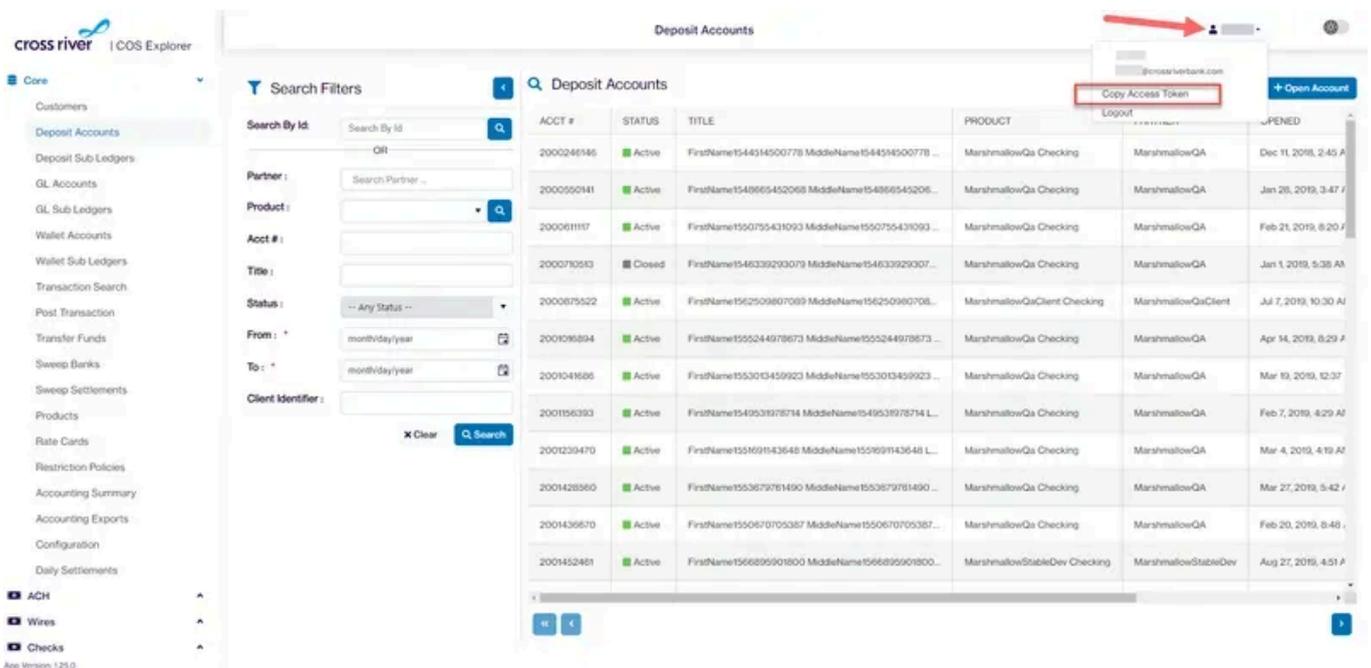
Token request response

Attribute	Description
`access_token`	A digitally signed JSON web token (JWT) sent from the oAuth server that allows access to specific Cross River resources
`scope`	A range of services that a user can access
`expires_in`	The amount of time until the token expires. - Our Integration Team will inform you of the expiration time or you can decode your access token as well. - We recommend that you retrieve a new access token a short time before the old token is set to expire. - Reuse tokens for their entire lifespan rather than getting a new token for each call to the same protected resource (API). **IMPORTANT:** Never decode your token on a publicly hosted website
`token-type`	Bearer token

HTTP components

The following HTTP components are used both in the API and Postman requests.

HTTP component	Tag	Description
Endpoint	`POST` `/connect/token`	Endpoint for retrieving an access token
Header	`content-type`	`application/x-www-form- urlencoded`
Body	`client_id`	The unique identifier for a client
Body	`client_secret`	An encrypted string of characters used to sign and validate ID tokens. **Important:** Secrets aren't recoverable by CR. If you lose a secret, a new one must be generated. **Do not** commit your secrets into source control.
Body	`grant_type`	This field will always have a value of `client_credentials`
Body	`audience` *optional*	A way for the user to validate if a particular access token is meant for them.
Body	`scope` *optional*	A specific range or a limited set of services that a user can access with an access token. If a scope isn't specified, the token returned will contain all scopes associated with your credentials. **Note:** Multiple scopes can be sent in the same request by adding a space between the name of each scope. For example: 'scope=scope1 scope2 scope3'

Auth server URLs

| Module	Auth server URL
Accounts	**https://idptest.crbcos.com/connect/token**
ACH	**https://idptest.crbcos.com/connect/token**
Wires	**https://idptest.crbcos.com/connect/token**
Checks	**https://idptest.crbcos.com/connect/token**
Core	**https://idptest.crbcos.com/connect/token**
Instant payments	**https://idptest.crbcos.com/connect/token**
Card issuing	**https://idptest.crbcos.com/connect/token**
Card payments	**https://crbcos-sandbox.auth0.com/oauth/token**
Lending	**https://oauthtest.crbnj.net/connect/token**

Troubleshooting

If the authentication token is valid, it will return a 200. If the authentication token isn't valid, it will return a 401.

If you unable to get a bearer token and you haven't received one in the past:

- Confirm the URL.
- Check that the `client_id` and `client_secret` are typed correctly. They are case sensitive.
- Check your `client_id` and `client_secret` against the one you received.
- Make sure there are no network or allowlist issues.

Contact our **Integration Team** if your account is locked as a result of 3 incorrect log in attempts.

2.3. Use access token
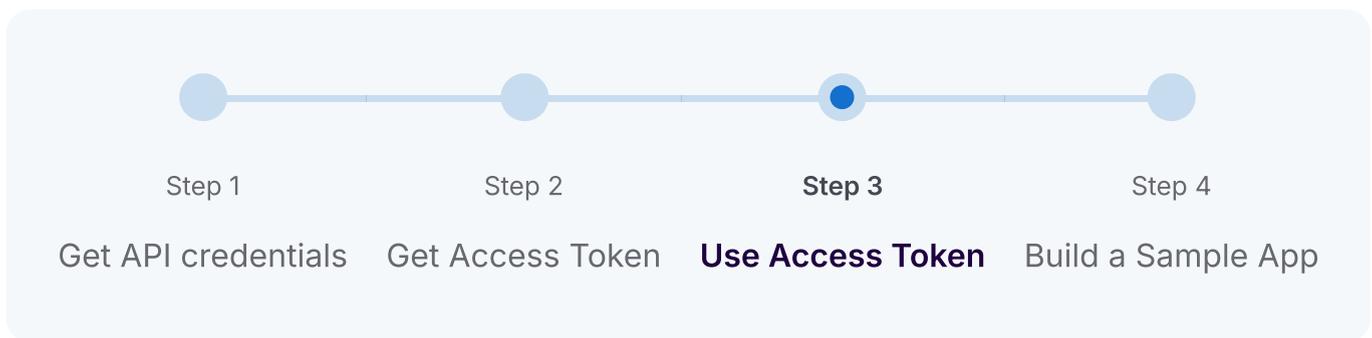
Step 1 — Get API credentials
Step 2 — Get Access Token
Step 3 — Use Access Token
Step 4 — Build a Sample App

Once you've successfully **authenticated**, an `access_token` is returned to you. Include this token in the header of your API calls.

The access token expires after a set period of time. The response containing the token also specifies the expiration time in seconds. Store and use your access token until it expires. We recommend you use the token until you receive a 401 unauthorized error, and then request a new token.

> **IMPORTANT**
>
> 1. Do not request a new token for every API request.
>
> 2. Make sure to protect your token. Anyone who steals your token can impersonate your client for the lifetime of the token.

API request header

In the header of each API request, include the access token as follows:

```
  Sample call for wire payment in cURL

curl --location --request 'POST https://sandbox.crbcos.com/Wires/v1/payments'
--header 'Authorization: Bearer [YOUR TOKEN HERE]' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-raw '{
  "accountNumber": "2255685659",
  "businessFunctionCode": "CTR",
  "receiverRoutingNumber": "021000021",
  "beneficiaryFi": {
    "idCode": "F",
    "identifier": "021000021",
    "name": "JP Morgan Chase"
  },
  "beneficiary": {
    "idCode": "D",
    "identifier": "123456789",
    "name": "Peter Griffin"
  },
  "beneficiaryReference": "XYZ123",
  "amount": 10000,
  "purpose": "payment"
}'
```

Postman

To use a token in Postman, navigate to the **Authorization** tab in your request, select **Bearer Token** as the authentication type, and paste your token into the provided field. Postman will automatically add the **Bearer** prefix and the token to the **Token** field.

Swagger

Provide the token using the method your version of Swagger requires.

In this example, at the top of this Swagger screen, paste the token into the **token** field and click **Explore**. The token is now activated.

2.4. Webhooks

Webhooks are an important component of any integration with Cross River. While APIs let you request data on demand, webhooks push real-time updates directly to your system eliminating the need for constant polling and reducing latency. In many cases, webhooks are more efficient and reliable than APIs alone, ensuring your application stays in sync with critical events like account changes, transaction updates, and processing outcomes.

> Use webhooks within the Cross River systems to notify you when different events occur. The event returns a resource object that contains relevant details about the subject of each event. The full event details are included and sent to your system.

We use webhooks to update you on status and to report transaction changes. Webhooks report to your system with real-time notifications when an event happens.

You must register via API to use webhooks:

- **Register for accounts, cards and payment events**
- **Register for card payments events**
- **Register for Lending events**

Our sandbox is a completely isolated environment, so feel free to experiment. When you're ready to move to production, let us know and we will get you production credentials to access the live environment.

Customer management

Module	Base URL for API calls
Customer management	https://sandbox.crbcos.com/core/

Accounts

Module	Base URL for API calls
Deposit accounts	https://sandbox.crbcos.com/core/
Deposit sweeps	https://sandbox.crbcos.com/sweepsintrafi/

Cards

Module	Base URL for API calls
Cards	https://sandbox.crbcos.com/cardmanagement/

Payments

Module	Base URL for API calls
Instant Payments	https://sandbox.crbcos.com/rtp/
Card payments: Push to pay	https://pushtopaystaging.crbnj.net/
Card payments: Pull	https://pullfromcardapistg.crbnj.net/
International Payments	https://sandbox.crbcos.com/international/
ACH	https://sandbox.crbcos.com/ach/
Wires	https://sandbox.crbcos.com/wires/
Checks	https://sandbox.crbcos.com/checks/

COS webhooks

Module	Base URL for API calls
COS webhooks	https://sandbox.crbcos.com/webhooks/

Lending

Module	Base URL for API calls
Loan origination	https://arixapisandbox.crbnj.net
Application Decisioning	https://lendingsandbox.crbcos.com/preapproval/v1

Customer management

Module	Swagger Link
Customer management	https://sandbox.crbcos.com/core/swagger/ui/index#/

Accounts

Module	Swagger Link
Deposit accounts	https://sandbox.crbcos.com/core/swagger/ui/index#/
Deposit sweeps	https://sandbox.crbcos.com/sweepsintrafi/swagger/ui/index#/

Cards

Module	Swagger Link
Cards	https://sandbox.crbcos.com/cardmanagement/swagger/ui/index#/

Payments

Module	Swagger Link
Instant payments	**https://sandbox.crbcos.com/rtp/swagger/ui/index#/**
Card payments: Push to pay	**https://pushtopaystaging.crbnj.net/swagger/ui/index#/**
Card payments: Push to pay batch	**https://pushtopaystaging.crbnj.net/batchswagger/ui/index#/Transactions**
Card payments: Pull	**https://pullfromcardapistg.crbnj.net/swagger/ui/index#/**
International payments	**https://sandbox.crbcos.com/international/swagger/ui/index#/**
ACH	**https://sandbox.crbcos.com/ach/swagger/ui/index#/**
Wires	**https://sandbox.crbcos.com/wires/swagger/ui/index#/**
Checks	**https://sandbox.crbcos.com/checks/swagger/ui/index#/**

COS webhooks

Module	Swagger Link
COS webhooks	**https://sandbox.crbcos.com/webhooks/swagger/ui/index#/**

Lending

Module	Swagger Link
API reference	**https://arixapisandbox.crbnj.net/swagger-ui**
Hooks	**https://lendingsandbox.crbcos.com/hooks/swagger/index.html**
Selling	**https://lendingsandbox.crbcos.com/selling/swagger/index.html**

3. Build a sample app
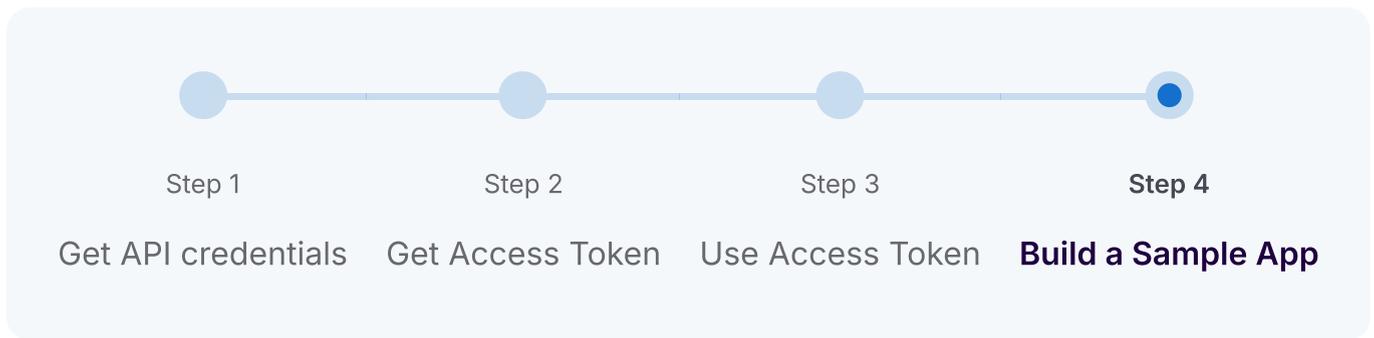
Step 1 — Get API credentials

Step 2 — Get Access Token

Step 3 — Use Access Token

Step 4 — **Build a Sample App**

- **Setup**: Before you start, refer to our quickstart guide to get connected to our APIs. To test the API calls, you can use cURL from the command line, or a service such as Postman or Swagger in our sandbox.

- **Customers and accounts**: Before you use Cross River services, you need to create a customer record for each of your customers

- **Cards**: Manage your customer's cards by working with Cross River to decide what you want to offer, such as physical or virtual cards.

- **Lending**: Lending includes a set of lending APIs calls to allow you to create, update, and manage your loans.

3.1. Setup

Before you start, refer to our **quickstart** guide to get connected to our APIs. To test the API calls, you can use cURL from the command line, or a service such as Postman or Swagger in our sandbox.

> To create a card or payment app, you must create **customer and accounts.**

Explore sandbox

We have full **sandbox environments** for you to explore. The sandbox is completely isolated from the production environment, so feel free to experiment. When you're ready to move to production, talk to your , who will get you production credentials to access the live environment.

Register relevant webhook events

Webhooks are an important component of any integration with Cross River. While APIs let you request data on demand, webhooks push real-time updates directly to your system—eliminating the need for constant polling and reducing latency. In many cases, webhooks are more efficient and reliable than APIs alone, ensuring your application stays in sync with critical events like account changes, transaction updates, and processing outcomes.

Register to receive webhook events. When webhook events are triggered, the event objects are sent to the registered URLs.

Step 1	Step 2	Step 3	Step 4
Get API credentials	Get Access Token	Use Access Token	**Build a Sample App**
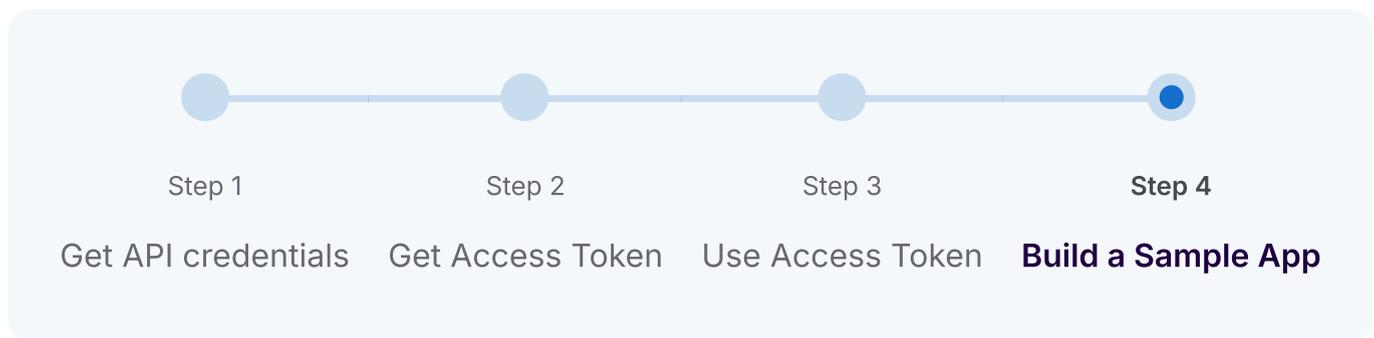
Create a customer record and a funded account:

- **Create a customer record**
- **Create** a deposit account
- **Fund** an account

Create a customer record

Before you use Cross River services, you need to **create a customer record** for each of your customers. The customer onboarding process includes creating a *customer record* with relevant customer information.

All customers are automatically scanned for regulatory compliance purposes, so you need to register for relevant webhooks events to receive customer record status updates.

The customer record can be for either *Personal* or *Business* customers. Once registered, a customer can be associated with one or more accounts.

Webhooks

Register for webhooks. The following webhooks are used:

Webhook	Description
`Core.Customer.Onboarded`	Notifies you that the customer record has been created
`Core.Customer.Ofac.Changed`	Notifies you that a customer's OFAC status has been updated
`Core.Customer.PepScan.Changed`	Notifies you that a customer's PEP status has been updated

Example of record creation

In this example, we'll onboard John Smith. First, let's create a customer record. We are registering John as a *Personal* customer.

> To onboard a business customer, first create a personal customer record for the *primary owner* of that business. After that, create a business customer and add the personal record as a **beneficial owner**.

1 Call `POST /core/v1/cm/customers`.

In the following example you can see **which attributes** are required.

> **IMPORTANT**
> We highly recommend you include an **idempotency key** in your request header to provide duplicate protection in the event of a failure.

```
curl -X POST /core/v1/cm/customers --header 'Content-Type: application/j
{
  "partnerId": "6e80b097-693c-4592-8440-02f345335bbf",
  "name": {
    "firstName": "John",
    "lastName": "Smith"
  },
  "classification": "Personal",
  "profile": {
    "regO": false,
    "politicallyExposedPerson": false,
    "taxIdType": "Ssn",
    "taxId": "119988776",
    "birthDate": "1953-09-22",
    "riskRating": "Low"
  "primaryAddress": {
    "addressType": "Home",
    "classification": "Residential",
    "isPrimary": true,
    "street1": "123 Any St",
    "city": "Anywhere",
    "state": "NY",
    "postalCode": "12345",
    "countryCode": "US"
  },
  "primaryPhone": {
    "isPrimary": true,
    "phoneType": "Home",
    "phoneNumber": "2015551234"
  },
  "primaryEmail": {
    "isPrimary": true,
    "emailType": "Personal",
    "emailAddress": "John.Smith@xxxxx.com"
  }
}
```

A successful API call returns a JSON response with the unique customer ID in the first line of the response body. Your customer has been created.

Onboarding a customer response body

```json
{
  "id": "9052b6a5-3f09-41d1-b526-ade80104eb79",
  "cifNumber": "32653745014",
  "classification": "Personal",
  "status": "Active",
  "ofac": "Pending",
  "pepScan": "Pending",
  "name": {
    "firstName": "John",
    "lastName": "Smith",
    "fullName": "John Smith"
  },
  "profile": {
    "regO": false,
    "politicallyExposedPerson": false,
    "enableBackupWithholding": false,
    "taxIdType": "Ssn",
    "taxId": "119988776",
    "birthDate": "1953-09-22",
    "riskRating": "Low"
  },
  "createdAt": "2021-01-25T17:55:24.4422582-05:00",
  "lastModifiedAt": "2021-01-25T17:55:24.4432543-05:00",
  "partnerId": "6e80b097-693c-4592-8440-02f345335bbf"
}
```

2. The `Core.Customer.Onboarded` webhook event is triggered when the customer record is created.

Customer onboarded event

```json
{
  "id": "3d9c5e1a-623b-4cf2-812e-ade80105048e",
  "eventName": "Core.Customer.Onboarded",
  "status": "Pending",
  "partnerId": "30dee145-b6a2-4058-8dc3-ac4000dee91f",
  "createdAt": "2021-11-22T10:50:20.553-05:00",
  "resources": [
    "core/v1/cm/customers/9052b6a5-3f09-41d1-b526-ade80104eb79"
  ],
  "details": []
}
```

Cross River scans the new customer record for OFAC and PEP compliance.

> Sometimes the results of the scan require a review by the our Anti-Money Laundering (AML) team.

On scan completion, `Core.Customer.Ofac.Changed` and `Core.Customer.PepScan.Changed` webhook events return with a status. Customers with no compliance issues show a `Clear` status.

Customer OFAC scan changed

```json
{
  "id": "45db5592-56ee-41f5-85e7-ade8010571ce",
  "eventName": "Core.Customer.Ofac.Changed",
  "status": "Pending",
  "partnerId": "30dee145-b6a2-4058-8dc3-ac4000dee91f",
  "createdAt": "2021-11-22T10:51:53.657-05:00",
  "resources": [
    "core/v1/cm/customers/9052b6a5-3f09-41d1-b526-ade80104eb79"
  ],
  "details": []
}
```

Customer PEP scan changed

```json
{
  "id": "a5000831-3e01-4231-9ec2-ade8010571c5",
  "eventName": "Core.Customer.PepScan.Changed",
  "status": "Pending",
  "partnerId": "30dee145-b6a2-4058-8dc3-ac4000dee91f",
  "createdAt": "2021-11-22T10:51:53.597-05:00",
  "resources": [
    "core/v1/cm/customers/9052b6a5-3f09-41d1-b526-ade80104eb79"
  ],
  "details": []
}
```

You have now created a customer record.

Update customer record

It is possible to update the customer details such as address, phone number and email. These details are considered *primary* information. If you add a second address, this is *secondary*.

1. Use the customer ID returned when you create the customer record to call `POST` `/core/v1/cm/customers/{id}/addresses` to add the **customer address**. The first address you add is the *primary* address. In the following example you can see which attributes are required.

Update customer address

```
POST /core/v1/cm/customers/9052b6a5-3f09-41d1-b526-ade80104eb79/addresse
{
  "addressType": "Home",
  "classification": "Residential",
  "isPrimary": true,
  "street1": "123 Any St",
  "city": "Anywhere",
  "state": "NY",
  "postalCode": "12345",
  "countryCode": "US"
}
```

2 Call `POST /core/v1/cm/customers/{id}/phones` to add the **customer phone number**. The first phone number you add is the *primary* phone number.

Update customer phone number

```
POST /core/v1/cm/customers/9052b6a5-3f09-41d1-b526-ade80104eb79/phones
{
  "isPrimary": true,
  "phoneType": "Mobile",
  "phoneNumber": "2015552345"
}
```

3 Call `POST /core/v1/cm/customers/{id}/email` to update the **customer email**.

Update customer email

```
POST /core/v1/cm/customers/9052b6a5-3f09-41d1-b526-ade80104eb79/email
{
  "isPrimary": true,
  "emailType": "Personal",
  "emailAddress": "john.jones@xxx.com"
}
```

Create a deposit account

CR provides a number of different types of accounts, including check and savings, Certificates of Deposit (CDs or time deposit accounts), and more.

To open any kind of deposit account you must have a valid product ID for the type of account you want to open, and a customer ID (onboarded customer record ID) for the account holder. Note that the account holder must have at least one address and phone number in their customer record, and their OFAC status must be *Clear*. In addition, the classification of the customer must match the configured classification for the product. For example, only business customers can be added to a business product.

Before you begin

Make sure you have:

- **API credentials**
- Partner ID (that you received when you registered)
- **Customer ID**
- **Product ID** (defines the type of account being opened)

> **IMPORTANT**
> We strongly recommend that you include an **idempotency key** in the request header to prevent duplicate payments in case of a failure.

Endpoints and webhooks

The following API endpoint is used:

API	Description
Open a deposit account	Opens a deposit account for a customer

The following webhook is used:

Webhook	Description
`Core.Account.Opened`	A new account was opened

Open an account

In the following scenario, you'll open an account for John Smith, a customer who you successfully onboarded.

To open an account

1. Call `POST core/v1/dda/accounts` .For this call, some attributes are required. See the full **list of attributes**.

   📦 Sample request

   ```
   POST /core/v1/dda/accounts
   {
     "customerId": "59e3bc15-bbec-4990-88e9-a9a600d3296c",
     "productId": "44015e68-1afb-40fc-9497-abc1014f52da",
     "title": "John Smith",
     "statementAddress": {
       "street1": "257 Dalton Groves",
       "city": "Barton City",
       "state": "MI",
       "postalCode": "48705",
       "countryCode": "US"
     }
   }
   ```

2. A successful API call returns a JSON response with the details of the new account.

```
Sample response                                                    ⎘

  POST /core/v1/dda/accounts
  {
     "customerId": "59e3bc15-bbec-4990-88e9-a9a600d3296c",
     "productId": "44015e68-1afb-40fc-9497-abc1014f52da",
     "title": "John Smith",
     "statementAddress": {
       "street1": "257 Dalton Groves",
       "city": "Barton City",
       "state": "MI",
       "postalCode": "48705",
       "countryCode": "US"
     }
  }
```

3   The `accountNumber` field provides the account number for the new account.

4   In the response example, the account is classified as `Personal` because the user
    configured the product classification as **Personal**. The account classification always
    matches the configured product classification.

5   The account status is automatically updated to `Active`, and is immediately available
    for use. This triggers the `Core.Account.Opened` event.

```
Core.Account.Opened Event Details                                  ⎘

  {
     "id": "259cdbca-6a89-4af8-a50e-ada3010fb13f",
     "eventName": "Core.Account.Opened",
     "status": "Pending",
     "partnerId": "e6c3824a-377f-44d5-a2f6-a9a600c9b37e",
     "createdAt": "2021-01-26T09:48:10.1011462-05:00",
     "resources": [
       "core/v1/dda/accounts/2235223803"
     ],
     "details": []
  }
```

Fund an account

When you work in the sandbox to test payment rails and account behavior you need to have funds in an account.

You can use any rail that has an inbound simulation endpoint to fund a sandbox account, if the account is configured for it. In particular, you can:

- **Simulate inbound ACH payments**
- **Simulate an inbound wire**

For any simulation, you need the number of the Cross River sandbox account that you want to fund. The originator information is not important, and in some cases can even be completely fictitious.

Next Steps

Check out our payment **tutorials**.

Cards

Step 1

Get API credentials

Step 2

Get Access Token

Step 3

Use Access Token

Step 4

Build a Sample App
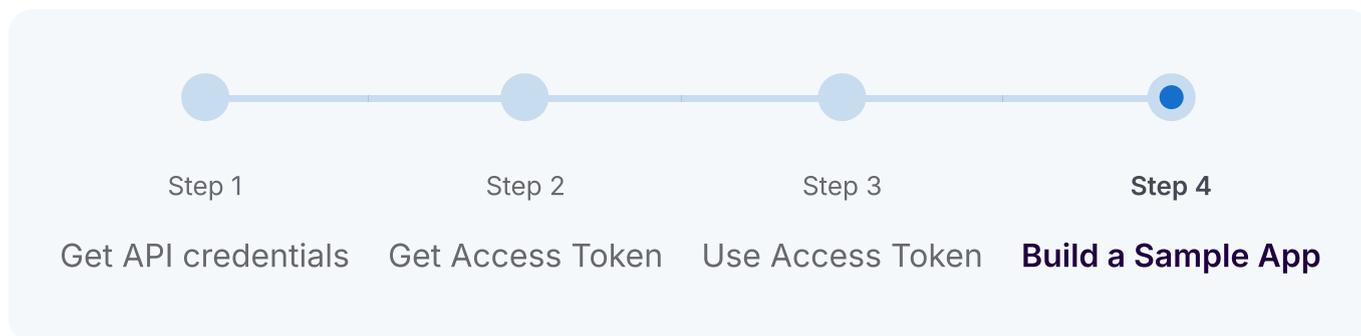
Get to know how to work with Cross River APIs. This page shows you how to:

- **Create** a card

- **Activate** a card

Create a card

Manage your customer's cards by working with Cross River to decide what you want to offer, such as physical or virtual cards. This is the *card configuration*. Cross River creates a card configuration profile for you for each <u>financial instrument</u> type you choose for your customers.

Before you begin

Make sure you do and have:

- **Create a customer record**

- **Create a deposit account**

- Cardholder's account number

- Customer ID (you get this when you create a customer)

- Configuration ID (Cross River provides ID to you when you configure your type/card)

We also recommend that you **register** for the relevant webhook events.

Endpoints and webhooks

Register for webhooks. The following API endpoints are used:

API	Description
Create new card	Requests creation of a new debit card

The following webhooks are used:

Webhook	Description
`Cards.Card.Created`	Debit card created

Order a card

You will learn how to order/create a new debit card. by creating a card for John Smith.

1.   Call `POST /cardmanagement/v1/cards`.

   In the following example you can see which attributes are required. See details of the complete **Add card** API.

```
curl -X POST /cardmanagement/v1/cards --header 'Content-Type: applicatio
    "accountNumber": "2608927303", \
    "customerId": "2b15a695-13dc-4b10-b4e5-af5b0138873c", \
    "configurationId": "a6b5a94c-f8f9-462b-8ce8-afa400f5b640", \
    "firstName": "John", \
    "lastName": "Smith", \
      "phone": { \
      "phoneType": "Home", \
      "phoneNumber": "9133413131" \
    }, \
    "emailAddress": "John.Smith@xxxxx.com", \
    "shippingAddress": { \
      "street1": "Lane Ave", \
      "street2": "string", \
      "city": "Big Town", \
      "state": "IL", \
      "postalCode": "72410", \
      "countryCode": "US" \
    }, \
    "billingAddress": { \
      "street1": "Lane Ave", \
      "street2": "string", \
      "city": "Big Town", \
      "state": "IL", \
      "postalCode": "72410", \
      "countryCode": "US" \
    }, \
    "nameOnCard": "John Smith", \
      "shippingType": "Normal", \
    "clientIdentifier": "string" \
}' 'https://sandbox.crbcos.com/CardManagement/v1/cards'
```

2 A successful API call returns a JSON response with the details of the new card. The card status will be unactivated until you activate the card. The id is the card ID, in this example **8709163d-140c-4d95-a111-afa8009e9cd1**, which you will need to **activate the card**.

Sample order a card response

```json
{
  "id": "8709163d-140c-4d95-a111-afa8009e9cd1",
  "partnerId": "cd9c12f4-7691-424a-b38b-af5b0134c611",
  "productId": "83bed086-8182-4151-a1e3-af5b01362783",
  "accountNumber": "2608927303",
  "status": "Unactivated",
  "statusReasonCode": "NotSet",
  "firstName": "John",
  "lastName": "Smith",
  "shippingAddress": {
    "street1": "Lane Ave",
    "street2": "string",
    "city": "Big Town",
    "state": "IL",
    "postalCode": "72410",
    "countryCode": "US"
  },
  "billingAddress": {
    "street1": "Lane Ave",
    "street2": "string",
    "city": "Big Town",
    "state": "IL",
    "postalCode": "72410",
    "countryCode": "US"
  },
  "phone": {
    "phoneType": "Home",
    "phoneNumber": "9133413131"
  },
  "emailAddress": "john@anygoogle.com",
  "nameOnCard": "John Smith",
  "isPinSet": false,
  "adminBlocked": false,
  "fraudSuspect": false,
  "configurationId": "a6b5a94c-f8f9-462b-8ce8-afa400f5b640",
  "category": "Credit",
  "paymentInstrument": "VirtualPan",
  "processor": "processor name",
  "shippingType": "Normal",
  "orderStatus": "OrderPending",
  "replacementStatus": "NotApplicable",
  "customerId": "2b15a695-13dc-4b10-b4e5-af5b0138873c",
  "clientIdentifier": "string",
  "createdAt": "2023-02-13T04:37:29.4869172-05:00",
```

```
      "lastModifiedAt": "2023-02-13T04:37:29.4869172-05:00"
```

3. The `Cards.Card.created` webhook event is triggered when the card is generated at the processor.

Sample Cards.Card.Created event

```
{
  "id": "cea6c5b5-13e7-4c2f-ba75-afce01110fe5",
  "eventName": "Cards.Card.Created",
  "status": "Pending",
  "partnerId": "cd9c12f4-7691-424a-b38b-af5b0134c611",
  "createdAt": "2023-02-13T04:42:29.4869172-05:00",
  "resources": [
    "cardmanagement/v1/cards/8709163d-140c-4d95-a111-afa8009e9cd1"
  ],
  "details": [
    {
      "cardId": "8709163d-140c-4d95-a111-afa8009e9cd1",
      "status": "Unactivated",
      "statusReasonCode": "NotSet"
    }
  ]
}
```

Activate the card

Before you begin

Make sure you have:

- **API credentials**
- Card ID from when you **ordered the card**

Endpoints and webhooks

API	Description
POST /cardmanagement/v1/cards/{id}/activate	Activates the card using the card ID

The tutorial uses these webhooks:

Webhook	Description
`Cards.Card.Activated`	Debit card activated

Activate the card

Activate the card you created in the **create a card** stage.

1. Call `POST /cardmanagement/v1/cards/{id}/activate`. The `id` attribute must be set to the card ID. In the sample below the ID is **8709163d-140c-4d95-a111-afa8009e9cd1**.

   📦 Sample activate card request ⧉

   ```
   curl -X POST
   --header 'Accept: application/json'
   --header 'Authorization: Bearer '<token>'
   https://sandbox.crbcos.com/CardManagement/v1/cards/8709163d-140c-4d95-a1
   ```

2. A successful API call returns a JSON response with the details of the card. The card `status` is now **activated**. The `OrderStatus` is **Completed**.

Sample activate card response

```json
{
  "id": "8709163d-140c-4d95-a111-afa8009e9cd1",
  "partnerId": "cd9c12f4-7691-424a-b38b-af5b0134c611",
  "productId": "83bed086-8182-4151-a1e3-af5b01362783",
  "processorCardId": "804951250206718",
  "accountNumber": "2608927303",
  "status": "Active",
  "statusReasonCode": "NotSet",
  "firstName": "John",
  "lastName": "Smith",
  "shippingAddress": {
    "street1": "Lane Ave",
    "street2": "string",
    "city": "Big Town",
    "state": "IL",
    "postalCode": "72410",
    "countryCode": "US"
  },
  "billingAddress": {
    "street1": "Lane Ave",
    "street2": "string",
    "city": "Big Town",
    "state": "IL",
    "postalCode": "72410",
    "countryCode": "US"
  },
  "phone": {
    "phoneType": "Home",
    "phoneNumber": "9133413131"
  },
  "emailAddress": "john@anygoogle.com",
  "nameOnCard": "John Smith",
  "panLastFour": "3629",
  "isPinSet": false,
  "expirationDate": "2026-02-13",
  "adminBlocked": false,
  "fraudSuspect": false,
  "configurationId": "a6b5a94c-f8f9-462b-8ce8-afa400f5b640",
  "category": "Credit",
  "paymentInstrument": "VirtualPan",
  "processor": "processor name",
  "shippingType": "Normal",
  "orderStatus": "Completed",
  "replacementStatus": "NotApplicable",
  "customerId": "2b15a695-13dc-4b10-b4e5-af5b0138873c",
```

```
      "clientIdentifier": "string",
      "processorCustomerId": "T83E9D675A3N3N9O8RZ1",
      "createdAt": "2023-02-13T04:37:29.487-05:00",
      "initialActivation": "2023-02-13T00:00:00-05:00",
      "activatedAt": "2023-02-13T04:43:19.282287-05:00",
      "lastModifiedAt": "2023-02-13T04:43:19.2962845-05:00"
  }
```

3   When the card status changes to `Active`, the `Cards.Card.Activated` webhook event fires.

Cards.Card.Activated webhook event

```
  {
    "id": "95ac33ca-3d7f-49aa-bfc2-afce01113310",
    "eventName": "Cards.Card.Activated",
    "status": "Pending",
    "partnerId": "cd9c12f4-7691-424a-b38b-af5b0134c611",
    "createdAt": "2023-02-13T04:44:31.282287-05:00",
    "resources": [
      "cardmanagement/v1/cards/8709163d-140c-4d95-a111-afa8009e9cd1"
    ],
    "details": [
      {
        "cardId": "8709163d-140c-4d95-a111-afa8009e9cd1",
        "status": "Active",
        "statusReasonCode": "NotSet"
      }
    ]
  }
```

3.4. Lending

Step 1 — Get API credentials
Step 2 — Get Access Token
Step 3 — Use Access Token
Step 4 — **Build a Sample App**
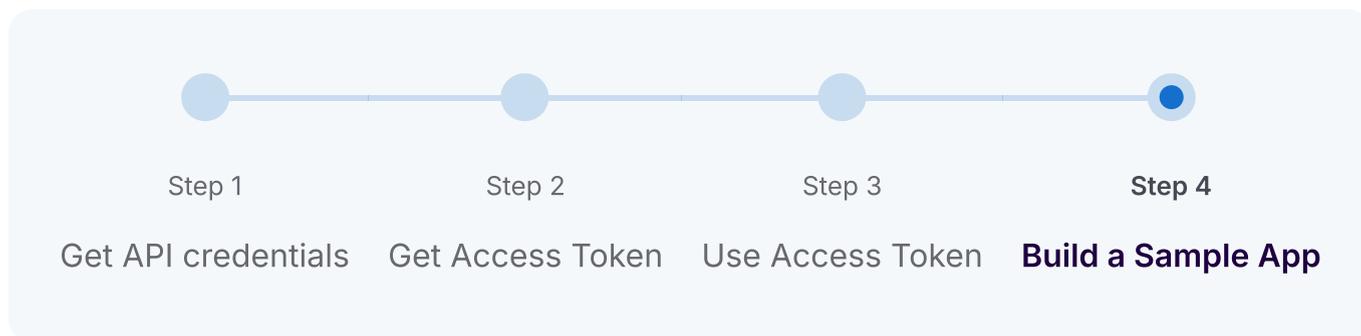
Lending includes a set of **lending API** calls to allow you to create, update, and manage your loans.

To start working with lending, make sure you:

- Receive API credentials with the scopes needed for Lending
  - If you have created the API Credentials, using the self-service **Org Management**, then you should also send a request to **arix.support@crossriver.com**, along with your clientid and MPLID, to complete the creation.
- Use the correct scope, for the APIs you want to use.
  - API scope for sandbox is: CosLending:PreApproval:stg

Sandbox

Module	Base URL for API calls	Description
Loan origination	https://arixapisandbox.crbnj.net	The base URL for loan origination API calls to the Arix sandbox environment
Application decisioning	https://lendingsandbox.crbcos.com/preapproval/v1	The base URL for sandbox of application decisioning

Swagger

Module	Swagger Link
API reference documentation	**https://arixapisandbox.crbnj.net/swagger-ui**
Hooks	**https://lendingsandbox.crbcos.com/hooks/swagger/index.html**
Selling	**https://lendingsandbox.crbcos.com/selling/swagger/index.html**

Status Page

To see a list of upcoming releases, monitor current API status, view incident reports, or get notified of scheduled maintenance, visit our **status page** and subscribe to alerts.

4. Program setup

- **Set up SFTP**: Use SFTP either to send files or to download them from Cross River, according to your needs and ours.

- **Customer onboarding**: Manage your customer information in the Cross River operating system (COS) using either APIs or COS explorer
  - **COS product types and IDs**: Explaining COS product types and IDs.

  - **COS Explorer**: How to work with our COS Explorer.

  - **Org management portal**: How to work with our Org management portal.

Set up SFTP

When you need to exchange sensitive information in a file format with Cross River, we require you to use Secure File Transfer Protocol (SFTP). Use SFTP either to send files or to download them from Cross River, according to your needs and ours. In some cases, you or we will encrypt these files, particularly if they contain any Personal Identifying Information (PII).

Using SFTP

SFTP lets you securely send and receive sensitive files and reports using a folder assigned specifically to your business on a secure server. Upload and download files through that folder or subfolders of that folder, as per your specific needs.

Using encryption

Encrypting files adds an additional layer of protection. Only authorized personnel with the correct key will be able to decrypt the encrypted file. In Cross River we use PGP encryption.

Get started

There are several steps to getting you up and running with our SFTP server.

1 **You complete the IP Access Request for Cross River SFTP Services form (from your RM).**
If you need to share files with Cross River, your Relationship Manager will send you an IP Access Request for CRB SFTP Services form. Among other information, you need to provide the static public IP addresses you'll use to access the SFTP folder, and a PGP public key for encrypting and decrypting files. Send the completed form back to your Relationship Manager

> **IMPORTANT**
>
> Cross River will allowlist only 5 IP addresses for you, so take that into account. The IP addresses must be static. Therefore, you need to proxy anything that is not static on your end.

2 **We set up your SFTP folder structure.**

Once Cross River has your details, our IT engineering department creates a standard set of folders and sub-folders for you. This unique path is for your business only. No other partner can access it. IT engineering sends you an email with the information you need to access the folders. The email includes a link to your credentials. Cross River does not save your password!

> **IMPORTANT**
>
> The link is only good for a few days, after which you'll need to request a password reset if you don't use it.
> The credentials also become invalid if more than two people access the link.

3 **Test SFTP upload.**

If you will be supplying files to Cross River, your IT department should set up a service account with an automated process for uploading those files to your SFTP folders. We strongly recommend that you test this out before you try to send real data. Contact your relationship manager with any questions or issues or open a ticket with your first line support.

4 **Set up PGP to send or receive files from Cross River. (This step is only necessary if you are sending or receiving PII. Please check with your RM.)**

If you need to send Cross River files, we will first send you our PGP public key for use in encrypting those files.

You should have already sent Cross River your PGP public key to receive files from us.

5   **Share your data.**

Once your SFTP folder is set up and your process is in place you can begin sharing files with us. Your relationship manager tells you if there is something more specific you need to do to receive reports, or how to prepare data to send to us.

Specific Reports

Learn more about preparing and sending reports and files for:

- **Accounts and payments**
- **Card payments**
- **Credit risk**
- **Lending**
- **XML batch payments (ISO 20022)**

4.2. Customer onboarding

Manage your customer information in the Cross River operating system (COS) using either APIs or **COS Explorer**. This information includes basic details needed to open a bank account or use a credit card, as well as more specific data about the customer, as needed. We call this a *customer record*.

Before you can open a deposit account or create a card you must create the customer record, sometimes called *onboarding*. You can then assign one or more customers to an account through customer *relationships*.

The customer onboarding process includes creating a **customer record** with relevant customer information. Follow this tutorial to **create a customer record** for each of your customers.

Optional steps

- **Add ID details**
- **Add a beneficial owner**

Error codes

See **COS system error codes**, along with lots of other reference information, on the COS reference codes page.

Customer record

Customer record

The customer record is the primary resource containing customer information in the Cross River system. Therefore, before creating an account for a customer, you must onboard that customer. The customer record supports classifications of type Personal or Business. Once onboarded, you can associate a customer with one or more accounts.

The example below shows how to **onboard a customer** for a personal customer.

```
POST /core/v1/cm/customers
{
  "partnerId": "7cc038be-fde9-4455-b27b-1497cf667362",
  "name": {
    "prefix": "Mr.",
    "firstName": "John",
    "middleName": "Robert",
    "lastName": "Smith",
    "suffix": "Jr.",
    "preferredName": "Jim"
  },
  "classification": "Personal",
  "profile": {
    "regO": false,
    "citizenshipCountryCode": "US",
    "politicallyExposedPerson": false,
    "enableBackupWithholding": false,
    "backupWithholdingPercent": 0,
    "taxIdType": "Ssn",
    "taxId": "123456789",
    "birthDate": "1965-09-15",
    "riskRating": "Low",
    "privacyOptOut": true
  }
}
```

Onboard a business customer such as corporation or LLC using the same endpoint with slightly different attributes.

```
POST /core/v1/cm/customers
{
  "partnerId": "a24cba49-2bb6-431d-a867-1de81d6e4127",
  "name": {
    "entityName": "ACME CO",
  },
  "classification": "Business",
  "profile": {
    "citizenshipCountryCode": "US",
    "enableBackupWithholding": false,
    "backupWithholdingPercent": 0,
    "taxIdType": "Ein",
    "taxId": "123456789",
    "dateFormed": "2019-09-10",
    "entityType": "Corporation",
    "riskRating": "Low",
    "ownershipType": "LegalEntity",
    "primaryOwnerCustomerId": "f9321f7f-3712-46e1-b965-2b79ead64dc9",
  }
}
```

Regardless of whether you are onboarding a personal or business customer, the `primaryOwnerCustomerId` attribute must contain a customer ID referencing a customer record of type Personal. So to onboard a business, you must first create a personal customer record for the primary owner of that business.

> **IMPORTANT**
>
> Some customer endpoints include a `dueDiligence` resource that may or may not be required when onboarding personal customers. Your assigned compliance liaison communicates requirements for any Due Diligence fields during your onboarding process.

Beneficial owners

A beneficial owner is a person who owns 25% or more of a business. For regulatory reasons, you need to **create a beneficial owner** resource in a *Business* customer record for each beneficial owner of that business. The `ownerCustomerId` attribute references the Personal customer record for each beneficial owner. You usually add beneficial owner resources to the business customer record immediately after onboarding a business.

```
Curl

POST /core/v1/cm/customers/{customerId}/beneficial-owners
{
   "ownerCustomerId": "c1210a2d-932e-43ca-be29-f358a4382385",
   "ownerTitle": "President"
}
```

Address

The physical addresses associated with customer can be **updated**.

```
Curl

POST /core/v1/cm/customers/{customerId}/addresses
{
  "isPrimary": true,
  "status": "Active",
  "classification": "Residential",
  "addressType": "Home",
  "street1": "123 Maple Street",
  "street2": "Apt. 12",
  "street3": "",
  "city": "New York",
  "state": "NY",
  "postalCode": "10025",
  "countryCode": "US",
}
```

Email addresses

Update email contact information for customer.

```
Curl

POST /core/v1/cm/customers/{customerId}/emails
{
  "isPrimary": true,
  "emailType": "Personal",
  "emailAddress": "john.smith@crossriver.com"
}
```

Phones

Update phone contact information for customer.

```
Curl

POST /core/v1/cm/customers/{customerId}/phones
{
  "phoneType": "Home",
  "isPrimary": true,
  "phoneNumber": "2015551234"
}
```

Identifications

Identifications are used to track metadata for customer-identifying documents such as driver's licenses and passports. **Add ID details** can be used to add new ID details.

```
Curl

POST /core/v1/cm/customers/{customerId}/identifications
{
  "isPrimary": true,
  "idNumber": "DL123456789",
  "idType": "DriversLicense",
  "issuedDate": "2018-08-30",
  "expDate": "2018-08-30",
  "verifiedDate": "2018-08-30",
  "issuingAuthority": "NJ DMV",
  "issuingStateOrProvince": "NJ",
  "issuingCountryCode": "US",
}
```

4.2.2. COS product types and IDs

In Cross River, a *product type* is a uniquely configured financial product you offer your customers. For example, a product type could be a debit card or a savings account, configured according to your needs and specifications. You open accounts for your customers under any product type you define and configure together with us. Speak to your relationship manager for more details, including how to set up product types for your customers.

For example, you might want to configure a product type to be a savings account product that uses Wires and ACH payments. You can then offer your customers savings accounts with these services and configurations.

Cross River provides you with a product ID for each product type that you want to offer your customers. To open any kind of deposit account you must have a valid product ID and a customer ID (onboarded customer record ID) for the account holder. Note that the account holder must have at least one address and phone number in their customer record, and their OFAC status must be *Clear*. In addition, the classification of the customer must match the configured classification for the product. For example, only business customers can be added to a business product.

COS Explorer

Once you are **onboarded** into the Cross River system and have received the email with your *Client ID* and *Secret* you are ready to login to the COS Explorer.

Access the COS Explorer portal

Production: **https://api.crbcos.com/explorer2/**

Sandbox: https://sandbox.crbcos.com/explorer2/

Welcome email

You will received a welcome email from *CrossRiver_DO_NOT_REPLY@crossriver.com*. If you don't see it in your inbox, check your spam or blocked mail folders.

Click **Create your Cross River Account**.
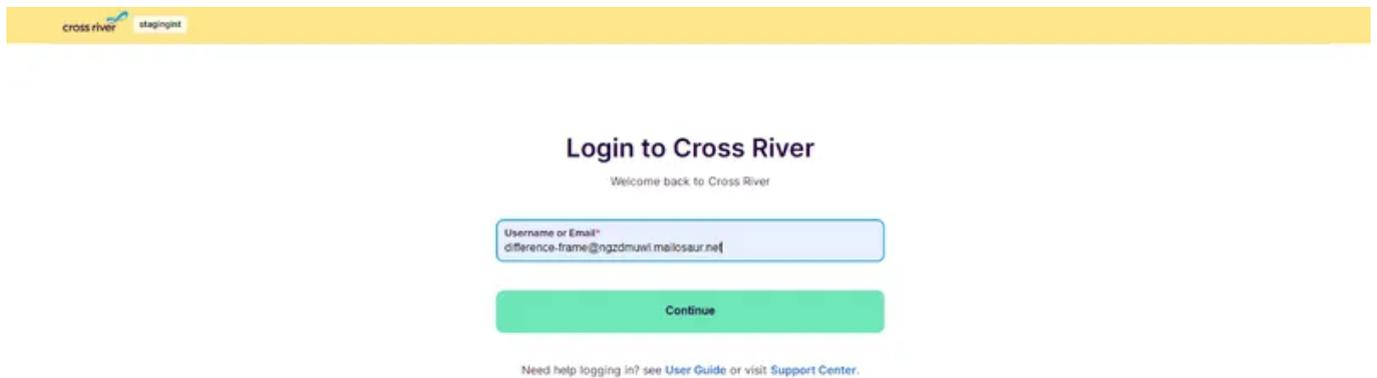
If you leave the wizard at any time, click the link in the original email to go back to where you left off.

Terms and conditions

Read through the terms and conditions, check **Accept**, and click **Next**.

SMS (text message) verification

We send you an SMS (text message) to your device to verify your identity. Enter the 6-digit code you receive in the login screen and click **Verify Code**.

Create your password

1. Enter a password that meets the on-screen requirements and re-enter the password.

2. Click **Create Password**.

Authenticator app setup

You must complete this step to continue the registration process and to be able to login in the future

To protect your identity and your account and information, we require you to sign in with multi-factor/2-factor authentication.

If you don't already have an authenticator app on your device, you need to download one before you continue.

For Android and iOS, we recommend using the follow authenticator app:

- Google Authenticator
- Microsoft Authenticator

Once you have your authenticator app installed, you need to either **scan the QR code** or **manually enter the key** into the authenticator app.
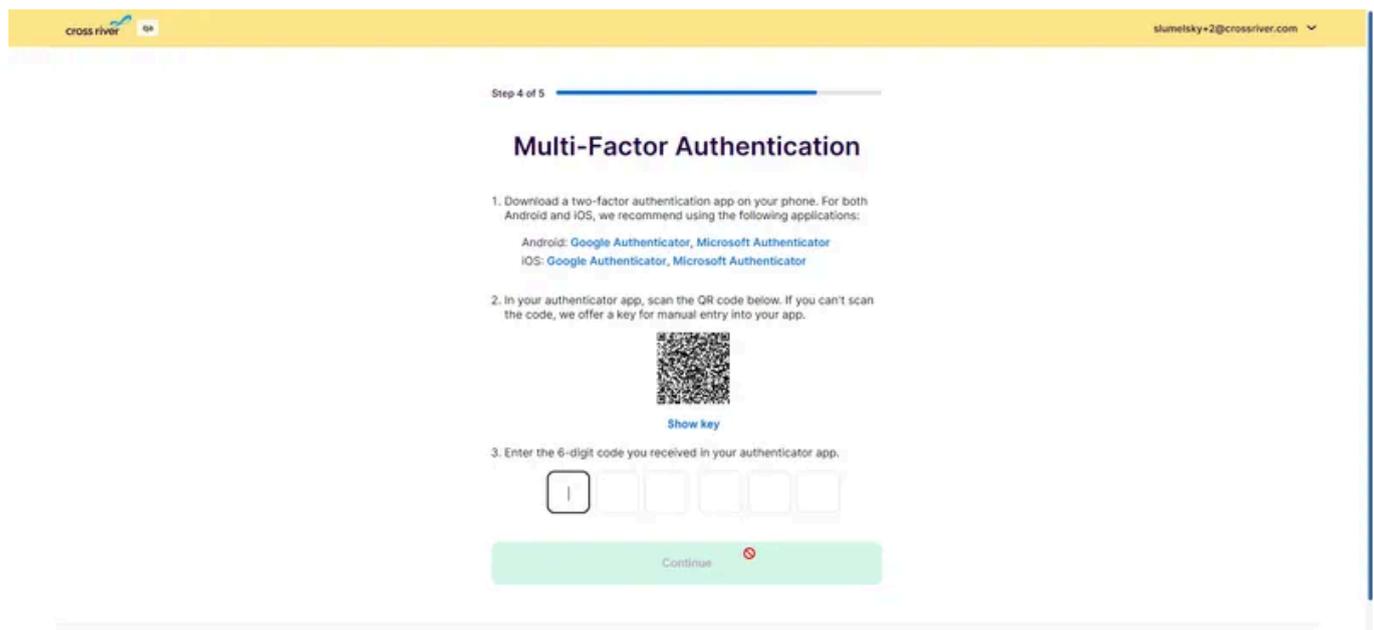
QR code

1. Scan the QR code in your authenticator app and, if necessary, enter the 6-digit code in the Multi-Factor authentication page.

2. Click continue.

Manual

1. Click **Show key**

2. Copy the key as the *Secret* in your authenticator app.

3. Enter the 6-digit code.

4. Click **Continue**.

Invalid MFA code

If you enter an invalid MFA code, a red message notifies you to try again.

Multi-Factor Authentication

1. If you don't already have one, download an authentication app on your device. For both Android and iOS, we recommend using the following applications:

   Android: **Google Authenticator, Microsoft Authenticator**
   iOS: **Google Authenticator, Microsoft Authenticator**

2. In your authenticator app, scan the QR code below. If you can't scan the code, we offer a key for manual entry into your app.

Show key

3. Enter the 6-digit code you received in your authenticator app.

| 1 | 1 | 1 | 1 | 1 | 1 |

Incorrect code, please try again

Continue

Oops! You entered an invalid MFA code. Here are some things to double check:

1. Did the code timeout before you clicked **Continue**? Remaining time is indicated by the countdown circle to the right of the account name and MFA code.
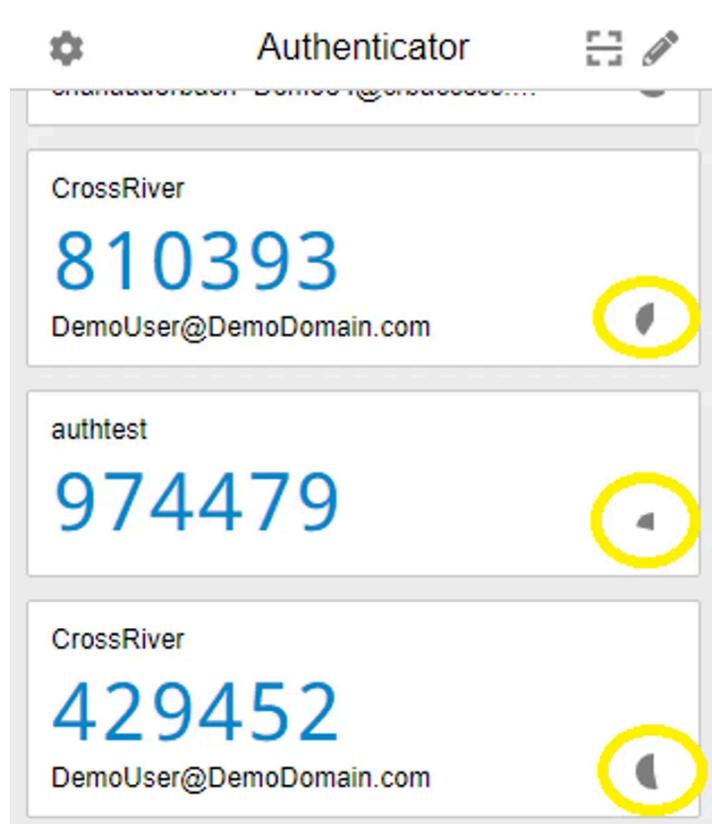
2. If you have the authenticator app set up for multiple environments or applications, double check that you entered the correct code.

   1. If it is not clear from the MFA connection names which is correct option, you might need to try different codes until finding the one that works.
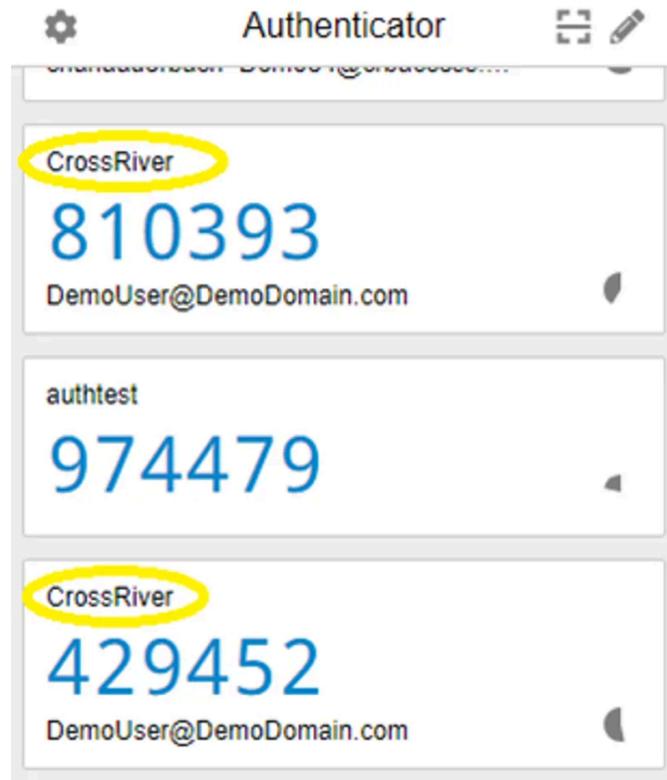
   2. Once you find the correct connection, you can rename the MFA connection in the app. A pencil icon at the top of MFA app screen will bring you to edit mode. In some apps, you will need to first select (or press and hold) the connection that should be edited, and then the icon will appear.
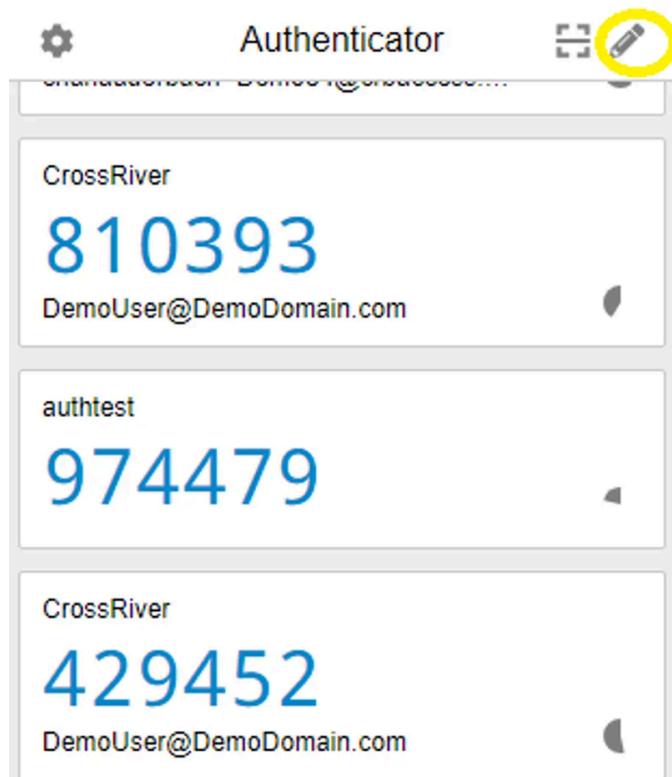
3. Once in edit mode, you can rename the connections as needed so that it will be clear which one applies to which environment.
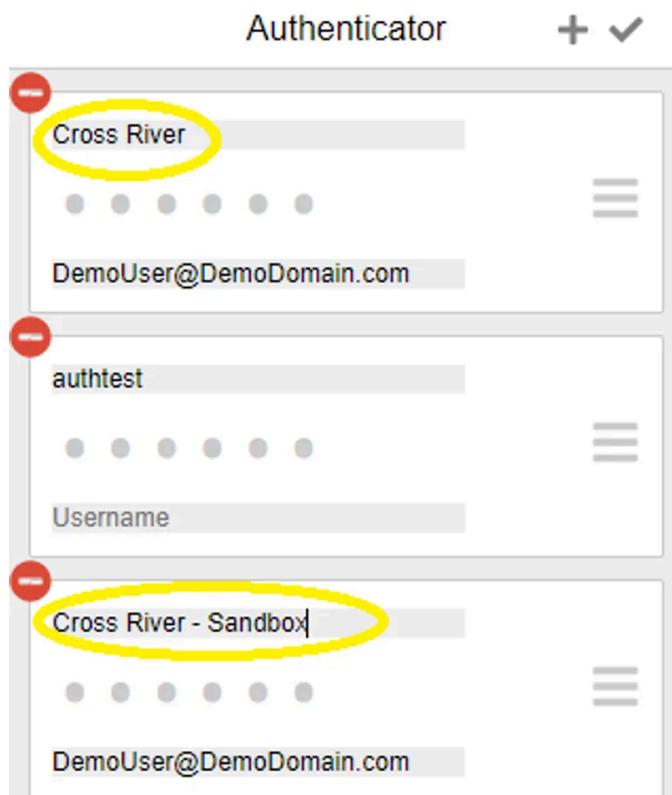
4. Save any changes, and next time it should be easier to understand which code to use.

Recovery codes

Use recovery codes to authenticate in case you lose your device.

1. Download or copy your recovery codes and keep them in a secure place that you will remember.
2. Confirm that you have stored your recovery codes
3. Click **Create account**.

The recovery codes page times out after 10 minutes.

You can only download the recovery codes once.
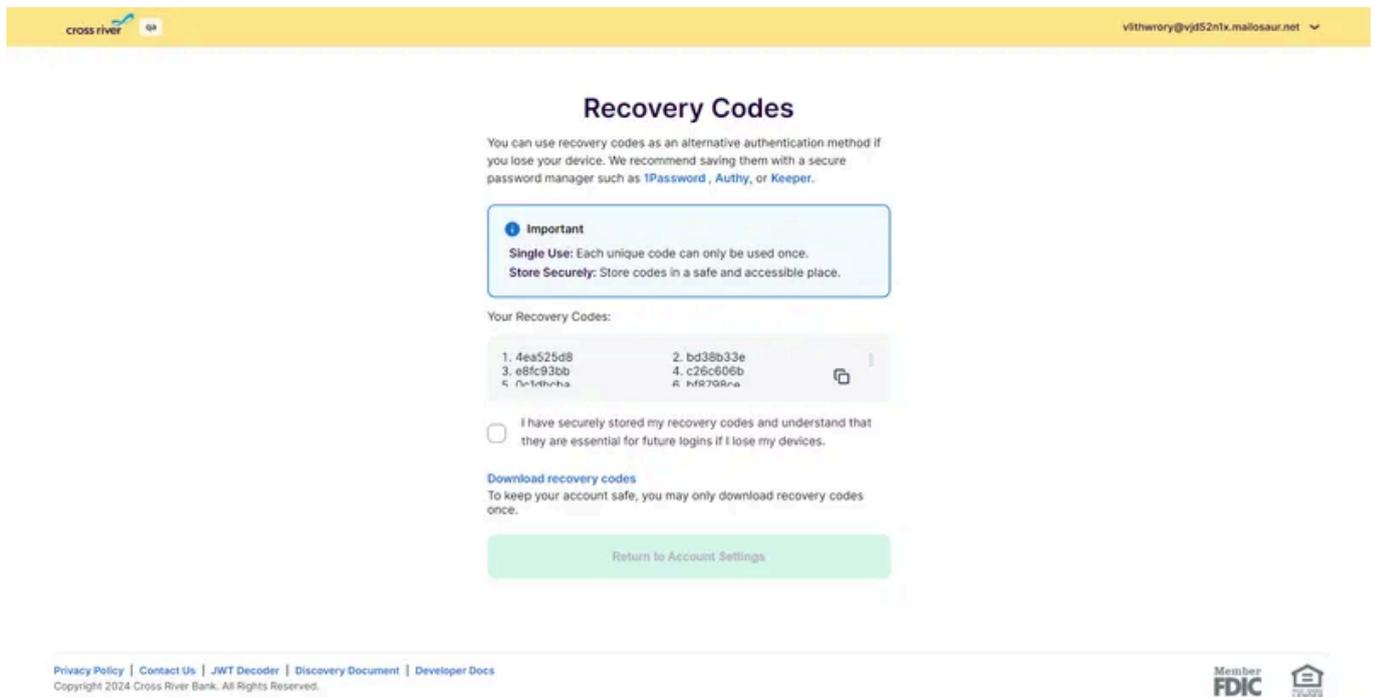
Your account is now active and you can use it to login to any of your CR apps.

IP allowlisting

Only a static IP can be used to access COS Explorer. Reach out to your IP Support if you need help with this.

The Identity Server IP addresses are:

- 172.67.26.222
- 104.22.40.134
- 104.22.41.134

The server is proxied via Cloudflare.

You can allow these FQDNs:

- idptest.crbcos.com

Troubleshooting

Forgot password

1. Click **Forgot password?** and enter your email.

2. Enter the 6-digit authentication code from your authenticator app.

3. You get a *Forgot Password* email. Click **Reset Password**.

4. In the Password Reset page, enter a new password, click **Reset Password**, and **Continue to the application**.

Reset multi-factor authentication

If you already have MFA configured:

1. In Identity Server, go to **Reset MFA** and click **Reset your MFA device**.

2. The Multi-Factor Authentication page opens and you can reset your MFA.

You can also create new multi-factor authentication recovery codes.

1. Click **create new multi-factor authentication recovery codes**.

2. The Recovery Codes page opens and you can copy or download your 10 new recovery codes.

If you have not yet configured your multi-factor authentication, you can enable MFA from **Account Settings**.

1. Click **Reset MFA Method**.

2. Click **Configure MFA**.

3. Follow the instruction in Multi-Factor Authentication/2-Step Authentication.

If your current MFA is SMS, you can enable MFA with your authenticator app.

In **Account Settings**

1. Click **Reset MFA Method**.

2. Click **Configure MFA**.

3. Follow the instruction in Multi-Factor Authentication/2-Step Authentication.

Use a recovery code

If you do not have access to your multi-factor (2-factor) authenticator, you can log in using one of your recovery codes.

1. Log in as usual

2. On the Multi-Factor Authentication page, you have the option to use a recovery code as your authentication option.

3. Enter one of your recovery codes in the text box. The recovery code is single-use and cannot be reused. To avoid future confusion, we recommend that you mark the recovery code as used.

← Multi-Factor Authentication

Log in with Recovery Code

Enter the recovery code provided during your account setup

Recovery Code

Login

Need help logging in? Visit our Support Center.

Privacy Policy | Support Center | JWT Decoder | Discovery Document | Developer Docs
Copyright 2023 Cross River Bank. All Rights Reserved.

Member FDIC

Account lockout

If you enter the wrong password for your username 5 times, the system locks your account for approximately 5 minutes. If after 5 minutes, you are still unable to access your account, contact Cross River Support.

Browser error - Firewall

You log in to COS Explorer and get following error screen:
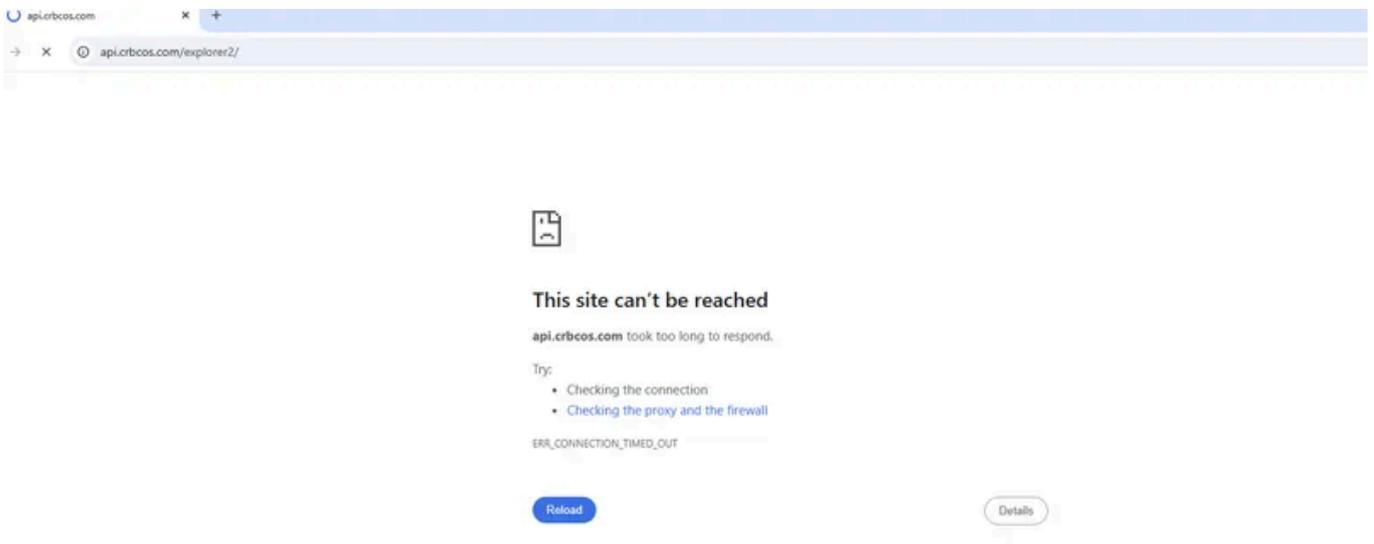
You are blocked by a firewall.

1. Contact your internal IT department to see if your organization enforces firewall rules for outbound traffic. If there are no firewall rules for outbound traffic, then:

2. Contact your internal IT department to make sure you're connecting to the Cross River COS Explorer Portal from an approved IP address. If you need to register more IP addresses, send an email to **COS support**.

4.2.3.1. User management

Managing users

You can use the **Users** screen of the **Admin** tab to group a set of resources, such as customers, products, and accounts. Once a resource (i.e. product or customer) has been assigned to a you, it cannot be changed.

You can use this area to support and make changes for your customers. We can set you up with 2 admin users so that you can create users on demand for your customers. This gives you independence to manage your customers and allows you to make changes out of hours, at their request.

You can also create or onboard new users.

⌄ Create a new user

1   In the **Admin** tab, click **Users** to open the **Users** search screen.

2   Click **+ New User**. The **Create User** screen displays.

3   In **Create User** enter the user's **Email**, the following fields then display **First Name**, **Last Name** and **Phone Number**.

4   Click **Status** and select **Active**.

> The **Phone Number** field must be a cellphone number as this will be used for MFA to authenticate the user.

Field	Description
Name	User name. Enter the full user name to display in the browser window when the user logs into Explorer.
Email	User email address. This address is used to log into Explorer and also serves as a recovery email for password resets.
Status	Select a user status. User status is **Inactive** by default. Change it to **Active** when creating a user.
User Type	This field displays **Partner** when the user is created.
Roles	Select the roles to add to the user, or click **Include All Roles** to add all available roles to the user. **Note:** Only the roles assigned to you will be visible. Some roles contain permissions which allow you to originate payments in Explorer. Your Explorer admins are responsible for making sure that your users are properly configured with only the appropriate user roles as well as authorized limits.
Authorized Limits	For each field , select a dollar limit (if applicable)

5   Click **Status** and select **Active**.

6   Click **Roles** and select the **roles** you want to assign the new user. Click **Save Changes**.

- *All* users must be configured with the **Partner Core Ready Only** role.

- If the user is assigned the **Partner Wire Origination** role you must configure that user's origination limit.

7 If you're assigning the user the **Partner Wire Origination** role, enter a value in the **Wire.Payments.Originate** field to indicate the maximum dollar limit per wire. Otherwise, you can ignore this field.

8 When you finish configuring all fields. Click **Save Changes.**

9 If you have successfully created a new user, a confirmation screen displays.

10 To complete the addition and configuration of a user, a different admin must **Approve Changes.**

User Id:	6615b1e52f1052d24e221bc1	6615b1e52f1052d24e221bc1
Name: *	Sample User	Sample User
Status: *	■ Inactive	■ Active
User Type:	Partner	Partner
Email:	user@emaildomain.com	user@emaildomain.com
Identity Provider ID:	54f85774-4266-4180-883e-2e606ac77eba	54f85774-4266-4180-883e-2e606ac77eba
Roles: *	Partner Core Read Only	Partner Core Read Only

11 The **Approve Pending Changes** screen displays. Click **Confirm**.

12

View user information

∨ Click a user name in the **Users** screen. The **User Details** screen displays.

User details

The main user information displays in the **User Details** area:

Field	Description
User ID	User ID generated by COS
Name	User name
Status	User status
User Type	This field always displays as **Partner** when the user is created.
Email	User's email address
Identity Provider ID	Unique ID automatically generated by COS third-party authentication vendor
Roles	List of roles assigned to the user
Authorized Limits	List of authorized limits assigned to the user per permission

Change user details

You can edit most of the user details using the 3-dot (More) menu in the **User Details** area.

To change user details:

Clickth 3-dot menu in the **User Details** area and select **Toggle Edit Mode**. Most of the fields become editable.

> Any changes made to the user configuration will need to be approved by another admin.

⌄ Search for users

Search for your users:

1   Go to **Admin** > **Users**.

2   **Search by Id** or click the filter icon and enter your search parameters:

Filter	Description
Name	User name
Type	User type (Internal/ Partner)
Status	User status (Active, Inactive or Any)
Partner	Partner name. You can click the magnifying glass to select one from the list.
Identity Provider	ID provided by the third-party authentication vendor
Has Changes	Yes, No, or Any

3   Click **Search**.

The search results display in the **Partners** list. Each row in the list represents an individual partner:

Column	Description
NAME	Partner name
STATUS	Partner status
TYPE	User type (Partner/ Internal)
ROLES	Number of roles assigned to user
PARTNERS	Number of partners accessible to user

User tasks

You can perform several tasks from the **User Tasks** area.

Search users

When you click **Search Users** in the **User Tasks** area, you return to the main **Users** screen.

View notes

To view and add notes on a user:

1 Click View Notes.

The **View Notes** dialog displays your saved notes:

Field	Description
DATE	Note creation date
SUBJECT	Note subject
AUDIENCE	Note audience (Internal /Partner)
CREATED BY	COS user who created the note
Body	Note text

You can click a note in the list to view the body of the note.

Add a note

1. Click **Add Note** in the **View Notes** dialog.

2. Enter the information in **Create New Note**.

3. Click **Submit**.
   The new note displays in the **View Notes** dialog. The notes are specifically for either an internal or external audience.

User roles

As a partner, there are user roles that you can assign when you **create a new user** in COS Explorer. Only the roles assigned to you will be visible.

Some roles contain permissions that allow you to originate payments in COS Explorer. Your Explorer admins are responsible for making sure that your users are properly configured with only the appropriate user roles, as well as authorized limits.

Values for user roles

Value	Description
Partner Core Read Only	Read-only access across all domains (for example, Core, ACH, Wires)
Partner Core Admin	Add/edit users. All admin actions are dual-control enforced and must be approved by another admin.
Partner Core Onboarding	Perform all functions related to onboarding customers: • Create new customers • Edit existing customers details, including PII • Open/edit/close accounts • Create book transfers • Add/removed account restrictions • CSR functions, such as placing stop payments or downloading statements
Partner Sub Ledger	Manage subledgers: • Open/edit/close subledgers • Add/edit beneficiary profiles of subledgers • Add/edit subledger account tiles • Add/remove restrictions
Partner Book Transfers	Move funds between any two accounts
Partner ACH Origination	Originate ACH payments: • Cancel payments • Bulk cancel payments (API only) • View payment information • Originate client batches (API only)
Partner Wire Origination	Originate wire payments: • Cancel payments • View payment information • Reverse inbound wire payments

Value	Description
	• View ABA routing directory information
Partner Wire Callback Approver	Approval via telephone callback for wires up to and including this limit
Partner Wire Origination Limit	The maximum dollar amount that can be originated by the user per wire.

Managing customers

Manage your customers from the **Customers** screen in the **Core** tab.

Searching for customers

1. Go to **Core** > **Customers**.

2. **Search by Id** or click the filter icon and enter your search parameters:

Filter	Description
Search By Id	Customer ID or search
Partner	Partner name or search
CIF #	Customer Identification File Number
Tax ID	Tax ID number
Classification	Classification (Business, Personal, or Any)
OFAC	OFAC status
PEP	Politically Exposed Person status
From	Start date for search period
To	End date for search period
Client Identif	Use this attribute to add your own unique identifying string to a payment call or COS record. This attribute is useful for **idempotency purposes** .

3. Click **Search**.

   The search results display in the **Customer Management** list. Each row in the list shows an individual customer.

Column	Description
NAME	Customer name
STATUS	Customer status in COS
OFAC	Customer OFAC status
PEP	Customer PEP status
CIF #	The Customer Identification File Number
TAX ID	Customer tax ID number
CLASSIFICATION	Customer classification (Business / Personal)
PARTNER	Customer partner name
CREATED	Customer creation date in COS

Onboarding a customer

When you onboard a customer, you might be able to add some customer records later depending on your agreement with Cross River.

To onboard a customer:

1. In the **Core** tab, click **Customers** to open the Customer search screen.

2. Click **Onboard Customer**.

3. In the Onboard Customer screen fill in the new customer details.

Field	Description
Partner	Enter your partner name or select it from the list
Classification	Customer classification:

Personal

Customer Name

- `Prefix` - Prefix
- `First` -Customer first name
- `Middle` -Customer middle name
- `Last` -Customer last name
- `Suffix` -Suffix
- `Preferred Name` -Customer preferred name

Customer Profile

- `Tax ID` Type-Customer tax ID type
- `Tax ID` -Customer tax ID number
- `DOB` -Date of birth
- `Reg O` -Pertains to loans issued to executive officers, directors, and principal shareholders of member banks
- `Backup Withholding` -Enable to allow withholdingtaxes on interest earned
- `Backup Withholding %` -If Backup Withholding is enabled, enter a percentage to withhold taxes on interest earned
- `PEP` -Enabled when customer is a politically exposed person (PEP)
- `Risk` -Customer/business risk classification

Field	Description

- `Citizenship` -Customer/business entity country of citizenship
- `Privacy Opt Out` -Indicates whether the customer opts out of information sharing
- `Parent Entity` -Enter or search for Parent entity

Due Diligence

- `Employment Status` -Customer employment status
- `Occupation` -Customer professional occupation
- `Industry` -Customer professional industry
- `Income Source` -Customer source of income
- `Income State` -State where customer earns income
- `Income Country` -Country where customer earns income
- `Employer` -Name of the customer employer
- `Employer State` -State where customer employer based
- `Employer Country` -Country of the customer employer
- `Source of Funds` -Customer source of funding for the account
- `Wealth Source` -Customer source of wealth
- `Annual Income` -Customer annual income

Customer Address

- `Is Primary` -Whether the address is customer primary address
- `Address Type` -Customer address type (Work, Home or Other)
- `Classification` -Classification of the customer address
- `Street 1-3` -Complete street address of the customer
- `City` -City where customer lives
- `State/Province` -State where customer lives

Field	Description
	`Postal Code` -Customer postal code `Country` -Country where customer lives Customer Phone `Is Primary` -Whether the phone number is customer primary phone number `Phone Number` -Customer phone number `Extension` -Extension for the phone number `Phone Type` -Type of phone number `Notes` -Notes on the phone number Customer Email `Is Primary` -Whether the email address is the customer primary email address `Email Type` -Select email address type `Email Address` -Customer email address **Business** Customer Profile `Entity Type` -Business entity legal classification `Tax ID Type` -Customer tax ID type `Tax ID` -Customer tax ID number `Ownership Type` -Entity ownership structure `Controlling Person` -Person who exercises control over entity `Date Formed` -Date when legal entity was formed `Backup Withholding` -Enable to allow withholdingtaxes on interest earned `Backup Withholding %` -If Backup Withholding is enabled, enter a percentage to withholdtaxes on interest earned `Risk` -Customer/ business risk classification

Field	Description

- `Citizenship` -Customer or business entity country of citizenship
- `Parent Entity` -Enter or search for Parent entity

Customer Address

- `Is Primary` -Whether the address is customer primary address
- `Address` Type-Customer address type (Work, Home or Other)
- `Classification` -Classification of the customer address
- `Street 1-3` -Complete street address of the customer
- `City` -City where customer lives
- `State/Province` -State where customer lives
- `Postal Code` -Customer Postal code
- `Country` -Country where customer lives

Customer Phone

- `Is Primary` -Whether the phone number is customer primary phone number
- `Phone Number` -Customer phone number
- `Extension` -Extension for the phone number
- `Phone Type` -Type of phone number
- `Notes` -Notes on the phone number

Customer Email

- `Is Primary` -Whether the email address is the customer primary email address
- `Email Type` -Select email address type
- `Email Address` -Customer email address

4   Click **Onboard Customer**. The new customer appears in the Customers list.

4.2.4. Org management portal

The Organization Management portal lets you manage your users and clients independently.

The Org Management application gives you more autonomy around managing users, roles, scopes, and clients for your organization. It increases your organization's security, as no one outside your organization needs to or be able to access secrets.

The Org Admin has the ability to:

- Delete a user

- Change a user's phone number

- Resend a registration email during sign-up

- Reset a user's MFA

- Add, edit, and delete the roles associated with a user

- Create, edit, disable, and delete clients (API machine to machine) from the organization

- Add, edit, and delete the scopes associated with a client

- Add, edit, and delete email domains associated with organizations.

Limitations

- A user who wants to gain access to their organization's data for Arix Marketplace Lending needs to create a support ticket with **arix.support@crossriver.com**.

- COS Explorer roles are managed within COS Explorer.

Admin user actions

As an Organization Management Portal **Admin User**, you can view applications, users, and domains.

Login

Access:

- **https://orgmanagementsandbox.crbcos.com/** (sandbox)

- **https://orgmanagement.crbcos.com/** (production)
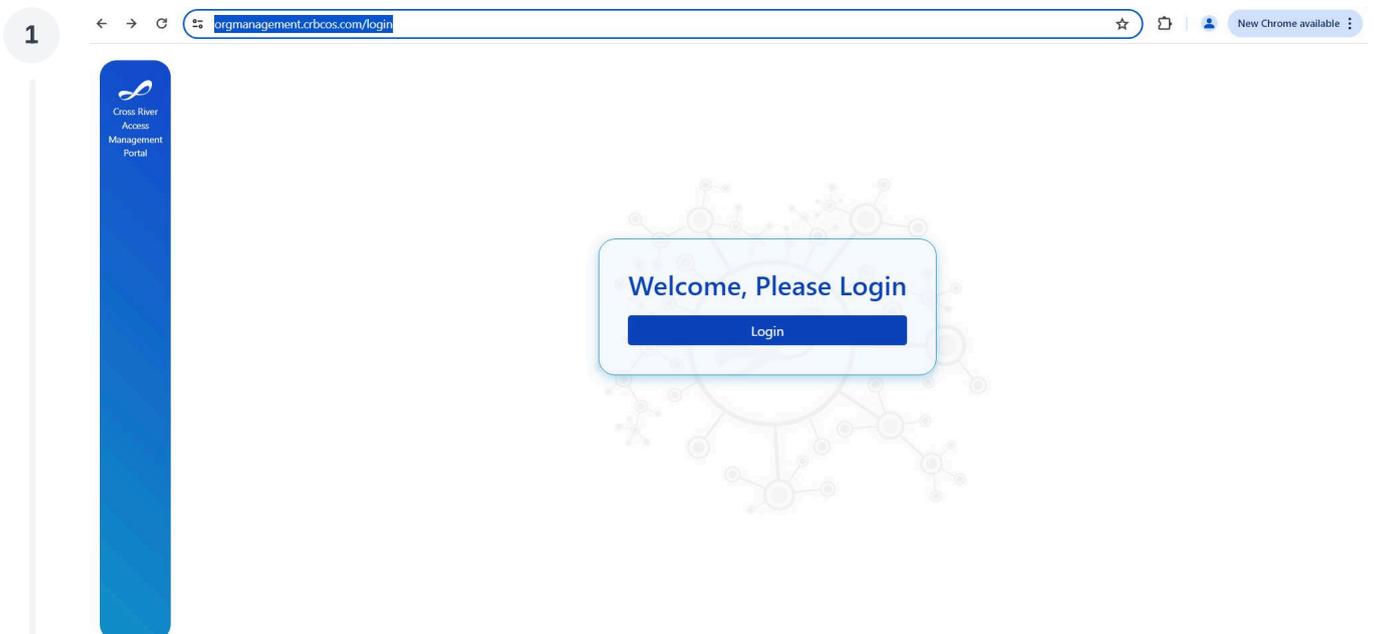
1

2 Click **Login**.

The Organization Management Portal opens, displaying the dashboard.

Dashboard

For each type of item (apps, clients, scopes, and so forth) in the network, view a tile showing the number of items that exists for a particular customer.
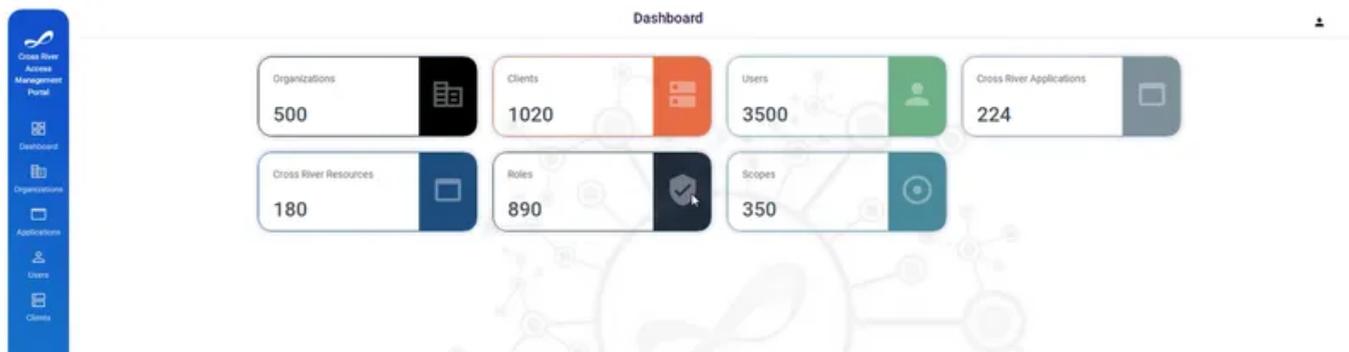
To display the dashboard, in the left-side icon bar, click **Dashboard**.

Applications

Within Applications, there are scopes and roles.

- *Scopes* provide an organization's applications with access—via the Cross River API—to user data. This way, they control the abilities and limits (i.e., the "scope") of the client application. Scopes are also known as protected resources.

- *Roles* define what features an organization's users can see and the permissions they have in the organization's applications. An organization can apply roles to different applications.

Use Case

Control access to CR functions and features, for example, P2P.

User Interface

Each organization is exposed to a subset of scopes and roles. For example, a crypto platform might be assigned 5 roles and scopes. However, an administrator might choose to let the users within that platform (i.e., the organization) see only 3 of those roles and scopes.
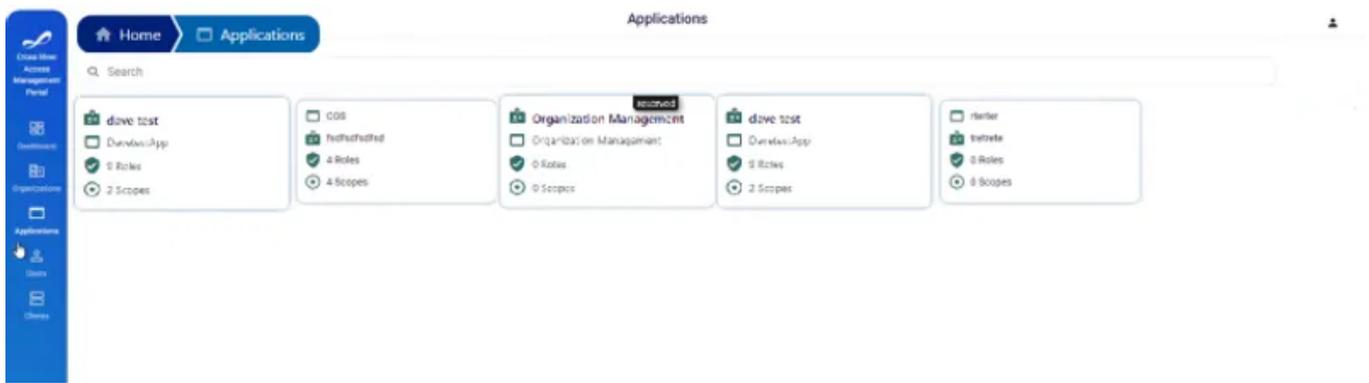
In the Applications window, each tile shows both the application name and the display name.

The back-office user has visibility to both names. The application user views only the display name. Also, the card shows the Scopes and Roles available to the organization.

> Suppose a back-office user creates a role for which the user's organization does not have access. In that case, in that user's tile, a red warning indicator will appear next to Roles.

Users

Associate users with an organization; edit user details. Each user has a name, email, and phone number.

Note that phone number is crucial for enabling user login because it's used for MFA. Attempting sign-in sends a verification code to the user's phone (can also be configured for email).

At first-time sign-in, the user decides the MFA method (i.e., verify to phone or email). Afterwards, if the user wants to change MFA preference, Cross River Admin intervention is needed.

The Cross River Admin verifies that the user-provided phone number and email do in fact exist and are valid. The Admin does this through an external application.

User Interface
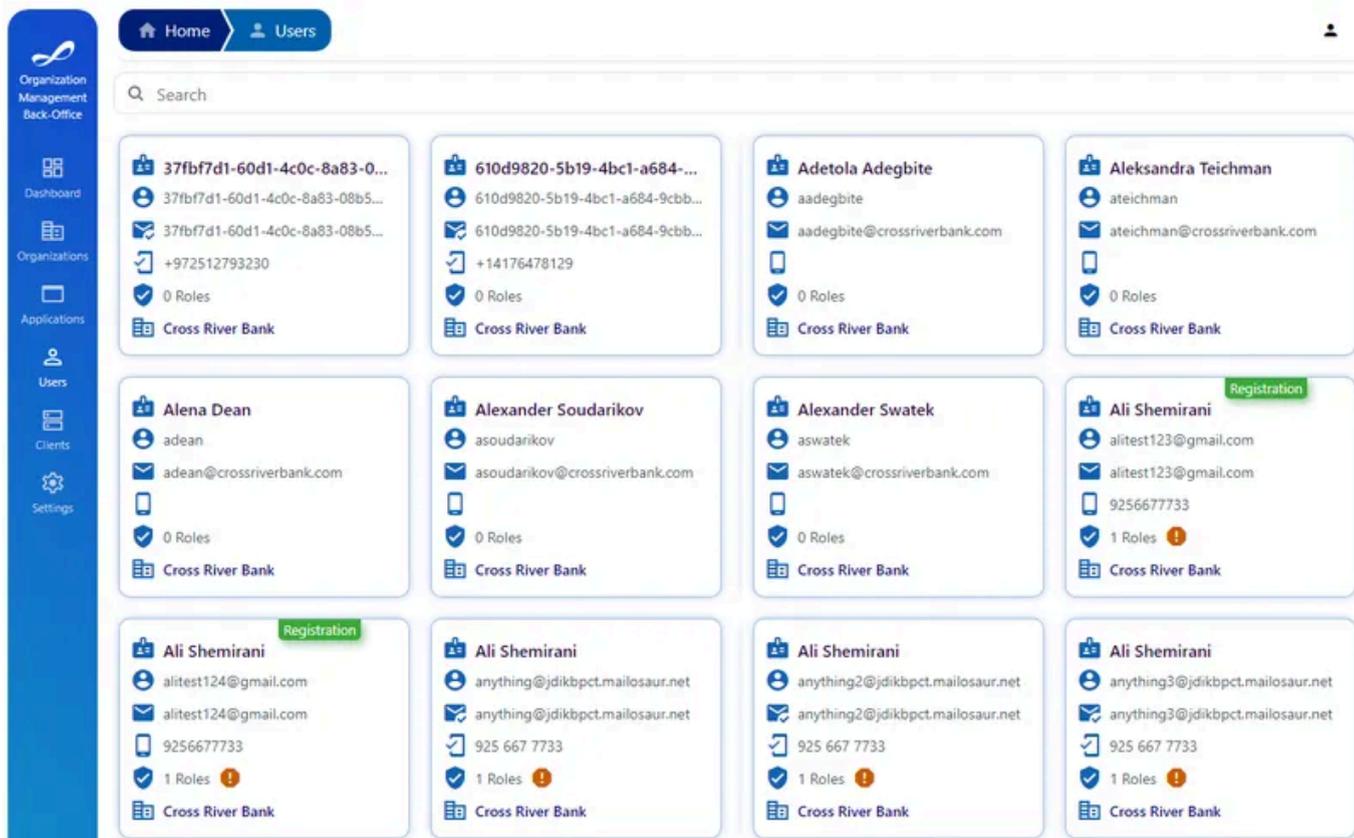
The UI object (i.e., tile) that appears to a user depends on:

- The user's role

- The scope associated with that role in the organization.

In the User view, details on each user appear within a separate tile.

Domains

A domain is a group of networked computers that share both user account information and a common security policy.

User Interface
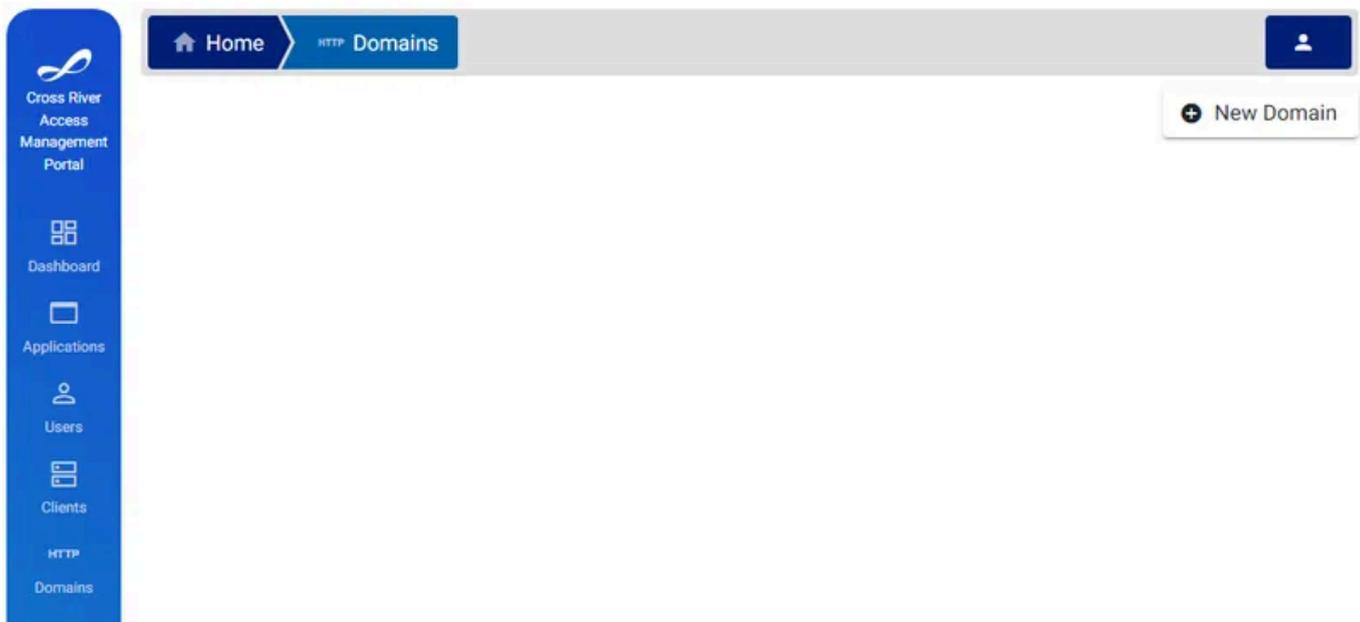
SSO

Cross River offers you the option to access Cross River applications with your own **SSO** (Single Sign On) login system. Benefits of SSO include a more seamless and cohesive user experience, as well as higher levels of security.

We support both OIDC and SAML configurations.

Sign-off

To exit the Organization Management Portal, in the upper-right corner of the screen, click the person icon; then, click **Logout**.

4.2.4.1. Sign in and security

Once you are onboarded into the Cross River system you need to register in our authentication server, Identity Server, to access all Cross River applications.

You need to create an account for both your Sandbox and Production environments. New user account creation is initiated by either:

- Cross River support

- Your organization's Admin User on the **Org Management** application.

Your user account is initiated with your name, organization email address, and your cell phone number, which is required for multi-factor authentication. You can use the same email/username for both Sandbox and Production environments. We recommend using a different password for the different environments.

Our Support team creates your sandbox account. Your Integration or Relationship Manager creates your Production account.

The Identity Server endpoints are:

- **Sandbox:** **https://idptest.crbcos.com/Account/Login**

- **Production: https://idp.crbcos.com/Account/Login**

IMPORTANT

IP allowlisting

Identity Server IP addresses are:

- 172.67.26.222
- 104.22.40.134
- 104.22.41.134

Organization management portal address:

- 66.206.202.116

The server is proxied via Cloudflare.

You can allow these FQDNs:

- `idptest.crbcos.com`
- `idp.crbcos.com`

Welcome email

You will received a welcome email from *CrossRiver_DO_NOT_REPLY@crossriver.com*. If you don't see it in your inbox, check your spam or blocked mail folders.

Click **Create your Cross River Account** to start the account registration process.

You are re-directed to the Terms and Conditions page to begin your registration process.

> If you leave the wizard at any time, click the link in the original email to go back to where you left off.

Terms and conditions

Read through the terms and conditions, check **Accept**, and click **Next**.

Verification

Select verification code method

If you are using a domestic (US) phone number, choose how you will received your verification code: phone call or Whatsapp message.

How would you like to receive your verification code?

Phone Call

— Or —

WhatsApp Message

If you use an international (non-US domestic) phone number, you receive the verification code by SMS.

Enter verification code

You receive a 6-digit code through your chosen method, used to verify your identity. On the login screen, enter the 6-digit code you received and click **Verify Code**.

Step 2 of 5

Enter the 6-digit code sent to your phone (********0371)

This helps us keep your account secure by verifying that it's you.

1	8	8	4	4	7

Verify Code

If you don't receive a code, restart the registration process from the **welcome email**.

Create your password

1 Choose a password that meets the on-screen requirements and enter it into the **Password** field.

2 Confirm your password by entering it in the **Confirm Password** field.

3 Click **Create Password**.

Authenticator app setup

IMPORTANT

You must complete this step to continue the registration process and to be able to login in the future

To protect your identity and your account and information, we require you to use an authenticator app as part of the MFA (multi-factor authentication) process.

If you don't already have an authenticator app on your device, you need to download one before you continue.

For Android and iOS, we recommend using the follow authenticator app:

- Google Authenticator
- Microsoft Authenticator

Once you have your authenticator app installed, you need to either **scan the QR code** or **manually enter the key** into the authenticator app (see below).

You may have to create a new account in the authenticator app before you can continue
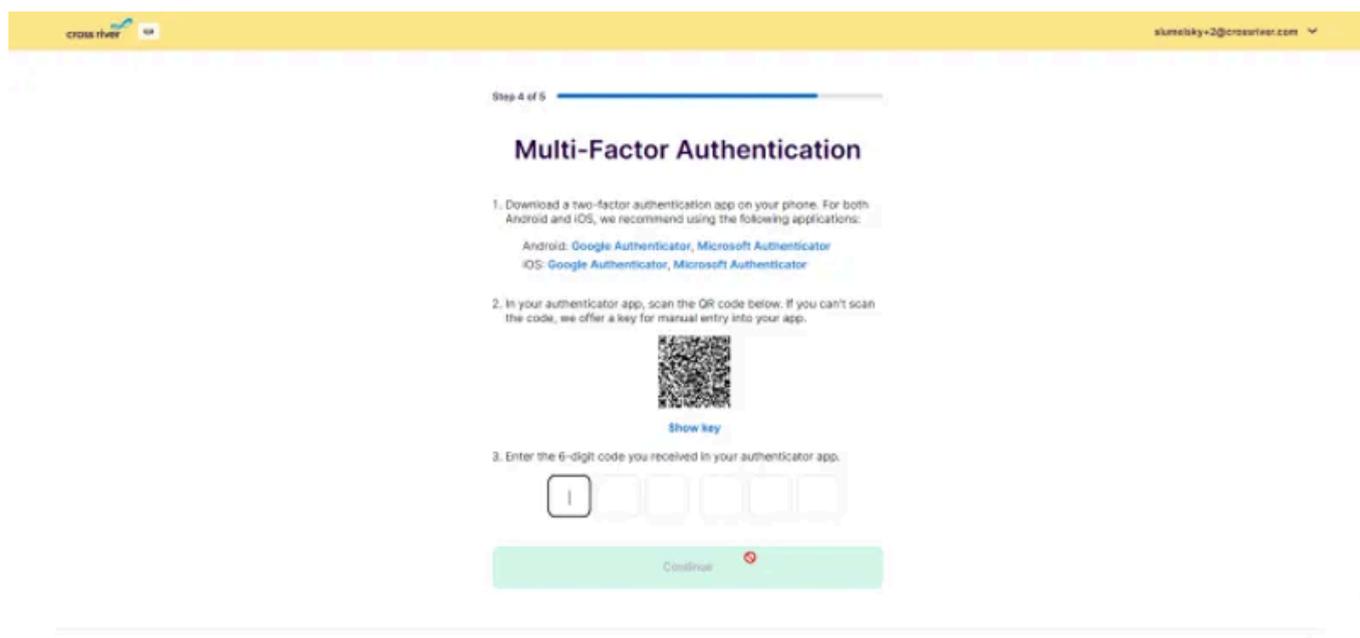
QR code

1 Scan the QR code in your authenticator app.

2 If requested, enter the 6-digit code in the Multi-Factor authentication page.

3 Click **Continue**.

Manual

1   Click **Show key**.

2   Copy the key as the *Secret* in your authenticator app.

3   Tap the account on the home page to generate a 6-digit code.

4   Enter the 6-digit code.

5   Click **Continue**.

If your MFA code is accepted, the browser automatically takes you to the next step in the registration process.

We suggest you rename your MFA connection in the app to make it easy to identify in the future.

Recovery codes

Use recovery codes to authenticate in case you lose your device.

1. Download or copy your recovery codes and keep them in a secure place that you will remember

2. Confirm that you have stored your recovery codes.

3. Click **Create account**.

   Your account is now active and you can use it to login to any of your CR apps.

IMPORTANT

The recovery codes page times out after 10 minutes.

You can only download the recovery codes once.

Recovery Codes

You can use recovery codes as an alternative authentication method if you lose your device. We recommend saving them with a secure password manager such as 1Password , Authy, or Keeper.

> **Important**
>
> **Single Use:** Each unique code can only be used once.
> **Store Securely:** Store codes in a safe and accessible place.

Your Recovery Codes:

1. 4ea525d8   2. bd38b33e
3. e8fc93bb   4. c26c606b
5. 0c3dbcba   6. b9970fca

☐ I have securely stored my recovery codes and understand that they are essential for future logins if I lose my devices.

Download recovery codes
To keep your account safe, you may only download recovery codes once.

Return to Account Settings

IP allowlisting

The Identity Server IP addresses are:

- 172.67.26.222

- 104.22.40.134

- 104.22.41.134

The server is proxied via Cloudflare.

You can allow these FQDNs:

- idptest.crbcos.com

- idp.crbcos.com.

Login to Cross River applications

1 Enter your email address on the application's Login page. The environment indication banner at the top of the screen shows you which environment you are working in.

2 Click **Continue** to go to the password screen.

3 In the password screen, enter your password and click **Continue**.

Troubleshooting

Forgot password

If you enter an invalid username and password combination the **Invalid username or password** message displays in red under the Password field.

1 Click **Forgot password?** and enter your email.

2   Enter the 6-digit authentication code from your authenticator app.

Enter the 6-digit code from your authenticator app

This helps us keep your account **forth-charge@ngzdmuwl.mailosaur.net** secure by verifying that it's you.

| 0 | 6 | 8 | 9 | 5 | 7 |

Login

3   You need to reauthenticate with an MFA code from your authenticator app before the password reset email can be sent. After entering the code, click **Login**.

Here are some things to double check:

- Did the code timeout before you clicked **Continue**? Remaining time is indicated by the countdown circle to the right of the account name and MFA code.

- If you have the authenticator app set up for multiple environments or applications, double check that you entered the correct code.
    - If it is not clear from the MFA connection names which is correct option, you might need to try different codes until finding the one that works.

    - Once you find the correct connection, you can rename the MFA connection in the app. A pencil icon at the top of MFA app screen will bring you to edit mode. In some apps, you will need to first select (or press and hold) the connection that should be edited, and then the icon will appear.

    - Once in edit mode, you can rename the connections as needed so that it will be clear which one applies to which environment.

    - Save any changes, and next time it should be easier to understand which code to use.

Reset multi-factor authentication

If you already have MFA configured:

1. In Identity Server, go to **Reset MFA** and click **Reset your MFA device**.

2. The Multi-Factor Authentication page opens and you can reset your MFA.

You can also create new multi-factor authentication recovery codes.

1. Click **Create new multi-factor authentication recovery codes**.

2. The Recovery Codes page opens and you can copy or download your 10 new recovery codes.

If you have not yet configured your multi-factor authentication, you can enable MFA from **Account Settings**.

1. Click **Reset MFA Method**.

2. Click **Configure MFA**.

3. Follow the instruction in **Authenticator app setup**.

If your current MFA is SMS, you can enable MFA with your authenticator app, in **Account Settings**.

1. Click **Reset MFA Method**.

2. Click **Configure MFA**.

Invalid MFA Code

If you enter an invalid MFA code, a red message notifies you to try again.

Here are some things to double check:

Did the code timeout before you clicked **Continue**? Remaining time is indicated by the countdown circle to the right of the account name and MFA code.

If you have the authenticator app set up for multiple environments or applications, double check that you entered the correct code.

- If it is not clear from the MFA connection names which is correct option, you might need to try different codes until finding the one that works.

- Once you find the correct connection, you can rename the MFA connection in the app. A pencil icon at the top of MFA app screen will bring you to edit mode. In some apps, you will need to first select (or press and hold) the connection that should be edited, and then the icon will appear.

- Once in edit mode, you can rename the connections as needed so that it will be clear which one applies to which environment.

- Save any changes, and next time it should be easier to understand which code to use.

Correct password, invalid MFA

If you try to log in to a Cross River application with the correct password but an invalid MFA code, a red message informs you that the code is invalid.

Here are some things to double check:

Did the code timeout before you clicked **Continue**? Remaining time is indicated by the countdown circle to the right of the account name and MFA code.

If you have the authenticator app set up for multiple environments or applications, double check that you entered the correct code.

- If it is not clear from the MFA connection names which is correct option, you might need to try different codes until finding the one that works.

- Once you find the correct connection, you can rename the MFA connection in the app. A pencil icon at the top of MFA app screen will bring you to edit mode. In some apps, you will need to first select (or press and hold) the connection that should be edited, and then the icon will appear.

- Once in edit mode, you can rename the connections as needed so that it will be clear which one applies to which environment.

- Save any changes, and next time it should be easier to understand which code to use.

Valid MFA code (forgot password flow)

1   Enter valid MFA code from authenticator app and click **Login**.

Enter the 6-digit code from your authenticator app

This helps us keep your account **forth-charge@ngzdmuwl.mailosaur.net** secure by verifying that it's you.

| 0 | 6 | 8 | 9 | 5 | 7 |

Login

2   After your MFA code is accepted, check your email for further instructions.

3   Click **Reset Password**.

cross river

Cross River - Forgot Password

Please click the button to reset your password.

Reset Password

4   Enter and confirm a password that meets the on-screen requirements. A checkmark will appear next to each fulfilled requirement.

5 Enter and confirm a new password that meets the security requirements.

6 Click **Reset Password**.

Step 3 of 5

Create Password

Create a secure password for your account at
forth-charge@ngzdmuwl.mailosaur.net

Password* 👁

Confirm Password* 👁

Your password must contain:

- 10 characters minimum
- Lowercase characters
- Numbers
- 4 unique characters
- Uppercase characters
- Special characters

Create Password

7 If the password is accepted you will be informed of the successful reset. Click **Continue to the application** to be automatically redirected to the Cross River application that you were trying to access.

Reset Password Success

Your password has been successfully reset

Continue to the application

Use a recovery code

If you do not have access to your multi-factor (2-factor) authenticator, you can log in using one of your recovery codes.

1. Log in as usual.

2. On the Multi-Factor Authentication page, you have the option to use a recovery code as your authentication option.

3. Enter one of your recovery codes in the text box. The recovery code is single-use and cannot be reused. To avoid future confusion, we recommend that you mark the recovery code as used.

Account lockout

If you enter the wrong password for your username 5 times, the system locks your account for approximately 5 minutes. If after 5 minutes, you are still unable to access your account, contact Cross River Support.

4.2.4.2. Configure SSO

Cross River offers you the option to access Cross River applications with your own SSO (Single Sign On) login system. Benefits of SSO include a more seamless and cohesive user experience, as well as higher levels of security.

We support both OIDC and SAML configurations.

> These instructions explain how to configure SSO on the Cross River side. You also need to configure this SSO connection on your specific identity provider side, for example, EntraID.
>
> Your Org Management Admin user configures SSO on the Cross River side.

Verify SSO enabled

If the option for SSO Settings appears on the navigation of the **Org Management screen** SSO is enabled for your organization. If SSO is not enabled, open a support ticket using Cross River ServiceNow.
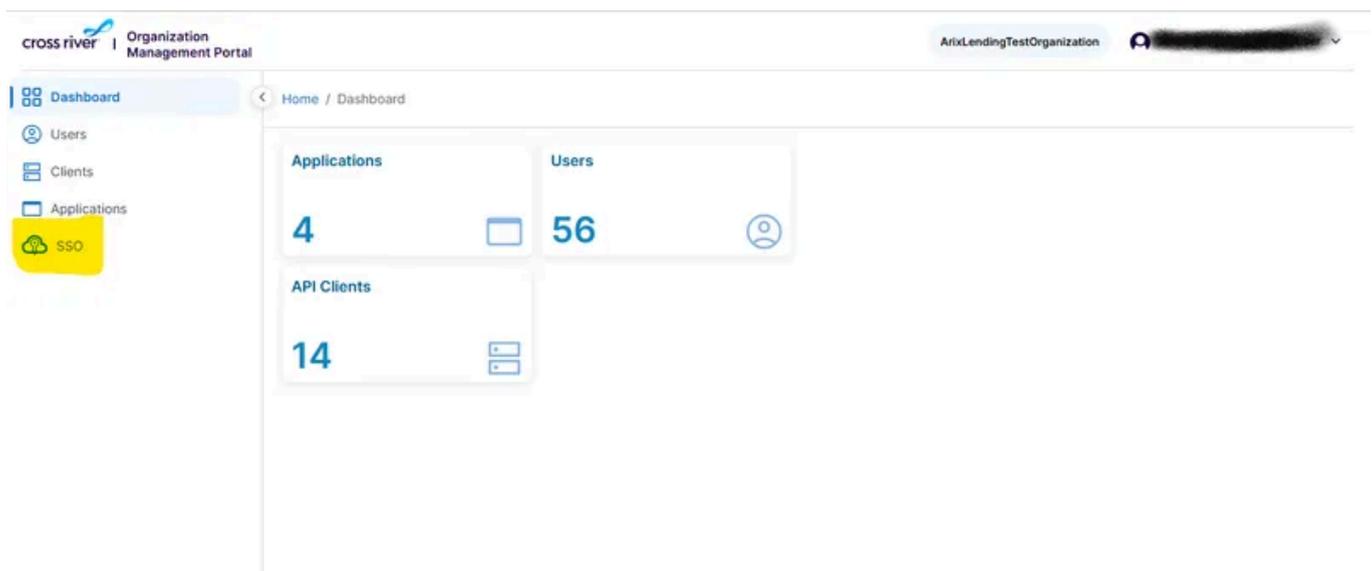
SSO appears on Org Management user interface

Configure Cross River-side SSO connection

Configure your SSO connection as follows:

1   Click **SSO** in the navigation pane, and then click **Configure**.
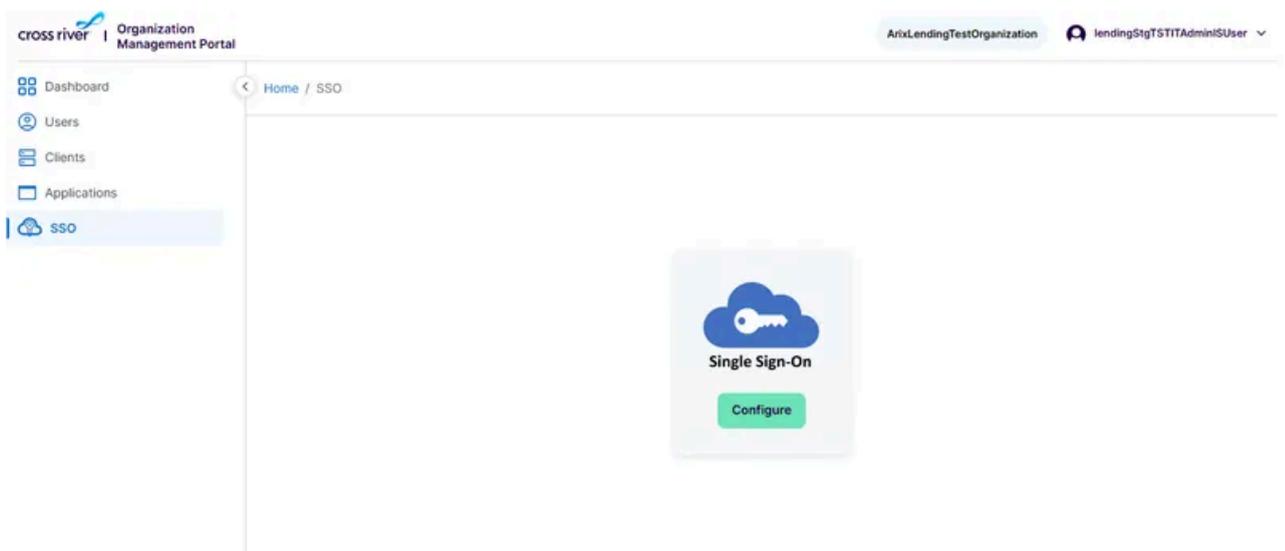
2   The SSO Configuration Panel opens. Select which type is required: **OIDC** or **SAML**. Fill in the fields according to the instructions on the page and click **Save**.

3   OIDC tab

4 SAML tab

5 Be sure to add the callback paths to your authentication server.

5. Reports

- **Accounts and payments**: Onboarding and several reports.

- **Card payments**: To assist partners with financial settlement and reconciliation, Cross River provides consolidated daily reports of payment transaction and chargeback activity.

- **Credit risk data reports**: You as a Cross River credit BIN sponsorship partner must supply Cross River on a monthly basis with a summary of specific credit risk metrics that are not visible to us.

- **Lending reports**: Arix servicing and transaction reports.

5.1. Accounts and payments

- **Onboarding**: Instructions on how to onboard for receiving COS reports

- **Overdrawn account**: This report contains a list of the partner's customer accounts that are overdrawn.

- **Daily account activity**: This report lets you see all the money movement for a single given master account.

- **Daily ACH payments**: Daily ACH Payment File Drop By Partner report.

- **Daily RTP activity**: This report lets you see all RTP payments for a single given COS partner.

- **Daily wire payments**: Daily Wire Payment File Drop By Partner report

- **Webhooks**: Webhook Events Export File Drop By Partner report.

- **Card payments**: Daily reports of payment transaction and chargeback activity.

5.1.1. Onboarding

This guide provides partners with the following:

- Instructions on how to onboard for receiving Cross River Operating System (COS) reports.

- A description of the report generation process, including the generation schedule, SFTP file path conventions and report file naming conventions.

- Additional points on COS reports.

Onboard a client to receive COS reports

- The partner emails Integration Support to set up an **SFTP** account.

- Integration Support sends the partner an SFTP setup form, which the partner fills out and sends back to Integration Support.

- CRB's Integration Support emails the username/password information back to the partner.

- The partner configures access to the SFTP folders, including access permissions for the folders.
    - The partner can set up sandbox and/or production folders within the SFTP master account.

- Integration Support notifies the partner when the process is complete.

Generation process

Once the partner has been onboarded, the reports are scheduled to run daily at 3AM EST, and are uploaded immediately following that.

The report files are uploaded to the following paths:

- \\sftp01\PTPs\<Partner Name>\PROD\COS\DailyReports\AccountActivity

- \\sftp01\PTPs\<Partner Name>\PROD\COS\DailyReports\AccountBalance

- \\sftp01\PTPs\<Partner Name>\PROD\COS\DailyReports\AchActivity

- \\sftp01\PTPs\<Partner Name>\PROD\COS\DailyReports\Webhooks
- \\sftp01\PTPs\<Partner Name>\PROD\COS\DailyReports\WireActivity
- \\sftp01\PTPs\<Partner Name>\PROD\COS\DailyReports\Overdrawn Account Report
- \\sftp01\PTPs\<Partner Name>\PROD\COS\DailyReports\RTP Daily Activity By Partner

File naming conventions

Report	Naming Convention
Account Activity Report	[PartnerName]_Daily_Account_Activity_[timestamp].csv
Account Balance Report	[PartnerName]_Daily_Account_Balance_[timestamp].csv
ACH Activity Report	[PartnerName]_Daily_Ach_Activity_[timestamp].csv Note: Data team needs to consolidate the naming convention on this one since we have some variations.
Webhooks Report	[PartnerName]_Webhook_Events_[timestamp].csv
Wire Activity Report	[PartnerName]_Daily_Wire_[timestamp].csv
COS Overdrawn Account Report	Overdrawn Account Report_[date].xlsx
RTP Daily Activity By Partner Report	[PartnerName] RTP Activity Report_[timestamp].csv

Additional points

- The partner receives a notification when a report is uploaded via SFTP.
- The report files in the SFTP folders are not deleted automatically.
- The reports will be PGP-encrypted.
- In addition to .csv and .xlsx, reports can be delivered in formats such as MT940 and PDF. Partners can contact the Relationship Manager for assistance with delivering reports in alternative formats.

5.1.2. Overdrawn account

The Overdrawn Account Report is an .xlsx file generated daily by the Cross River Operating System (COS)and sent to each partner via **SFTP**. It contains a list of the partner's customer accounts that are overdrawn.

Overdrawn Account Report
For Mar 10, 2022

Partner	Master Account Number	Account Title	Date Account Opened	Master Current Balance	Master Available Balance	Date Overdrawn	Fed Days In Overdraft

Report details

Column	Description
Partner	Partner name.
Master Account Number	Customer's master account number.
Account Title	Account title (customer name).
Date Account Opened	COS account opened date.
Master Current Balance	Current balance on the account.
Master Available Balance	Available balance on the account.
Date Overdrawn	Day the account first became overdrawn.
Fed Days in Overdraft	The number of days the account has been overdrawn.

Overdraft notice

On the 1st and 7th days of a customer's account being overdrawn, COS sends the following form notice to the customer in PDF format, with the fields in the letter populated from the Overdrawn Account Report and additional data fields.

Overdraft Notice

cross river

Date 03/10/2022
1st Overdraft notice
Dear <Account Title> ,

Our records indicate that your <Product Name> account ending in <Last 4 digits of account number> has been overdrawn since <Date Overdrawn> . The current amount of the overdraft is <Account Balance>

Please make a deposit immediately to cover this overdraft.

If you are unable to cover the entire amount at this time, or feel there is an error in this account, please contact <Partner> immediately. Failure to bring your account to a positive balance may result in your account being closed.

Your prompt attention to this matter is respectfully requested.

Should you have any questions, please feel free to contact <Partner>.

Sincerely,

Customer Support

5.1.3. Daily account activity

The purpose of this section is to explain the Daily Account Activity report. This report lets you see all the money movement for a single given master account.

This report can be used to reconcile between what you requested from the Cross River Operating System (COS) and what COS actually processed.

Term	Description
CR	Cross River
Partner	Cross River's immediate customer, i.e. you

Report details

The table below shows the different columns included in the report together with descriptions and explanations of the information they represent.

Column	Description
Id	This is internal to Cross River and can be disregarded.
Transaction Id	Unique identification number for the related core transaction.
TraceNumber	A unique number assigned to the transaction by COS.
Status	Transaction status.
Transaction Type	Core transaction type, which can be either Debit or Credit.
ActivityType	Indicates whether the activity is internal (between two sub accounts under the same master account) or external (between two master accounts).
Source	Activity type, which includes: • Transaction: Activity from transactions will first soft post, remaining as status pending for the day, and later hard post during the nightly settlement process. Once hard posted a sequence number and running balance are assigned. • MemoPosts: Activity from memo posts are a temporary debit or credit on the account. Commonly they will be removed and then posted as a transaction.
MasterAccountNumber	Master account affected by the transaction.
SubAccountNumber	Sub ledger account affected by the transaction.
Transaction Code	Indicates transaction types as follows: • Incoming ACH • Outgoing ACH • Account Transfer • Fee • Fee Refund • Deposit

Column	Description
	• Withdrawal
	• Interest
	• Misc Credit
	• Misc Debit
	• Incoming Wire
	• Outgoing Wire
	• Check
	• Cash
	• Reversal
	• Adjustment
	• Sale
	• Card Auth
	• Payment
	• Refund
	• ATM Transaction
	• Zelle Debit
	• Zelle Credit
	• RTP Debit
	• RTP Credit
Description	Transaction description.
Rail	Rail type (i.e. ACH, Wires, etc.)
RailId	Rail ID, which is a combination of the transaction code and the payment ID.
Amount	Transaction amount.
Balance	Balance resulting from the transaction.
SequenceNumber	Sequence number of the payment in the batch. The sequence number is inserted once the transaction has been posted.
ProductId	Product identifier for the account involved in the transaction.

Column	Description

5.1.4. Daily ACH payments

Daily ACH Payment File Drop By Partner report.

Using the Cross River Operating System (COS) **ACH APIs**, your account can both originate and receive payments through an ACH Operator. The information required for a payment varies depending on the relevant SEC code and is governed by NACHA Operating Rules and Guidelines. Required information will also vary for domestic or international payments.

ACH files are received daily from both Cross River's clients (originators) and the Federal Reserve Bank (FRB). The files are automatically imported into Cross River's ACH manager, systematically validated for correctness, and then verified for release to the FRB for via a two-stage process of review with authorization.

Report details

The table below provides information for some of the fields within your report. For information on Nacha-specific fields please refer to your copy of the Nacha Operating Rules.

Column	Description
AccountNumber	COS account number related to the payment.
ReferenceId	A unique ID for the payment.
PaymentType	The type of payment, which includes: • **Origination**: A new payment originating from either Cross River or another bank. Most payments are of this type. • **Return**: Related to a previous origination that has been returned by the receiving bank. • **DishonoredReturn**: Related to a previous return, that has been dishonored by the receiving bank. • **Correction**: Related to a previous origination. The receiving bank accepted the original payment but is now notifying you of information you should correct next time you send a payment to this receiver (e.g. use a different account number).
ServiceType	The type of ACH service, which includes: • **Standard**: Payment will be effective the following day. International payments must use this type. • **SameDay**: Payment will be effective the same day it was originated provided it was originated before the daily cutoff time. Not available for certain payment scenarios.
TransactionType	The payment transaction type, which includes: • **Push**: a credit payment being sent from an originator to a receiver, or • **Pull**: a debit payment taken from a receiver and moved to the originator.
Direction	The payment direction, which includes: • **Inbound**: payment received from another bank. • **Outbound**: a payment sent to another bank.
Status	The status of the payment at the time the report was generated. Statuses include:

Column	Description
	Created: the payment has been received but hasn't been processed yet. This status will only appear briefly. • **Pending**: the payment is waiting to be batched and sent to the FRB. • **Hold**: the payment is currently being held and is being reviewed by Cross River's Operations team. • **Batched**: the payment has been batched, and Cross River is carrying out a final review before the payment is sent in a batch file to the FRB. • **Processing**: For inbound payments, we are attempting to post the payment to the receiving account. For outbound payments, the payment has been sent to the FRB, but has not been posted yet. An outbound standard payment may remain in this status for a day or more. Same-day payments will transition to Complete soon after processing. • **Complete**: the payment has been posted and accepted by the FRB (in the case of outbound payments). This is a final status. • **Canceled**: Indicates that an outbound payment has been canceled at the Partner's request. A payment can only be canceled while either pending or on hold. This is a final status. • **Rejected**: Cross River's Operations team was unable to process the payment and has rejected it. For inbound payments, the payment request is returned to the originating bank. This is a final status.
SecCode	The Standard Entry Class (SEC) code for the payment.
ClientBatchId	Unique identifier for a batch (GUID). This only applies to partners that originate client batches.
ClientBatchSequence	Sequence number of the payment in the batch. This only applies to partners that originate client batches.
FedBatchId	Fedwire or ACH batch ID used for settlement tracking.
FedBatchSequence	Sequence number of the payment in the Federal Reserve batch on which the payment went out or came in.

Column	Description
Posting	Status of the related Core transaction for the payment. Can be pending, posted, or failed.
CoreTransactionId	The ACH payment's related core transaction ID.
Description	Company entry description.
Amount	The transaction amount.
EffectiveDate	Effective Entry Date.
Addenda	Payment-related information.
ReasonCode	Code for the reason for an ACH return or notification of change.
ReasonData	Supporting data for the reason code.
TraceNumber	This corresponds to the NACHA "Trace Number" field and is a unique number assigned to the transaction.
SettlementDate	Corresponds to the NACHA "Settlement Date" field.
CreatedAt	The date and time the payment was created.
CanceledAt	The date and time the payment was canceled.
RejectedAt	The date and time the payment was rejected.
ProcessedAt	The date and time the payment was processed.
CompletedAt	The date and time the payment was completed.
PostedAt	The date and time the transaction was posted, specifically at end of day settlement.
PartnerId	The unique identification number for the partner resource.
ProductId	The product identifier for the account involved in the ACH payment.
OriginatingBankRoutingNumber	The ABA number for the bank where the transfer originated.
OriginatorName	This corresponds to the NACHA "Company Name" field name of the originator of the ACH transaction.

Column	Description
OriginatorAccountNumber	This is the account number where the transaction originated from.
OriginatorAccountType	This is the type of account the transaction originated from.
OriginatorData	This corresponds to the NACHA "Company Discretionary Data" field.
OriginatorIdentification	This corresponds to the NACHA "Company Identification" field.
ReceiverName	This corresponds to the NACHA "Individual Name" field.
ReceiverAccountNumber	This corresponds to the NACHA "DFI Account Number" field.
ReceiverAccountType	This corresponds to the NACHA "Transaction Code" field.
ReceiverData	This corresponds to the NACHA "Discretionary Data" field.
ReceiverIdentification	This corresponds to the NACHA "Individual Identification Number" field.
ReceivingBankRoutingNumber	This field corresponds to the NACHA "Receiving DFI Identification" field.
UltReceiverAccountNumber	The ultimate receiver's account number.
UltReceiverAccountType	The ultimate receiver's account type.
UltReceiverData	Data for the ultimate receiver.
UltReceiverIdentification	The ultimate receiver's identification.
Fcb1RoutingNumber	Foreign corresponding bank 1 routing number.
Fcb2RoutingNumber	Foreign corresponding bank 2 routing number.

Column	Description
er	
Fcb3RoutingNumber	Foreign corresponding bank 3 routing number.
PostingCode	Status for the payment's related Core transaction.
PreviousPaymentId	Payment ID for the original payment related to a return or NOC that we received.
PreviousReasonCode	The reason code for the original payment related to a return or NOC that we received.
PreviousTraceNumber	Trace number for the original payment related to a return or NOC that we received.
PreviousSettlementDate	Settlement Date for the original payment related to a return or NOC that we received.
PreviousReasonData	Supporting data for the reason code for the original payment related to a return or NOC that we received.
OriginalPaymentId	Payment ID for the original payment related to a return that we received for dishonored returns.
OriginalReasonCode	The reason code for the original payment related to a return that we received for dishonored returns.
OriginalTraceNumber	Trace number for the original payment related to a return that we received for dishonored returns.
OriginalSettlementDate	Settlement Date for the original payment related to a return that we received for dishonored returns.
OriginalReasonData	Supporting data for the reason code for the original payment related to a return that we received for dishonored returns.
OriginatorRoutingNumber	This corresponds to the NACHA "Originating DFI Identification" field.
ReceiverRoutingNumber	The receiver's routing number.

Column	Description
ExtCardTransactionType	(Extended payment details) – NACHA-specific
ExtReference1	(Extended payment details) – NACHA-specific
ExtReference2	(Extended payment details) – NACHA-specific
ExtTerminalIdentification	(Extended payment details) – NACHA-specific
ExtTransactionSerial	(Extended payment details) – NACHA-specific
ExtTransactionDate	(Extended payment details) – NACHA-specific
ExtAuthCode	(Extended payment details) – NACHA-specific
ExtTerminalLocation	(Extended payment details) – NACHA-specific
ExtTerminalCity	(Extended payment details) – NACHA-specific
ExtTerminalState	(Extended payment details) – NACHA-specific
Fields beginning with `Iat` only apply to International ACH Transactions.	
IatTransactionTypeCode	Code for the transaction type of the international transaction.
IatOriginatorAddress	Street address of the originator of the international transaction.
IatOriginatorCity	The city of the originator of the international transaction.
IatOriginatorState	The state of the originator of the international transaction.
IatOriginatorPostalCode	The zip/post code of the originator of the international transaction.

Column	Description
IatOriginatorCountryCode	The country code of the originator of the international transaction.
IatReceiverAddress	The street address of the receiver of the international transaction.
IatReceiverCity	The city of the receiver of the international transaction.
IatReceiverState	The state of the receiver of the international transaction.
IatReceiverPostalCode	The zip/post code of the receiver of the international transaction.
IatReceiverCountryCode	The country code of the receiver of the international transaction.
IatOriginatingBankName	The name of the bank where the transaction originated.
IatOriginatingBankIdQualifier	The ID qualifier corresponds to the originating bank identification.
IatOriginatingBankIdentification	The identifier of the bank originating the international transaction.
IatOriginatingBankCountryCode	The country code of the bank where the international transaction originated.
IatReceivingBankName	The name of the bank where the international transaction was received.
IatReceivingBankIdQualifier	The ID qualifier corresponding to the receiving bank identification.
IatReceivingBankIdentification	The identifier of the bank receiving the international transaction.
IatReceivingBankCountryCode	The country code of the bank receiving the international transaction.
IatUltReceiverName	The ultimate receiver's name.

Column	Description
IatUltReceiverAddress	The ultimate receiver's street address.
IatUltReceiverCity	The ultimate receiver's city.
IatUltReceiverState	The ultimate receiver's state.
IatUltReceiverPostalCode	The ultimate receiver's postal code.
IatUltReceiverCountryCode	The ultimate receiver's country code.
IatFcb1Name	The name of the first foreign correspondent bank.
IatFcb1IdQualifier	The ID qualifier for the first foreign correspondent bank.
IatFcb1Identification	The first foreign correspondent bank's identification.
IatFcb1CountryCode	The first foreign correspondent bank's country code.
IatFcb2Name	The name of the second foreign correspondent bank.
IatFcb2IdQualifier	The ID qualifier for the second foreign correspondent bank.
IatFcb2Identification	The second foreign correspondent bank's identification.
IatFcb2CountryCode	The second foreign correspondent bank's country code.
IatFcb3Name	The name of the third foreign correspondent bank.
IatFcb3IdQualifier	The ID qualifier for the third foreign correspondent bank.
IatFcb3Identification	The third foreign correspondent bank's identification.
IatFcb3CountryCode	The third foreign correspondent bank's country code.
ExtPaymentType	(Extended payment details) – NACHA-specific

Column	Description
InsertedAt	This is internal to CRB and can be disregarded.
ExtProcessControl	(Extended payment details) – NACHA-specific
ExtResearchNumber	(Extended payment details) – NACHA-specific
Purpose	Internal reason for the payment. This is an internal field and is not included in the payment message.
ExtCheckSerialNumber	(Extended payment details) – NACHA-specific
ExtItemType	(Extended payment details) – NACHA-specific
ExtCardAccountNumber	(Extended payment details) – NACHA-specific
ExtCardExpDate	(Extended payment details) – NACHA-specific
ExtDocReferenceNumber	(Extended payment details) – NACHA-specific
ExtNetworkIdentification	(Extended payment details) – NACHA-specific
ExtTransactionTime	(Extended payment details) – NACHA-specific
ExtTransactionDesc	(Extended payment details) – NACHA-specific
MemoPostId	Unique ID for the memo post transaction.
WasReturned	Indicates whether the payment was returned.
WasCorrected	Indicates whether the payment was corrected.
HoldDays	The number of days a credit was withheld (where applicable; for Outbound Pull payments only).

Daily RTP activity

This report lets you see all RTP payments for a single given Cross River Operating System (COS) partner.

You can use this report to reconcile between what you requested from COS and what COS actually processed.

Term	Description
COS	Cross River Operating System
Partner	Cross River's immediate customer, i.e. you

Report details

The table below shows the different columns included in the report together with descriptions and explanations of the information they represent.

Column	Description
TransactionId	The unique identification number for the related core transaction.
TransactionAmount	The dollar amount of the payment.
PaymentStatus	The payment status in COS.
Payment_TypeName	The core transaction type. For a full list of payment types, see **below.**
PaymentSource	The source initiating the payment. This may be one of the following: • API • Clearing House (for inbound payments) • Partner Portal (when a partner user enters a payment request in COS Explorer) • Ops Portal (when Cross River Ops enters a payment request in COS Explorer)
PartnerName	The name of the COS partner participating in the payment.
ProductName	The COS product name for the COS account participating in the payment.
ClientIdentifier	An optional unique internal identifier for the payment, defined by the partner. **Note**: COS does not enforce uniqueness or idempotency based on this value. It is, however, an important part of implementing a partner's idempotency solution. This value can be used to search for a payment to check if COS had successfully processed your request when in doubt. This should not be done if the response indicates success. It is only to be used in edge cases when there is doubt regarding the response (i.e. an exception occurred). For more information, see **Idempotency**.

Column	Description
DebtorName	The debtor name for the payment. This can be either the COS customer or external debtor, based on the direction of the payment.
AccountNumber	The COS master account involved in the payment.
SubAccountNumber	The COS sub ledger account involved in the payment.
CreditorName	The creditor name for the payment. This can be either the COS customer or external creditor, based on the direction of the payment.
CreditorAccountNumber	The creditor account number. This can be the account number for either the COS customer or the external customer, based on the direction of the payment.
Direction_Desc	The payment direction (Inbound or Outbound).
Purpose	The payment purpose.
ReferenceId	The payment reference ID in COS.
SentAt	The date and time the payment was executed.
CompletedAt	The date and time the payment completed.
RejectedAt	The date and time the payment was rejected. If this field is populated, then the **CompletedAt** field is always empty.
RTPTransactionStatus	Status of the RTP transaction as reported by the receiving institution. For a list of statuses, see the RtpTransactionStatus table below.
ConfirmedTransactionStatus	The RTP transaction status, as reported by the receiving institution and confirmed by COS. For information on available statuses, see the instant payment **request and response codes**.
ConfirmedReasonC	The reason the payment did not complete, as confirmed by COS. For information on available reason codes, see below.

Column	Description
ode	
Confirme dAddition alInfo	Additional payment information, as confirmed by COS. For a list of values, see **ConfirmedAdditionalInfo** below.

Outbound request for payment
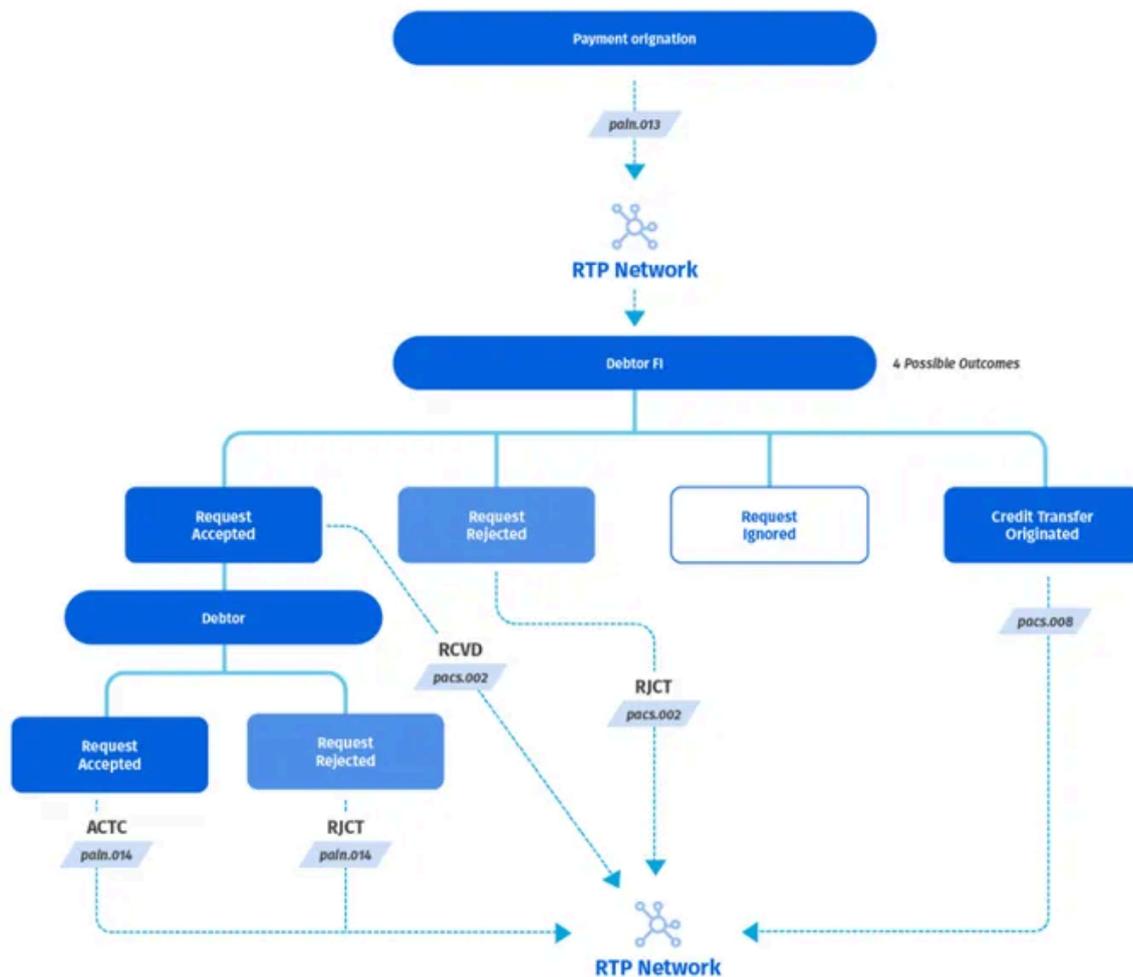
Inbound request for payment
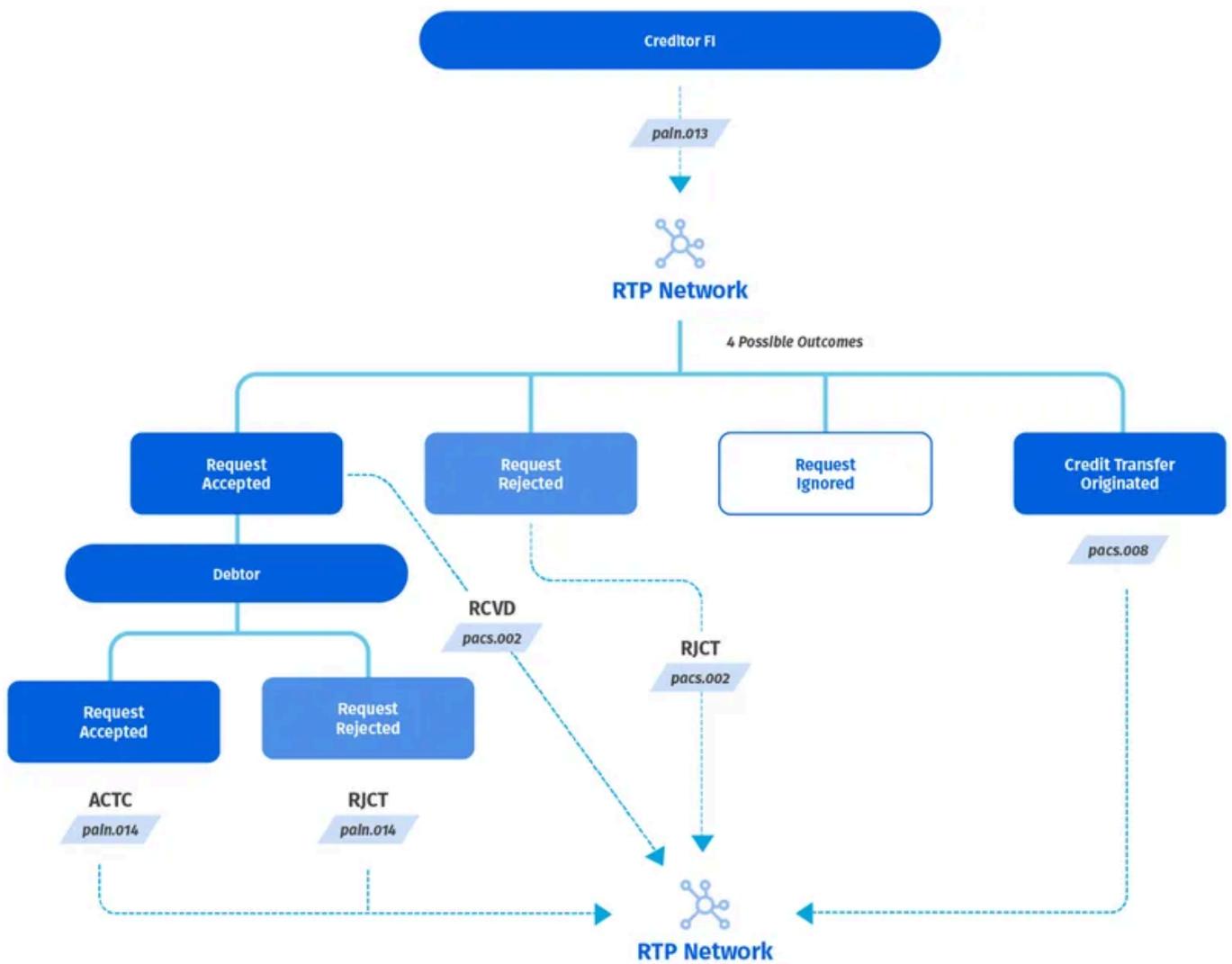
Enum values for payment type

TypeName	Value	Description
PaymentTypes	0	Credit Transfer
PaymentTypes	1	System Timeout
PaymentTypes	2	Return Request
PaymentTypes	3	Return Response
PaymentTypes	4	Remittance Advice
PaymentTypes	5	Request For Information
PaymentTypes	6	Payment Ack
PaymentTypes	7	Request For Payment
PaymentTypes	8	Request For Payment Response
PaymentTypes	9	Request For Information Response
PaymentTypes	10	Request For Payment Cancellation
PaymentTypes	99	Unknown

Payment Types

Type	Description
CreditTransfer	Payment sent by a Debtor FI to a Creditor FI.
ReturnRequest	The originator of the original payment is requesting the funds be returned. This is a non-monetary transaction. Sending a Return Request is not currently supported.
ReturnResponse	Response to a Return of Funds request. This is a non-monetary transaction. The actual money movement to return funds would be done in another payment as a credit transfer. This is a non-monetary transaction.
SystemTimeout	Notification to the Creditor FI that a Credit Transfer has timed-out This is a non-monetary transaction.
RemittanceAdvice*	The ability for the Debtor to send stand alone remittance information to the Creditor and the ability for the Creditor to send detailed invoice information to the Debtor (B2B or B2C). This is a non-monetary transaction.
RequestForInformation*	Used to request additional details related to a Credit Transfer or a Request for Payment that has been received. This is a non-monetary transaction.
PaymentAck*	A Creditor (end-user) may use a Payment Acknowledgement to acknowledge a Credit Transfer has been received and applied A Creditor FI must use a Payment Acknowledgement to confirm the funds associated with a Credit Transfer previously accepted without posting (ACWP transaction status), has posted to the Creditor's account. This is a non-monetary transaction.
RequestForPayment*	Requests the initiation of a Credit Transfer from the party receiving the request. This is a non-monetary transaction.
RequestForPaymentResponse*	Used to provide a business response to a Request for Payment. This is a non-monetary transaction.
RequestForInformationResponse*	Used by the sender to provide the requested additional information in the form of an amendment to the original Request for Payment or Credit Transfer. This is a non-monetary transaction.
Unknown	Payment type was not recognized

RtpTransactionStatus

Status of the payment, as set by the receiving institution. This applies to Credit Transfers and Requests for Payment.

Status	Description
ACTC	Payment has been accepted
RJCT	Payment or Payment Related Message has been rejected
RCVD	Payment Related Message has been received by the receiving institution
ACWP	Payment instruction included in the Credit Transfer is Accepted without being posted to the Creditor Customer's account.

Values for payment source

TypeName	Value	Description
PaymentSource	0	Phone
PaymentSource	1	Fax
PaymentSource	2	Email
PaymentSource	3	Clearing House
PaymentSource	4	Api
PaymentSource	5	Rtp System Timeout
PaymentSource	6	Ops Portal
PaymentSource	7	Partner Portal
PaymentSource	8	Return Of Funds
PaymentSource	9	Auto Resend

Reason Codes

Reason Codes provide the reason a message did not complete and can be found on the payment Result.Code. The Result.Code will be OK if the payment was successfully sent/received.

Code	Description
650	Cannot parse the message
690	Signature mismatch or verification error
BLKD	Payment has been blocked
AC02	Debtor account Is Invalid
AC03	Creditor account Is Invalid
AC04	Account closed
AC06	Account is blocked
AC07	Creditor account closed
AC10	Debtor account currency is invalid or missing
AC11	Creditor account currency is invalid or missing
AC13	Debtor account type missing or invalid
AC14	Creditor account type missing or invalid
AG01	Transaction is forbidden on this type of account
AG03	Transaction type is not supported/authorized on this account
AGNT	Incorrect Agent
AM02	Specific transaction/message amount is greater than allowed maximum
AM04	Amount of funds available to cover specified message amount is insufficient
AM09	Amount received is not the amount agreed or expected
AM11	Transaction currency is invalid or missing
AM12	Amount is invalid or missing
AM13	Transaction amount exceeds limits set by clearing system
AM14	Transaction Amount exceeds limits agreed between bank and client
BE04	Specification of creditor's address, which is required for payment, is missing / not correct
BE06	End customer specified is not known at associated Sort/National Bank Code or no longer exist in the books
BE07	Specification of debtor's address, which is required for payment, is missing / not correct
BE10	Debtor country code is missing or invalid
BE11	Creditor country code is missing or invalid
BE13	Country code of debtor's residence is missing or Invalid
BE14	Country code of creditor's residence is missing or Invalid
BE16	Debtor identification code missing or invalid
BE17	Creditor identification code missing or invalid

DS24	Waiting time expired due to incomplete order
DT04	Future date is not supported
DUPL	Payment is a duplicate of another payment

DS0H	Signer is not allowed to sign for this account
FF02	Syntax error reason is provided as narrative information in the additional reason information
FF03	Invalid Payment Type Information
FF08	End to End Id is missing or invalid
MD07	End customer is deceased
NARR	Reason is provided as narrative information in the additional reason information
RC01	Bank identifier code specified in the message has an incorrect format
RC02	Bank Identified is invalid or missing
RC03	Debtor FI identifier is invalid or missing
RC04	Creditor FI identifier is invalid or missing
TM01	Invalid Cut Off Time
TK01	Invalid Token
TK02	Sender Token Not Found
TK03	Receiver Token Not Found
TK04	Token Expired
TK05	Token Found with Counterparty Mismatch
TK06	Token Found with Value Limit Rule Violation
TK07	Single Use Token Already Used
TK08	Token Suspended
NOAT	Receiving Customer Account does not support/accept this message type
OK	Completed
1100	Any Other Reasons Reason is provided as narrativein the additional information
9909	Central Switch (RTP) system malfunction
9910	Instructed Agent signed-off
9912	Recipient connection is not available
9934	Instructing Agent signed-off
9946	Instructing Agent suspended
9947	Instructed Agent suspended
9948	Central Switch (RTP) service is suspended

ConfirmedAdditionalInfo values

2591366899	1000	RJCT	NARR	Transaction exceeds inbound payment amount velocity limit
2116822038	500	RJCT	DS24	NULL
2591366899	1000	RJCT	NARR	Transaction exceeds max inbound transfer amount of $5.00
2591366899	1000	RJCT	NARR	Transaction exceeds max inbound transfer amount of $5.00
2591366899	1000	RJCT	NARR	Transaction exceeds max inbound transfer amount of $5.00
2591366899	500	RJCT	NARR	Transaction exceeds inbound payment count velocity limit
2591366899	500	RJCT	NARR	Transaction exceeds inbound payment count velocity limit

Daily wire payments

Daily Wire Payment File Drop By Partner report.

Using the Cross River Operating System (COS) **wires APIs**, you can both originate and receive wire transfers through the Fedwire system. The level of information required varies depending on whether the transaction is purely domestic or international. Domestic wire payments require less information.

Term	Meaning
CR	Cross River
Partner	Cross River's immediate customer, i.e. you

Report details

The table below shows the different columns included in the report together with descriptions and explanations of the information they represent.

Column	Description
Id	Indicates which type of identification information is used. This will be shown as a single character as follows: • **B** - SWIFT Bank Identifier Code (BIC) • **C** - CHIPS Participant • **D** - Demand Deposit Account (DDA) Number • **F** - Fed Routing Number • **T** - SWIFT BIC or Bank Entity Identifier (BEI) and account number • **U** - CHIPS Identifier
AccountNumber	The number of the sub account under the Partner's relevant master account.
CoreTransactionId	
ReferenceId	
ClientBatchId	
ClientBatchSequence	
FedBatchId	
FedBatchSequence	
Direction	The direction of this transfer. The options are: • **Inbound**: a payment received from another bank. • **Outbound**: a payment being sent to another bank.
Source	
Status	Status indicates the payment status which could be: • **Created**: the payment has been received but hasn't been processed yet. This status will only appear briefly.

Column	Description
	Pending: the payment is waiting to be batched and sent to the through the Fedwire system. **Hold**: the payment is currently being held and is being reviewed by Cross River's Operations team. **Batched**: the payment has been batched, and CRB is carrying out a final review before the payment is sent in a batch file through the Fedwire system. **Processing**: For inbound payments, we are attempting to post the payment to the receiving account. For outbound payments, the payment has been sent to the FRB, but has not been posted yet. An outbound standard payment may remain in this status for a day or more. **Completed**: the payment has been posted and accepted by the FRB (in the case of outbound payments). This is a final status. **Canceled**: Indicates that an outbound payment has been canceled at the Partner's request. A payment can only be canceled while either pending or on hold. This is a final status. **Rejected**: Cross River's Operations team was unable to process the payment and has rejected it. For inbound payments, the payment request is returned to the originating bank. This is a final status.
PaymentType	A description of the payment type, which could be one of the following: **Transfer**: a new payment originating from either Cross River or another bank. Most payments are of this type. **Drawdown**: a request for a drawdown. **DrawdownResponse**: indicates the payment is a response to a drawdown request. **ServiceMessage**: This entry represents an informational message transferred between banks and not an actual payment. This is used when there's a relationship to a previously processed wire. **Reversal**: reversal of a previously sent wire payment.
Posting	
Purpose	

Column	Description
Amount	The transaction amount.
Currency	The currency the payment is being or was made in.
Imad	This is the mandatory unique number given to each Fedwire payment when using the Federal Reserve Bank Service. You can use this number to track your wire transfer. • **IMAD** indicates an inbound transfer • **OMAD** indicates an outbound transfer
Omad	
ReceiptDate	The date the payment was received.
ReceiptTime	The time of day the payment was received.
BusinessFunctionCode	This will always be shown as CTR for a customer transfer.
TypeCode	This column shows the type of transfer taking place and can show one of these codes: • **10**: indicates a funds transfer in which the sender and/or receiver may be a bank or a third party. • **15**: indicates a foreign-funds transfer to or from a foreign central bank or government, or an international organization with an account at the Federal Reserve Bank of New York. • **16**: indicates a settlement transfer with another Fedwire member.
SenderRoutingNumber	This is the sender's ABA number.
SenderName	The name of the party sending the transfer.
SenderReference	

Column	Description
ReceiverRoutingNumber	This is the receiver's ABA number.
ReceiverName	The name of the party receiving the transfer.
OriginatorToBeneficiary1	This is optional free-text information included by the originator to the beneficiary. An example could be:
OriginatorToBeneficiary2	
OriginatorToBeneficiary3	
OriginatorToBeneficiary4	
OriginatingFildCode	`"originatorToBeneficiary1": "THANK",` `"originatorToBeneficiary2": "YOU",` `"originatorToBeneficiary3": "PAID",` `"orginatorToBeneficiary4": "IN FULL",` This is the single-character code indicating the originating institution's type as follows: **B** - SWIFT Bank Identifier Code (BIC) **C** - CHIPS Participant **D** - Demand Deposit Account (DDA) Number **F** - Fed Routing Number **T** - SWIFT BIC or Bank Entity Identifier (BEI) and account number **U** - CHIPS Identifier

Column	Description
Originating FiIdentifier	This shows the originating institution's identifier as per the selected FiIdCode.
Originating FiName	The name of the originating party's financial institution.
Originating FiAddress1	Address details of the originating party's financial institution.
Originating FiAddress2	
Originating FiAddress3	
OriginatorIdCode	This is the single-character code to indicate the originator type. The code selected determines which identifier information must be used and is shown for the originator as follows: **B** - SWIFT Bank Identifier Code (BIC) **C** - CHIPS Participant **D** - Demand Deposit Account (DDA) Number **F** - Fed Routing Number **T** - SWIFT BIC or Bank Entity Identifier (BEI) and account number **U** - CHIPS Identifier **1** - Passport Number **2** - Tax Identification Number **3** - Driver's License Number **4** - Alien Registration Number **5** - Corporate Identification **9** - Other Identification
OriginatorIdentifier	This is the originator's ID information determined by the code used in the previous column.
Originator	The name of the party originating the transfer.

Column	Description
Name	
OriginatorAddress1	Address details of the originating party.
OriginatorAddress2	
OriginatorAddress3	
IntermediaryFildCode	This is the single-character code indicating the intermediary institution's type as follows: • **B** - SWIFT Bank Identifier Code (BIC) • **C** - CHIPS Participant • **D** - Demand Deposit Account (DDA) Number • **F** - Fed Routing Number • **T** - SWIFT BIC or Bank Entity Identifier (BEI) and account number • **U** - CHIPS Identifier
IntermediaryFildentifier	This shows the intermediary institution's identifier as per the selected FildCode.
IntermediaryFiName	The name of the intermediary financial institution. This will be empty If an intermediary institution is not being used for this transaction
IntermediaryFiAddress1	Address details of the intermediary financial institution.
IntermediaryFiAddress2	
IntermediaryFiAddress3	

Column	Description
Beneficiary FildCode	This is the single-character code indicating the beneficiary institution's type as follows: • **B** - SWIFT Bank Identifier Code (BIC) • **C** - CHIPS Participant • **D** - Demand Deposit Account (DDA) Number • **F** - Fed Routing Number • **T** - SWIFT BIC or Bank Entity Identifier (BEI) and account number • **U** - CHIPS Identifier
Beneficiary FiIdentifier	This shows the beneficiary institution's identifier as per the selected FildCode.
Beneficiary FiName	The name of the beneficiary party's financial institution.
Beneficiary FiAddress1	Address details of the beneficiary's financial institution.
Beneficiary FiAddress2	
Beneficiary FiAddress3	
Beneficiary IdCode	This is the single-character code to indicate the beneficiary type. The code selected determines which identifier information must be used and is shown for the beneficiary as follows: • **B** - SWIFT Bank Identifier Code (BIC) • **C** - CHIPS Participant • **D** - Demand Deposit Account (DDA) Number • **F** - Fed Routing Number • **T** - SWIFT BIC or Bank Entity Identifier (BEI) and account number • **U** - CHIPS Identifier • **1** - Passport Number • **2** - Tax Identification Number

Column	Description
	• **3** - Driver's License Number • **4** - Alien Registration Number • **5** - Corporate Identification • **9** - Other Identification
Beneficiary Identifier	This is the beneficiary's ID information determined by the code used in the previous column.
Beneficiary Name	The name of the beneficiary party.
Beneficiary Address1	Address details of the beneficiary party.
Beneficiary Address2	
Beneficiary Address3	
Beneficiary Reference	
ReleasedAt	The date and time the payment was **released**.
Processed At	The date and time the payment was **processed**.
EffectiveDate	The actual date the transaction was **posted**.
CreatedAt	The date and time the payment was **initiated**.
CanceledAt	The date and time the payment was **canceled**.
RejectedAt	The date and time the payment was **rejected**.
Completed At	The date and time the payment was **completed**.
PostedAt	The date and time the payment was **posted**.

Column	Description
OriginalPaymentId	
ProductId	The COS product identifier for the products included with your COS package.
PartnerId	The Partner's Cross River identification number.
LastModifiedAt	
InsertedAt	

Webhooks

Webhook Events Export File Drop By Partner report.

You can use **webhooks** within the Cross River Operating System (COS) to notify you when different events occur.

Report details

The table below shows the different columns included in the report together with descriptions and explanations of the information they represent.

Column	Description
EventId	The unique ID for the event.
EventName	The name of the event.
Status	This column shows the event status, which could be: • **Pending**: the event has been created, but no attempt to send it has been made yet. • **Success**: the event was successfully sent to the registered URL. • **Failed**: the event could not be delivered to the registered URL.
Resource	Refers to the resource relating to the event. For example, an account that was opened.
CreatedAt	The date and time the event was created.
LastAttempted At	The date and time the event was last sent.
PartnerId	The unique identification number for the partner resource.

This section describes the different webhook events you can register for. Where relevant, additional information is provided for some of the events.

5.2. Card payments

To assist partners with financial settlement and reconciliation, Cross River provides consolidated daily reports of payment transaction and chargeback activity.

In finance and accounting, financial settlement and reconciliation reporting are essential. Reporting involves verifying and balancing financial transactions. This ensures control, accuracy, and transparency in financial records.

Use daily reports to:

- Track the flow of money in and out of a business
- Identify any errors or discrepancies in financial records
- Prepare financial statements
- Comply with regulatory requirements
- Stay on top of chargeback status

Benefits

- Address potential risks
- Optimize cash flows
- Make strategic decisions in a timely way based on the organization's current financial position.

Daily report types

- **Settlements (detailed)**
- **Settlements (summary)**
- **Exceptions**
- **Chargebacks**

5.2.1. Daily settlement (detailed)

Daily pre-settlement reports help you match payments with the batches of transactions they relate to.

The *detailed* daily settlement report provides a breakdown of all the individual transactions occurring during a date range that you specify.

You receive this report using the Secure File Transfer Protocol (SFTP). **SFTP** lets you receive and send information securely.

This report is generated automatically, and pushed to your assigned subfolder on the secure server, where you access it.

> **IMPORTANT**
>
> SFTP must be **set up** *before* you create a report request with Cross River's Data Team. This allows the reporting team to automate the delivery of Settlement and Reconciliation reports to the appropriate folders.

Contact **ptpe.support@crossriver.com** if you have any issues accessing your reports.

Report distribution

Recipients include user-partners only.

Report structure

Detailed daily settlement reports have 2 structures: *basic* and *expanded*.

The basic report filename uses this convention:
PartnerName_CRB_Settlement_Details_YYYY_MM_DD

The expanded report filename uses this convention:
PartnerName_CRB_Settlement_ExpandedDetails_YYYY_MM_DD

Basic report structure

This table presents the basic report structure.

No.	Field	Default	Description
1	TransactionRequestId	✓	ID of the automatically created transaction associated with this settlement day
2	Network	✓	Card network the transaction was processed through
3	Response Code	✓	Card networks return response codes to approve or decline a transaction. They follow the standards set by the **International Organization for Standardization (ISO) 8583:1987**, which defines a specific message format so that different systems can communicate. Every network can adapt the standard for their own use
4	Response Description	✓	Card networks return response codes to approve or decline a transaction. They follow the standards set by the **International Organization for Standardization (ISO) 8583:1987**, which defines a specific message format so that different systems can communicate. Every network can adapt the standard for their own use
5	TransactionRequestedAt	✓	Time at which the transaction was requested by the partner. Dates in UTC.
6	ActualTransactionAt	✓	Time at which the transaction was processed by the network. Dates in UTC.
7	CreditCardId	✓	Token for the signed-up card. The partner gets this upon the first card sign-up, per each cardholder.
8	Retrieval Reference Number	✓	The transaction identifier vs. all parties, including the card networks. With the RRN, the partner can reach out directly to the network to get more info about the transaction.
9	TraceNumber	✓	CRB reference number: it is a unique number created in card transactions.

No.	Field	Default	Description
10	Statement Descriptor	✓	An arbitrary string attached to the transaction. Often useful for displaying to users.
11	Destination	✓	For Purchases: • AFT: Settlement For Disbursements • OCT: Network
12	Transaction Amount	✓	Transaction Amount. Passed in to Create Transactions APIs: • Push transactions (-) debit the account • Pull transactions (+) credit the account
13	InterchangeFee	✓	The fee paid to the issuer for each payment made with the card network. Every time a transaction is made via a card network (for example, Visa or Mastercard), the acquirer pays the cardholder's bank an interchange fee. The merchants then pays the interchange fee back to the acquirer.
14	InterchangeFeeIndicator	✓	**D** - Debit **C** - Credit
15	InterchangeCategoryDescriptor	✓	Interchange fee rate description (defined by the card networks)
16	EstimatedNetworkFee	✓	The fee paid to the card scheme for using their network. The fee is an accumulation of a set of charges based on the specific ac
17	NetworkFeeCode	✓	Visa network fees
18.	IntegrityNetworkFee		The Transaction Integrity Fee (TIF) is assessed on debit and prepaid card transactions that do not qualify for Custom Payment Service (CPS).

No.	Field	Default	Description
			The most common transaction to incur the transaction integrity fee will be keyed in debit card transactions that are processed without address verification information (AVS).
19	Settlement Date	✓	Cross River settlement date
20	CutoffDate	✓	The network cutoff date, according to each network
21	TransactionType	✓	• Pull - transfers funds from a funding account • Push - transfers funds to a receiving account • Reversal • Dispute

Expanded report structure

This table presents the expanded report structure.

No.	Field	Default	Description
1	TransactionRequestId	✓	ID of the automatically created transaction associated with this settlement day
2	Network	✓	Card network the transaction was processed through
3	ResponseCode	✓	Card networks return response codes to approve or decline a transaction. They follow the standards set by the **International Organization for Standardization (ISO) 8583:1987**, which defines a specific message format so that different systems can communicate. Every network can adapt the standard for their own use
4	ResponseDescription	✓	Card networks return response codes to approve or decline a transaction. They follow the standards set by the **International Organization for Standardization (ISO) 8583:1987**, which defines a specific message format so that different systems can communicate. Every network can adapt the standard for their own use
5	TransactionRequestedAt	✓	Time at which the transaction was requested by the partner. Dates in UTC.
6	ActualTransactionAt	✓	Time at which the transaction was processed by the network. Dates in UTC.
7	CreditCardId	✓	Token for the signed-up card. The partner gets this upon the first card sign-up, per each cardholder.
8	RetrievalReferenceNumber	✓	The transaction identifier vs. all parties, including the card networks. With the RRN, the partner can reach out directly to the network to get more info about the transaction.
9	TraceNumber	✓	Cross River reference number: it is a unique number created in card transactions.

No.	Field	Default	Description
10	Statement Descriptor	✓	An arbitrary string attached to the transaction. Often useful for displaying to users.
11	TransactionType	✓	1. Pull - Transaction to transfer funds from a funding account 2. Push - Payment transaction to transfer funds to a receiving account 3. Reversal 4. Dispute
12	Destination	✓	
13	Transaction Amount	✓	Transaction Amount. Passed in to Create Transactions APIs: • Push transactions (-) debit the account • Pull transactions (+) credit the account
14	TransactionCurrency	✓	The beneficiary currency
15	InterchangeFee	✓	The fee paid to the issuer for each payment made with the card network. Every time a transaction is made via a card network (for example Visa orMastercard), the acquirer pays the cardholder's bank an interchange fee. The merchants then pays the interchange fee back to the acquirer.
16	InterchangeFeeIndicator	✓	**D** - debit **C** - credit
17	InterchangeCategoryDescriptor	✓	Interchange fee rate description (defined by the card networks)

No.	Field	Default	Description
18	Estimated NetworkFee	✓	The fee paid to the card scheme for using their network. The fee is an accumulation of a set of charges based on the specific ac
19	NetworkFeeCode	✓	Visa network fees
20	IntegrityNetworkFee		The Transaction Integrity Fee (TIF) will be assessed on debit and prepaid card transactions that do not qualify for Custom Payment Service (CPS). The most common transaction to incur the transaction integrity fee will be keyed in debit card transactions that are processed without address verification information (AVS).
21	Settlement Date	✓	CRB settlement date
22	CutoffDate	✓	The network cutoff date, according to each network
23	CardBrand	✓	The brand of the card used in the transaction
24	CardProductType	✓	The type of card used in the transaction: • Unknown • Credit • Debit • Prepaid • Combo • Charge Card • Deferred Debit
25	FirstName		The cardholder's first name
26	LastName		The cardholder's last name
27	First6		The first 6 digits of the card used in the transaction (same as BIN).

No.	Field	Default	Description
25	Last4		The last 4 digits of the card used in the transaction
26	IssuerCountryCode		The country of the card's issuer

Related topics

- **Daily settlement (summary)**
- **Daily exceptions**
- **Daily chargeback report**
- **Send funds to payee (push) API**
- **Request funds from payer (pull) API**

5.2.2. Daily settlement (summary)

Introduction

Daily pre-settlement reports help you match payments with the batches of transactions to which they relate.

The daily settlement summary report shows the following. This reflects the settlement transactions to be transferred on this particular day:

- Starting and ending balance held at Cross River for a stated date range
- A high-level summary of merchant partner activity during that range.

Together, these reflect the settlement transactions to be transferred on this day.

Report generated?

Every day that Cross River settles funds. This is the day that the bank settles transactions with the merchant partner.

Sent and received

- By email
- Via **SFTP** file export

Report file format

PartnerName_CRBPayments_Settlement_Summary_YYYY_MM_DD

Report structure

Aggregation level: Networks

<u>Fields</u>: Report Date, Total Settlement Amount, Daily Limit, Amount Balance, Required Replenishment, etc.

<LOGO>	Merchant Transactions Total			
Totals				
Report Date	**Total Settlement Amount**	**Daily Limit**	**Account Balance**	**Required Replenishment**
04/24/2023	$443,340.12	N/A	49,959,212.00	N/A

Card Network "A"

Report Date	**Network**		**Count Transactions**	**Amount**
04/24/2023	Original Credit		2,044.00	$ 295,051.27
04/24/2023	Interchange			$ 0.10
04/24/2023	Visa Charges			0.00$
	Total		**2044**	**$ 295,051.27**

Card Network "B"

Report Date	**Network**		**Count Transactions**	**Amount**
04/24/2023	Original Credit		2,044.00	$ 295,051.27
04/24/2023	Interchange			$ 0.10
	Total		**2044**	**$ 295,051.27**

Card Network "C" [*]

Report Date	**Network**		**Count Transactions**	**Amount**
04/24/2023	Original Credit		2,044.00	1,849.00
04/24/2023	Interchange			
	Total		**2044**	**1,849.00**

* This could be any of the card networks listed in theNetwork Identification supplement.

Related topics

- **Daily settlement (detailed)**
- **Daily exceptions**
- **Daily chargeback report**

- **Send funds to payee (push) API**
- **Request funds from payer (pull) API**

5.2.3. Daily exceptions

The daily exceptions report lists the transactions that contain irregularities.

This report includes unprocessed, incomplete, interrupted, or suspicious transactions. It also contains transactions with unusual balances. In addition, this report could hold mismatches or conflicts between data in the Cross River and the card networks. These could be, for example, transaction status, amounts, and so forth.

Unlike the daily settlement report, where you trigger each transaction, exceptions are triggered by another person, event or action, and are unexpected.

Cross River generates a daily exception report every day that we settle transactions with merchant partners.

You receive this report using the Secure File Transfer Protocol (SFTP). **SFTP** lets you receive and send information securely.

This report is generated automatically, and pushed to your assigned subfolder on the secure server, where you access it.

> **IMPORTANT**
> SFTP must be set up *before* you create a report request with Cross River's Data Team. This allows the reporting team to automate the delivery of Settlement and Reconciliation reports to the appropriate folders.

Report distribution

Recipients include user-partners only.

Report structure

Detailed daily exception reports have 2 structures: *basic* and *expanded*.

The basic report filename uses this convention:

PartnerName_CRBPayments_Exceptions_Itemized_YYYY_MM_DD

The expanded report filename uses this convention:

PartnerName_CRB_Settlement_Exceptions_Expanded_YYYY-MM-DD

Basic report structure

No.	Field	Default	Description
1	ExceptionID	✓	
2	ExceptionCode	✓	
3	OriginalTransaction RequestId	✓	ID of the automatically created transaction associated with this settlement day
4	Network	✓	
5	ResponseCode	✓	
6	TransactionType	✓	- Pull - Push - Chargeback - Reversal - Adjustment
7	ResponseDescription	✓	
8	TransactionRequestedAt	✓	
9	OriginalTransaction RequestedAt	✓	
10	CreditCardId	✓	
11	RetrievalReference	✓	
12	TraceNumber	✓	
13	Destination*	✓	- For AFT: Settlement - For OCT: Network
14	TransactionAmount	✓	
15	TransactionIndicator	✓	
16	OriginalCurrency	✓	

No.	Field	Default	Description
17	InterchangeFee	✓	
18	InterchangeFeeIndicator	✓	
19	InterchangeCategoryDescriptor	✓	
20	EstimatedNetworkFee	✓	
21	IntegrityNetworkFee	✓	
22	IntegrityNetworkFee	✓	
23	SettlementDate	✓	
24	CutoffDate	✓	

Expanded report structure

No.	Field	Default	Description

No.	Field	Default	Description
1	ExceptionID	✓	
2	ExceptionCode	✓	
3	OriginalTransactionRequestId	✓	ID of the automatically created transaction associated with this settlement day
4	Network	✓	
5	ResponseCode	✓	
6	TransactionType	✓	- Pull - Push - Chargeback - Reversal - Adjustment
7	ResponseDescription	✓	
8	TransactionRequestedAt	✓	
9	OriginalTransactionRequestedAt	✓	
10	CreditCardId	✓	
11	RetrievalReference	✓	
12	TraceNumber	✓	
13	Destination*	✓	For AFT: Settlement

No.	Field	Default	Description
			• For OCT: Network
14	TransactionAmount	✓	Transaction Amount
15	TransactionIndicator	✓	• **D** - Debit the merchant • **C** - Credit the merchant
16	OriginalCurrency	✓	
17	InterchangeFee	✓	
18	InterchangeFeeIndicator	✓	
19	InterchangeCategoryDescriptor	✓	
20	EstimatedNetworkFee	✓	
21	IntegrityNetworkFee	✓	
22	IntegrityNetworkFee	✓	
23	SettlementDate	✓	CRB Settlement Date
24	CutoffDate	✓	
25	CardholderFirstName	✓	Cardholder First Name
26	CardholderLastName	✓	Cardholder Last Name

No.	Field	Default	Description
27	IssuerCountryCode	✓	Card issuer country code
28	SystemTraceAuditNumber	✓	A unique Cross River reference number created in card transactions
29	RetrievalReference	✓	The transaction identifier vs. all parties, including the card networks. Using this number, the partner can directly reach out to the network to get more info about the transaction.
30	StatementDescriptor		An arbitrary string attached to the transaction, often useful for displaying to information users
31	CardType	✓	Debit/Credit/Prepaid
32	Credit Card Id	✓	Token for the signed-up card. The partner gets this Id upon first-time card sign-up, per each card holder.
33	First6	✓	First 6 digits of the payment card
34	Last4	✓	Last 4 digits of the payment card

Related topics

- **Daily settlement (detailed)**
- **Daily settlement (summary)**
- **Daily chargeback report**
- **Send funds to payee (push) API**
- **Request funds from payer (pull) API**

Daily chargeback report

Daily chargeback reports help you review and manage chargeback cases. This is not a financial report. Both new chargebacks and updates for ongoing cases appear in the same report file.

You receive this report using the Secure File Transfer Protocol (SFTP). **SFTP** lets you receive and send information securely.

This report is generated automatically, and pushed to your assigned subfolder on the secure server, where you access it.

> **IMPORTANT**
> SFTP must be set up *before* you create a report request with Cross River's Data Team. This allows the reporting team to automate the delivery of Settlement and Reconciliation reports to the appropriate folders.

Report distribution

Recipients include user-partners only.

Report structure

The chargeback report filename uses this convention:
PartnerName_CRB_Chargebacks_Details_YYYY-MM-DD.csv

The chargeback report structure includes the fields presented here.

No.	Field	Required	Default	Description
1	CRBChargebackId	✓		Unique reference number generated by Cross River for each chargeback case, used as the name of the evidence artifact
2	ExternalVendorID	✓		
3	**ChargebackState**	✓		1. First chargeback (new chargeback) 2. Representment (merchant provided compelling evidence the next day etc) 3. Incoming pre-arbitration (MC) 4. Outgoing pre-arbitration (Visa) [out to the issuer]
4	OriginalTransactionRequestId	✓		ID of the automatically created transaction associated with this settlement day - **ARN**
5	ReasonCode			Network-specific reason code that identifies the evidence the merchant must provide to win the case
6	ReasonDescription			Description corresponding to the network Exception Code
7	ChargebackRequestedAt			Timing of the dispute request
8	DaysOutstanding			Days since dispute was opened
9	**Resolution Type**			
10	Adjustment Type		Financial record	Debit\Credit

No.	Field	Required	Default	Description
	→ when is populated - Recon should consume			
11	Adjustment Amount → when is populated - Recon should consume		Financial record	AdjustmentAmount→2000 ChargebackAmount→5000 TransactionAmount→7000
12	**ActionStatus**			
13	LastStatus Date			Date of most recent change in Action Status
14	CreditCardId	✓		Token for the signed-up card, received when you first sign up the card. One token per card holder.
15	Chargeback Amount			Amount disputed by cardholder. May differ from the Original Settled Amount in the case of a partial chargeback or due to differences in the exchange rate.
16	Network	✓		Card network the transaction was processed through
17	OriginalTransactionResponseCode	✓		Original transaction - Card networks return response codes to approve or decline a transaction. They follow the standards set by ISO 8583:1987, which defines a specific message format so that different systems can

No.	Field	Required	Default	Description
				communicate. Every network can adapt the standard for their own use
18	OriginalTransactionResponseDescription	✓		Original transaction - Card networks return response codes to approve or decline a transaction. They follow the standards set by the International Organization for Standardization (ISO) 8583:1987, which defines a specific message format so that different systems can communicate. Every network can adapt the standard for their own use.
19	OriginalTransactionRequestedAt	✓		Time when the transaction was requested by the partner. Dates in UTC.
20	OriginalActualTransactionAt	✓		Time at which the transaction was processed by the network. Dates in UTC.
21	RetrievalReference	✓		RRN
22	NetworkIdentifier	✓		Network transaction identifier
23	OriginalTransactionAmount	✓		Transaction Amount. Passed in to Create Transactions APIs • Push transactions are (-) • Pull transactions are (+)
24	NetworkFee			
25	InterchangeFee			Interchange fee

No.	Field	Required	Default	Description
26	OriginalTranscationType	✓		• **Pull** • *Push* • *Reversal* • *Dispute*
27	FirstName			
28	LastName			
29	CardBrand			
30	CardProductType			
31	First6			
32	Last4			
33	EvidenceInstructions			Default-Empty

Complex field values

This section presents possible values for specific fields when they include a large number of possible values.

Chargeback state types

This table shows you values for the `ChargebackState` field. The type explains the stage of processing the chargeback reached at report generation time.

No.	Dispute state type	CB Type Description	Financial	Comments
1	First Chargeback	Initial Chargeback	✓	Settlement file is already debited
2	Merchant Response Review	Merchant Response received and under review		
3	Outgoing Pre-Arbitration	Merchant Response was accepted and Outgoing Pre-Arb was created and submitted to Issuer (Visa Allocation Disputes only)		
4	Representme nt	Merchant Response was accepted and Representment was processed	✓	
5	Incoming Pre-Arbitration	Issuer has responded to previously processed Representment and has submitted a Cardholder response via an Incoming Pre-Arbitration	✓	
6	Arbitration	An Arbitration Ruling has been filed by either the Issuer or Acquirer		
7	Outgoing Pre-Compliance	Acquirer has submitted a Pre-Compliance request to the Issuer		
8	Incoming Pre-Compliance	Issuer has submitted a Pre-Compliance request to the Acquirer		If the merchant accept it - it becomes financial(step 5)

No.	Dispute state type	CB Type Description	Financial	Comments
9	Compliance	A Compliance Ruling has been filed by either the Issuer or Acquirer		
10	GFC	Good Faith Collection has been submitted by either the Issuer or Acquirer		
11	Chargeback Reversal	See ARN and Internal Case# for reference to original Chargeback	✓	(The issuer recalled it within 3 days)
12	Duplicate Chargeback	See ARN and Internal Case# for reference to original Chargeback	✓	Imminently "fight" it and get the money back

Resolution types

This table shows you values for the `ResolutionType` field. Resolutions are different ways a chargeback case is finished.

No.	Resolution Type	Resolution Type Description
1	Resolved to Merchant	Merchant is liable - see ActionStatus for next steps
2	Resolved to Issuer	Issuer is liable - See ActionStatus for update
3	Resolved to Write Off	Acquirer/Processor is liable
4	Merchant Response Denied	Submitted Merchant Response has been denied - See Action Status and Custom Filed for Reason
5	Pending (see Action Status)	Case is pending an external action - See Action Status and Custom Field for Reason
6	Issuer Denied Pre-Arb/Comp	See Action Status and Custom Field for Reason and Next Steps
7	Issuer Accepted Pre-Arb/Comp	Issuer has accepted liability
8	Acquirer Denied Pre-Arb/Comp	Acquirer has denied incoming case. Pending response from Issuer
9	Acquirer Accepted Pre-Arb/Comp	Acquirer has accepted liability on behalf of the merchant
10	Arb/Comp Ruling in Issuer Favor	Issuer has been deemed liable for the dispute
11	Arb/Comp Ruling in Acquirer Favor	Acquirer has been deemed liable for the dispute
12	Arb/Comp Ruling Withdrawn by Issuer	Issuer has withdrawn request for case ruling and has accepted dispute liability
13	Arb/Comp Ruling Withdrawn by Acquirer	Acquirer has withdrawn request for case ruling and has accepted dispute liability on behalf of the merchant
14	GFC Accepted by Issuer	Issuer has accepted liability
15	GFC Accepted by Acquirer	Acquirer has accepted liability on behalf of the merchant

Actions

This table shows you values for the `ActionStatus` field. The action status inform you what you need to do next, or what was done last.

No.	Action	Action Description
1	Case Closed in Issuer's favor - No Further Recourse	See Custom Field for explanation
2	Case Closed in Merchant's favor - Time Elapsed	Merchant win
3	Merchant Response Needed - See Reason Code	Required Compelling Evidence can be inferred from Dispute Reason Code
4	Merchant Response Needed - See Custom Field	Specific information is required of the merchant - please see custom field
5	Outgoing Pre-Arb Sent to Issuer Pending Issuer Response	Issuer has up to 30 days to respond
6	Outgoing Pre-Comp Sent to Issuer Pending Issuer Response	Issuer has up to 30 days to respond
7	Representment Processed back to Issuer	Issuer has 30-45 days to repsonse with an incoming Pre-Arb
8	Merchant Response needed for Incoming Pre-Arb/Comp	See Custom Field for explanation
9	Reversal processed to offset most recent Process	See Chargeback Type (First Chargeback or Representment)

Related topics

- **Daily settlement (detailed)**
- **Daily settlement (summary)**
- **Daily exceptions**
- **Send funds to payee (push) API**

- **Request funds from payer (pull) API**

Credit risk data reports

As a Cross River credit BIN sponsorship partner, we need you to send us a monthly summary of specific credit risk metrics that are not visible to us. To make things easy, we've got a common data exchange format (.csv - comma-separated values) for you to use. This page will walk you through the metrics you need to share with us, the data exchange format, and how to send the file our way.

Before you begin

- Ensure you've submitted the complete **IP Access Request for CRB SFTP Services** form. Get this form from your CR Implementation or Relationship Manager. When Cross River gets your completed form, we begin the process of setting up your SFTP access. Learn more about **SFTP** setup.

- Once you are set up for SFTP, ensure you have a **\ClientCredit** subfolder in your Cross River SFTP folder. This is where you'll put your csv file. CR provides you with the full path when you get your access credentials. Contact your Relationship Manager with any questions.

File structure

The credit risk metrics file must be formatted in a specific way. To prepare the credit risk metrics file:

- **Use this file naming convention**:
  CreditRiskMetrics_PartnerAbbreviation_datetimestamp.csv
  Use a 3- to 6-character string for the PartnerAbbreviation is that clearly refers your organization, and that Cross River will understand. Format the *datetimestamp* as **yyyymmddhhmm**. If the date and time stamp is automated, the format can include seconds.

- **Use this file format/delimiter**: .csv (comma-separated values)

- **File header**: Use these and only these column names in your file: `COSPartnerID`, `MetricMonth`, `MetricAbbrev`, `MetricValue`

- **File footer**: Do not include a footer.

- **Build the file**:
  Each row/record in the .CSV represents a single monthly credit risk metric value. Each record you send must include entries each of these 4 columns: `COSPartnerID`, `MetricMonth`, `MetricAbbrev`, and `MetricValue`. The table below explains them in detail. List the metrics in whatever order you like. No specific order is required.
  Cross River BIN Sponsor card programs can vary. You still need to send the entire list of metrics, even if a given metric isn't relevant. If a metric does not apply, give it a `MetricValue` of **0**.
  Your relationship manager will work with Cross River's Credit Risk team to answer any questions about determining applicable metrics for your program.

Sequence/Position	Column	Description	Format
1	`COSPartnerID`	Your Cross River partner ID supplied to you by us. This ID acts as a unique identifier for you so we know which partner supplied the credit risk metrics	GUID (36 characters)
2	`MetricMonth`	The month the credit risk metric record is for. This value is the last day of the month the report covers	YYYY-MM-DD (last day of the month)
4	`MetricValue`	The actual credit risk metric supplied as a number (either a count of a metric or a dollar ($) amount)	Must be a number

Metric abbreviation catalog

Metric	Abbreviation	Description	Metric Type ($ amount or Count)
Total apps received	TAR	Number of completed applications (number of Pending, Declined, and approved together should equal the number of Total Apps received)	Count
Total apps pending	TAP	Number of completed applications that are pending	Count
Total apps incomplete	TAI	Number of incomplete applications	Count
Total apps declined	TAD	Number of declined applications	Count
Total approvals	TAA	Number of approved applications	Count
Total subprime approvals (if applicable to your program)	TSA	Number of subprime approvals (Less than 660 FICO or equivalent).	Count
Total application declines overridden/exceptions	TADO	Number of applications initially declined and later judgmentally reviewed and approved (Bank may request for exception/overridden reason).	Count
Average Limit Assigned	ALA	Average of all customers' credit limit amounts at end-of-month	$ amount
$ Total Credit Limit/Exposure	TCL	Total of all credit limit amounts at end-of-month	$ amount
$ Highest Credit Limit	HCL	Highest credit limit amount at end-of-month	$ amount
$ Month End Balance (total outstanding/acc	MEB	Total balance at end-of-month	$ amount

Metric	Abbreviation	Description	Metric Type ($ amount or Count)
ount receivables)			
$ First Pay Default	FPD	Sum of past-due balances from cardholders who failed to make their first payment on or before their scheduled due date, given that Cross River's issuing program supports only 1 repayment cycle	$ amount
$ Balances 30 DPD	B3DPD	Sum of balances 30 days past due	$ amount
$ Balances 60 DPD	B6DPD	Sum of balances 60 days past due	$ amount
$ Balances 90 DPD	B9DPD	Sum of balances 90 days past due	$ amount
$ Balances Charged Off	BCO	Sum of charged-off balances	$ amount
$ Fraud Losses	TFL	Sum of fraud losses	$ amount
# of total Cardholders	NTC	Number of cardholders regardless of status	Count
Number of open cards	NOC	Number of open cards (exclude lost or stolen, fraud, closed, or charged off cards)	Count
Number of cards issued	NCI	Number of cards issued (both reissued and new cardholders)	Count
Number of Auth Prohibited Cards	NAPC	Number of cards with status Authorization Prohibited	Count
# First Pay Default	NFPD	Number of cardholders who failed to pay balance amount in full before or on due date	Count

Metric	Abbreviation	Description	Metric Type ($ amount or Count)
# Cardholders 30 DPD	C3DPD	Number of cardholders 30 days past due	Count
# Cardholders 60 DPD	C6DPD	Number of cardholders 60 days past due	Count
# Cardholders 90 DPD	C9DPD	Number of cardholders 90 days past due	Count
# Cardholders Charged Off	CCO	Number of cardholder charge-offs	Count
# of Reages	NOR	Number of re-ages (If your program practices re-aging, supply the number of re-aged accounts completed)	Count
# of Hardship/Forbearance Enrollments	NOH	Number of hardship/forbearance enrollments	Count
# Overlimit Cardholders	NOCL	Number of accounts over assigned credit limit	Count
$ All Balances Overlimit	BOCL	Sum of balances over assigned credit limit	$ amount
Requested Credit Limit Increases Approved	CLIA	Total approved credit limit requests by cardholders	Count
Voluntary Credit Limit Decreases Approved	CLDA	Total approved credit limit decrease requests by cardholder	Count
Requested Credit Limit	CLID	Number of declined credit limit requests by cardholder	Count

Metric	Abbreviation	Description	Metric Type ($ amount or Count)
Increases Declined			
Involuntary Credit Limit Decreases	CLDD	Number of declined credit limits conducted by Program Manager	Count
Proactive credit line increase Approved	PCLIA	Number of approved credit limits initiated by Program Manager	Count
# Primary Account Cardholder Closures	NACL	Number of primary account cardholder closure requests by cardholder	Count
# Involuntary Account Closure	NICL	Accounts involuntarily closed due to bad behavior/adverse action	Count
# Total Inactive Accounts	TIA	Accounts without a balance in current and prior cycle	Count
# Pricing Changes (increases/decreases)	NPC	Number of pricing changes made to an account(s)	Count
# Total Monthly Refunds	NMR	Number of monthly refunds	Count
$ Total Monthly Refunds	TMR	Sum of monthly refunds	$ amount
# Total Monthly Sales	NMS	Number of monthly purchase transactions	Count
$ Total Monthly Sales	TMS	Sum of monthly purchase transactions	$ amount

Metric	Abbreviation	Description	Metric Type ($ amount or Count)
$ Total Cardholder payments in Month	TCP	Sum of all monthly payments	$ amount
$ Interchange Income	TII	Sum of interchange income	$ amount
$ Fee Income	TFI	Sum of fee income (if applicable to program)	$ amount
$ Interest Income	TIIN	Sum of monthly interest	$ amount
Number of cardholder sent to external collection Agency	COLL	Number of accounts reported to an external collection agency	Count
Funding Direct Utilized (= on Program Manager Balance Sheet)*	FDU	Sum of receivables on your program's balance sheet	$ amount
Funding Partner Utilized (= on Funding Partner's Balance Sheet)*	FPU	Sum of receivables on any third-party balance sheet	$ amount
Total Partner(s) Funding Utilized $	TPFU	Sum utilized for all card receivables on a third-party balance sheet	$ amount

Metric	Abbreviation	Description	Metric Type ($ amount or Count)
Funding Partner available $	FPA	Total presently available on a third-party balance sheet for card receivables	$ amount
$ Recoveries	TAMR	Amount recovered from charged-off/write-off	$ amount
# Disputes	TND	Number of disputed transactions	Count
$ Disputes	TAMD	Total balance from disputed transactions	$ amount
# Chargeback	TNC	Number of chargeback transactions	Count
$ Chargeback	TAMC	Total balance from chargeback transactions	$ amount
$ Securitization Activity	MSA	Total amount securitized monthly (If you issue credit securitized by an asset, such as a car value, total amount of those values)	$ amount
# Cardholders in Promo Rate	PR	Number of cardholders in a promotional rate period	Count
$ Aged Write-offs	AAWO	Total amount of aged write-offs in a month	$ amount
# Aged Write-offs	CAWO	Number of aged write-offs in a month	Count
$ Bankruptcy Write-offs	ABWO	Total amount of bankruptcy write-offs in a month	$ amount
# Bankruptcy Write-offs	CBWO	Number of bankruptcy write-offs in a month	Count
$ Deceased Write-offs	ADWO	Total amount of deceased write-offs in a month	$ amount
# Deceased Write-offs	CDWO	Number of deceased write-offs in a month	Count

Metric	Abbreviation	Description	Metric Type ($ amount or Count)
$ Fraud Write-offs	AFWO	Total amount of fraud write-offs in a month	$ amount
# Fraud Write-offs	CFWO	Number of fraud write-offs in a month	Count
$ Rewards Issued	RI	Total amount of rewards/points issued in a month	$ amount
$ Rewards Reversed	RR	Total amount of rewards/points reversed in a month	$ amount
$ Rewards Redeemed	RREDM	Total amount of rewards/points redeemed in a month	$ amount
$ Rewards Outstanding Liability	ROL	Total amount of outstanding rewards/points liability	$ amount
Total Collateral Value	TCL	Total collateral value on book	$ amount
$ Statement Credit Issued	SCI	Total amount of statement credit issued in a month	$ amount

Sample file

The sample below presents the monthly credit risk metric report from a fictitious Cross River partner, **ABCD, Inc**, partner ID **a926ccfc-3cba-4a59-b3f8-c4d4b277f61f**, for the month of July 2023.

File Name: CreditRiskMetrics_ABCD_202308291005

File Format: .csv

```
COSPartnerID,MetricMonth,MetricAbbrev,MetricValue
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,TAR,1513
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,TAP,0
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,TAI,4
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,TAD,604
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,TAA,905
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,TSA,0
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,TADO,0
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,ALA,5500
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,TCL,17500000
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,HCL,10000
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,MEB,350000
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,FPD,15000
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,B3DPD,50000
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,B6DPD,3000
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,B9DPD,200
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,BCO,1400
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,TFL,15000
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,NTC,30000
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,NOC,1500
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,NCI,45000
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,NAPC,0
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,NFPD,14
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,C3DPD,100
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,C6DPD,37
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,C9DPD,2
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,CCO,204
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,NOR,0
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,NOH,0
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,NOCL,68
a926ccfc-3cba-4a59-b3f8-c4d4b277f61f,2023-07-31,BOCL,6809.75
```

Ln 1, Col 1   100%   Windows (CRLF)   UTF-8

Download the file:

📄 **CreditRiskMetrics_ABCD_202308291005...**   ⬇

Duplicate value handling

If in the same month you provide a new monthly metric value for a metric that has already been received, Cross River uses only the most-recently provided metric value for that month.

File share method

Share the .csv file monthly.

Upload the file using **SFTP** to your **\ClientCredit** subfolder.

> If you do not yet have an SFTP folder with Cross River, contact your Cross River relationship manager. They will help set you up.

Troubleshooting

Issue	Resolution
You don't know your Partner ID	Request your Partner ID form your relationship manager
You are notified by Cross River that there's a problem with the .csv file	If your .csv file has problems, Cross River will let you know what they are and how to fix them

- In general, before sending, check these values for validity:
- Filename is formatted correctly
- For each record:
    - Partner GUID is correct
    - Month end date is correct and in the correct format
    - Metric Abbreviation is a valid one from provided list
    - MetricValue is expressed as a number

5.4. Lending reports

To access the Arix SFTP:

1. **Set up SFTP with Cross River**.

2. Access your SFTP folder using the credentials and information you receive from your Relationship Manager.

> To transfer the files securely, you must use a client that supports SSH with the following public-key algorithms:
>
> - RSA
> - sha2 521
> - sha2 384
> - sha 256

These loan reports are available:

- **Servicing**
- **Transaction**

6. API Basics

- **Structure**: Our APIs are organized around REST, have object oriented URLs, accept form-encoded request bodies, return JSON-encoded responses, and use standard HTTP response codes, authentication, and methods.

- **Static IPs**: At Cross River you need to allowlist your *static*, *public* IP address before you can access our products. Your IP is allowlisted as part of the partner onboarding process.

- **Idempotency**: Cross River's COS system supports idempotency to retry requests without the risk of performing the request multiple times. This is especially useful in situations where there is a network outage, and you aren't sure if a previous request has been processed successfully.

- **Pagination**: Pagination is a process that divides a large dataset into smaller chunks. All endpoints that return a list of resources support pagination.

- **API versioning**: All API endpoints contain a numbered version in the URL. Whenever breaking changes are made to the API, a new major version will be created.

- **HTTP status codes**: Standard HTTP status codes that our system might return.

6.1. Structure

At Cross River, we have a robust set of APIs spanning our suite of products. To access our APIs and try them out in our sandbox, contact Integration Support to get started.

Our APIs are organized around REST, have object oriented URLs, accept form-encoded request bodies, return JSON-encoded responses, and use standard HTTP response codes, authentication, and methods.

When you call an API, you've sent a request. The answer you receive back is the response.

Resource/object

A resource (object) is the category of information that you want to receive information for, via API. For example, in our P2C product, a card and a transaction are resources, and in our lending product, a loan is a resource.

Endpoints and methods

- An endpoint is the URL address of an API that you want to retrieve. You can retrieve an endpoint by using a method.

- The method is the prefix you add to your endpoint to send the relevant API request. They are:

Prefix	Description
GET	A GET request retrieves resource information. A GET request never has a body.
POST	A POST request adds or creates a resource.
PUT	A PUT request updates or fixes resource information.
DELETE	A DELETE request deletes or cancels a resource.
PATCH	A PATCH request updates or fixes a smaller scope of resource information.

Parameters

There are 3 types of parameters:

Path

A path parameter can be added to a URL endpoint to return a specific response. The path parameter is added to the URL in curly brackets (**{ }**) and follows a backslash (**/**).

For example, if you want to retrieve specific information on an account, you can add `/{accountnumber}` to the URL.

When your API includes curly brackets, a path parameter is required.

Body

Body parameters are the data included in the body of an API, and the information they represent can be changed. The body of the request and response messages are called payloads.

Query

A query parameter narrows down and filters the results of your request based on the information you are requesting. The query parameter is added to the URL and follows a question mark (**?**). Only GET calls use query parameters.

Request headers

A request header is an HTTP header used in a request that provides information about the request context. It let's the server tailor the response.

In our documentation requests are presented in cURL.

Header	Description
`Authorization: {bearer token}`	Authorization credentials for HTTP authentication. Include the bearer token in the `Authorization` header.
`Content-Type`	Required for operations with a request body such as POST and PUT requests. The value is `application/json` indicating that the request body format is JSON. • To override the `Content-type` in your clients, use the `Accept` header, append the .json suffix or `?format=json` • To embed the response in a JSON callback, append `?callback=myCallback`
`Accept: application/json`	Sets the output type to JSON.

```Curl
curl --location --request GET 'https://cr-sandbox-domain/{xxx}
--header 'Accept: application/json'
--header 'Authorization: {Bearer token}' 'https://cr-sandbox-domain/'
```

Request ID

For every request, the response header contains a Requst-ID value. This unique identifier is used by the Cross River Support Team for troubleshooting. We strongly recommend you save this identifier.

Next steps

When you're ready to start trying out our APIs, follow these steps:

1. **Get API credentials**
2. **Get an access token** (a bearer token).
3. **Use the access token**

4. Start calling our **APIs**.

6.2. Static IPs

At Cross River you need to allowlist your *static*, *public* IP address before you can access our products. Your IP is allowlisted as part of the partner onboarding process.

A static IP address, as opposed to a dynamic IP address, is a permanent, non-changing network address that identifies a device on the internet. It is a 32 bit number in the form of a dotted quad (IPv4 format), for example, 192.168.0.12. A static IP address is typically provided by an internet service provider and informs servers of the location of a specific device.

A public IP address is an external-facing IP address used to access the Internet. Public IP addresses are provided by the internet service provider (ISP) and assigned to the router. It is a unique IP address on the internet.

To make sure that you provide us with the correct IP address we recommend that you speak with your company's internal IT department. They should provide you with the correct IP address to allowlist.

> Cross River Support cannot assist you in finding your public, static IP address.

6.3. Idempotency

> **IMPORTANT**
>
> Idempotency keys are not applicable to Marketplace Lending (Arix) users.
>
> For Arix, duplicate protection is built into the compliance engine to help prevent double funding.

Our system supports idempotency to retry requests without the risk of performing the request multiple times. This is especially useful in situations where there is a network outage, and you aren't sure if a previous request has been processed successfully.

With an idempotency key, a unique value generated by the client, our server recognizes subsequent retries of the same request. This guarantees that retrying a request with the same idempotency key doesn't result in another execution of the endpoint.

How it works

In API design, idempotency ensures that making the same request multiple times results in the same outcome as making it once. This is especially useful in scenarios where a client retries a request due to a network timeout or an uncertain response.

Idempotency saves the resulting status code and body of the first request made for any given idempotency key, regardless of whether it succeeded or failed. Subsequent requests with the same idempotency key return the same cached results of the original request, including errors.

For example, if a client sends a request to deposit a check or initiate a payment, an idempotent API prevents the operation from being processed more than once—even if the client resends the same request.

By using an idempotency key, clients can safely retry requests without worrying about unintended side effects like duplicate transactions. This helps improve reliability and user experience in distributed systems where intermittent failures are expected.

Key generation

The idempotency key is not permanently saved in our system. A previously processed request is determined by a duplicate value in the combination hash of user client id from the token, URI endpoint, idempotency-key, and request-body. If the request body is modified in any way and re-sent, it won't be seen as a duplicate request and is processed normally.

Therefore, if the intent is to process the request a second time, the idempotency key should be changed to a new value.

> Any duplicated or matched submissions are rejected.

Idempotency keys are eligible to be removed from the system automatically after they're at least 24 hours old, and a new request is executed if a key is reused after the original has been pruned. The idempotency layer compares incoming parameters to those of the original request and errors unless they're the same to prevent accidental misuse.

Results are only saved if an API endpoint started executing. If incoming parameters failed validation, or the request conflicted with another that was executing concurrently, no idempotent result is saved. This is because no API endpoint began execution. It is safe to retry these requests.

Server side

Our server has an idempotency middleware. This middleware checks each of the requests coming into the application to see if the idempotency key is present in the headers.

If the idempotency-key is present in the request, it queries the database to check if there's a record corresponding to that idempotency-key. If there is, the middleware stops any further execution in the middleware layer itself, and immediately responds with the saved data as a response.

Otherwise, it continues to the application layer and creates a new record in the database with the Idempotency key and the generated response, and finally return the same response to the client.

A previously processed request is determined by a combination of same endpoint, request body and idempotency key. If the request body is modified in anyway, it will not be seen as a duplicate request and will be processed normally.

Unique key

Every time a request is made with an idempotency key, the server saves resulting status code. Because it is a unique value, the server uses that information to recognize subsequent retries of the same request.

POST requests

All POST requests accept idempotency keys. Make sure to include a unique key in your request to protect against accidental duplicate requests.

PUT, GET and DELETE requests

PUT, GET and DELETE requests are naturally idempotent and there is no value in adding an idempotency key. The key is ignored if present in these requests.

Idempotent requests

To perform an idempotent request, you must provide an Idempotency-Key: ' `xxxxx` ' in the header
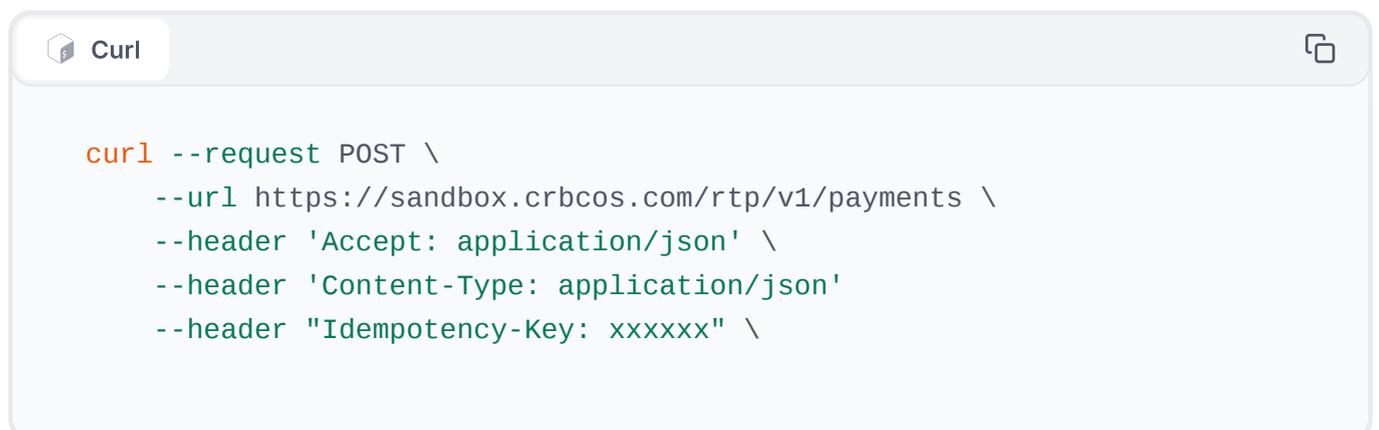
```
Curl

curl --request POST \
    --url https://sandbox.crbcos.com/rtp/v1/payments \
    --header 'Accept: application/json' \
    --header 'Content-Type: application/json'
    --header "Idempotency-Key: xxxxxx" \
```

How to check if a request is idempotent

You can detect if a request is being handled as a duplicate and returning a cached response by looking for the `original-request-id` response header. If an `original-request-id` value appears in the response header, it means the request has been handled as a duplicate.

The `original-request-id` value correlates to the CR generated `request-id` of the original request processed under the idempotency key provided.

> **IMPORTANT**
>
> The idempotency-key isn't searchable. Use the `clientIdentifer` field in the request payload to have a transaction-unique, searchable ID.
>
> If you use both the `clientIdentifer` and the `idempotency-key`, ensure that the `clientIdentifer` doesn't automatically refresh. If it does, the idempotency-key hash check will appear unique (even if the idempotency-key is the same), and allows the transaction to process as unique.

6.4. Pagination

Pagination is a process that divides a large dataset into smaller chunks. All endpoints that return a list of resources support pagination.

When using a list method on a resource, our system supports parameters to specify the paging of the results returned.

For example, if you want to return the second page of your customer list with a 50-record page size, specify that in the request query string:

`pageNumber` integer

Current page number determined by the total number of records and the number of records per page

`pageSize` - integer

Number of records to list on a page. Maximum is 50.

```
Paging example                                                                ⧉

  https://api.crbcos.com/core/v1/cm/customers?pageNumber=2&pageSize=50
```

Results are wrapped in a standard paging object as follows:

`id` string

Unique identifier

`name` string

Customer name

`pageNumber` integer

Current page number determined by the total number of records and the number of records per page

---

`pageSize` integer

Number of records to list on a page. Maximum is 50.

`hasPreviousPage` boolean

True if there is a previous page, otherwise false

`hasNextPage` boolean

True if there is a next page, otherwise false

```json
{
  "results":[
    {
      "id":"123",
      "name":"John C. Customer"
    }],
  "pageNumber":2,
  "pageSize":50,
  "hasPreviousPage":true,
  "hasNextPage":false
}
```

6.5. API versioning

All API endpoints contain a numbered version in the URL. Whenever breaking changes are made to the API, a new major version will be created.

```
Curl

https://api.crbcos.com/core/v1/cm/customers
```

Breaking changes

- Adding new required fields to request
- Changes to the response format
- Data type changes
- Modifying an endpoint URL
- Removing endpoints

Non-breaking changes

- Adding new endpoints
- Adding new optional fields to request
- Adding new fields to response
- Adding new values to fields (e.g. a new status value)
- Bug fixes

Deprecated Versions

When we release a new major version, we will continue to support the previous version for a period of at least 6 months before it is deprecated.

6.6. HTTP status codes

The table below presents standard HTTP status codes that our system might return.

Code	Text	Explanation	Recovery
200	OK	The request has succeeded	N/A
400	Bad request	The request was not processed, due to something the server considers to be a client error.	Typically due to malformed request syntax, invalid request message framing, or deceptive request routing
401	Unauthorized	The request was not successful because it lacks valid authentication credentials (API key) for the requested resource	Provide a valid API key
403	Forbidden	The API key doesn't have permissions to perform the request	Regenerate or modify the API key.
404	Not found	The server cannot find the requested resource	Common causes of 404 responses are mistyped URLs or pages that are moved or deleted without redirection
408	Request timeout	The server has decided to close the connection because it did not receive a complete request from the client within the server's allotted timeout period	Check connection.
409	Conflict	The request conflicts with another request (perhaps due to using the same idempotent key)	Resolve conflicts and retry
424	External dependency failed	The request couldn't be completed due to a failure in a dependency external to Cross River	Fix root cause and retry

Code	Text	Explanation	Recovery
429	Too many requests	Indicates the client has sent too many requests in a given amount of time	Slow down the rate of requests is commonly called
5xx	Server errors	Someting went wrong on Cross River's end	

7. Glossary

Term	Description
1099 form	**IRS tax form** that reports on income earned from sources other than wages, salary, or tips (for which the W-2 is used). Institutions issue 1099's for money paid as interest, dividends, etc.
ABA Routing Number	Every financial institution has a **nine-digit code** to identify itself for financial transactions (can be found printed on the bottom of checks) The American Bankers Association (ABA) developed the system in 1910 to facilitate the sorting, bundling, and delivery of paper checks to the drawer's (check writer's) bank for debit to the drawer's account.
ACH	In the US, the ACH Network is the national automated clearing house (ACH) for electronic funds transfers. The ACH payment rail manages ACH inbound and outbound payments sent through the FedACH payment system. In Cross River, ACH refers to our payment product that uses **ACH**.
Account	Use to describe a demand deposit, savings, other asset accounts, or an extension of open -ended credit from which a customer is able to transact. **Example** Examples of account types include: savings, CDs, credit card
AFT	Account funding transaction. **General function**: Pulls funds from an account and uses them to fund a non-merchant account, such as that of an end-consumer. For example, load a credit, debit, or prepaid card, top up a digital wallet, or fund a P2P money transfer. **Cross River benefits**: Through our Card Rails and Merchant Acquiring product, Cross River enables partners to originate pull payments from debit cards. This provides a convenient and cost-effective method to deliver and receive card payments. This automated payment solution saves time, improves cash flow, and minimizes risk exposure, while ensuring security and privacy of financial information.
Allowlist	An allowlist is always a list of entities who are allowed to do something. In Cross River this could be a list of: 1. Customers who have been approved to open accounts 2. Low-risk customers

Term	Description
	3. Domains allowed access to Cross River systems
AML	Anti-money laundering. (See Money Laundering below).**History:-** In the 1980s, the war on drugs led governments again to turn to money laundering rules in an attempt to track and seize the proceeds of drug crimes in order to catch the organizers and individuals running drug empires. The September 11 attacks in 2001, which led to the **Patriot Act** in the U.S. and similar legislation worldwide, led to a new emphasis on money laundering laws to combat terrorism financing.
API	Application Programming Interface. A software intermediary that allows two applications to talk to each other. An API is a tool that allow developers to access data and interact with external software components in response to a request.
ARN	An acquirer reference number, or ARN, is a unique number created in credit or debit card transactions when it transfers from the merchant's bank through the payment processor, and to the cardholder's bank.
BaaS	Banking as a Service. Offering banking services to customers.
BAI	Business Application Identifier
Bank rail	See *Payment rail*
Beneficiary	A natural person or other legal entity who derives money or other benefits from something. Usually used to indicate a person who receives distributions from a trust, will or life insurance policy. It can also refer to a recipient of a payment. **Example** Jane is the beneficiary of her husband's life insurance policy.
Beneficial owner	An individual who directly or indirectly, owns a % of the equity interests of a legal entity customer. **Example** The beneficial owner of the land will have a right to the income from the property.
BID	Pertaining to payment cards. **Business identifier**. a unique number assigned by Visa to a financial institution.

Term	Description
Blocklist	Customers flagged by the system and prohibited from opening accounts. These customers are reported to the appropriate regulatory authority.
Borrower	Use to describe a loan customer. Can be a consumer or entity (In the days before we sell the loan on, the borrower is our customer). **Example** Once approved for the loan via the MPL, the funds are transferred directly via Arix, to the borrower.
COS	Cross River Bank Operating System
Credit	Debt that is incurred or allowed to be incurred. i.e. a loan or the amount a customer is permitted to spend on a credit card
Credit an account	The act of adding/transferring funds to an account, opposite of *debit an account*. **Example** Interest will be compounded daily and will be credited to the account monthly.
Debit an account	The act of removing/transferring funds from an account, opposite of *credit an account*. **Example** This is used to push funds to one COS account and debit from another account
Disburse	To pay out funds (on behalf of a client to a third party). **Example** Once approved for the loan via the MPL, the funds are disbursed directly via Arix, to the beneficiary.medical service provider
Endpoint (EP)	The location in a communication channel through which an API accesses the resources required to perform its function.
Entity	A non individual that can enter into contracts with CRB. **Example** A legal entity includes trusts, estates, LLCs, corporations, non-profits, and all organizational structures that engage in business with CRB.
FDIC	**Federal Deposit Insurance Corporation** (FDIC) is one of two agencies that provide deposit insurance to depositors in U.S. depository institutions.

Term	Description
Fedwire	**Fedwire** (formerly known as the Federal Reserve Wire Network) is a real-time gross settlement funds transfer system operated by the United States Federal Reserve Banks that allows financial institutions to electronically transfer funds between its more than 9,289 participants (as of March 19, 2009).
FI	Financial institution
fiserv	Global provider of financial services technology: **https://www.fiserv.com/**
Funds flow (FoF)	The path the funds take to get from one account to another
General ledger	A GL (general ledger) account is a parent account belonging to an institution or organization. A GL account at CRB records all transactions for that account. The transactions are related to accounting elements, including assets, liabilities, equity, revenues, expenses, gains, and losses. See also *Subledger*.
HFI and HFS	After a loan is made, the funds are either Held For Investment or Held For Sale.
Holdback	The clause in a commercial loan that puts aside a portion of the loan until a milestone is reached.
IAM	Identity and Access Management
IAT	Internation ACH Transactions: IAT was established by Nacha as an extension of ACH. IAT is designed for US banks (which payers must supply adequate IAT information) to monitor and report international transactions for OFAC compliance.
Image cash letters	Check processing for COS checks deposited at other banks.
ISO 20022	The **ISO standard** for electronic data interchange between financial institutions.
KYB	Know Your Business (KYB) is a regulatory and legal requirement for banks and other related institutions to identify and verify the identity of

Term	Description
	their clients.
KYC	Know Your Customer (KYC) is the mandatory process of identifying and verifying the identity of your client when opening an account and periodically over time. Banks must make sure that their clients are genuinely who they claim to be.
Loan tape	Loan Tape denotes an electronic file or set of files that captures lending product data from a financial firm's systems. (Also: Loan Data Tape, Loan Exposures Tape, Servicing Tape, "Loan-by-Loan File"). It is typically a database extract that needs to be specified in detail (the "scope" of the extract) or spreadsheet. The term likely originates in magnetic data tapes used in earlier generations of computer storage. A loan tape can be considered as a one-time snapshot of a subset of an organization's Credit Portfolio Information.
Memo post	*Memo post,* or *memo posting*, is a term used in traditional computerized banking environments where batch processing is employed. A memo post represents a temporary credit or debit transaction/entry made to an account for which the complete posting to update the balance will be done as part of EOD (end-of-day) batch processing.
Money laundering	Money laundering is the illegal process of concealing the origins of money obtained illegally by passing it through a complex sequence of banking transfers or commercial transactions. The overall scheme of this process returns the "clean" money to the launderer in an obscure and indirect way. One problem of criminal activities is accounting for the proceeds without raising the suspicion of law enforcement agencies. **Interesting fact:** The **United Nations Office on Drugs and Crime** (UNODC) estimates that the amount of money laundered globally in one year is "2–5% of global GDP, or $800bn – $2tn in current US dollars.
MPL	Marketplace Lender. An MPL offers loans to higher risk individuals who would otherwise be turned down for a loan. They approach Cross River with the relevant documentation and information to facilitate the loan of the money. The MPL itself does not lend the money. Only a bank can do the lending, and Cross River is a bank.

Term	Description
Nacha	The **National Automated Clearing House Association** manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data in the United States.
NARR	Short for narrative. Part of the ISO 200022 standard.
NOC	Notification of Change (NOC) is a notification from the ACH network that something about a bank account has changed. For example, if you as a PayPal user submit a payment for which the name on the bank account has changed, then PayPal receives a NOC that lists the corrected name.
OCT	Original credit transaction. **General function**: A real-time payment method that enables the direct transfer of funds to cardholders around the globe. Using the push payment capabilities of Visa OCT and MasterCard MoneySend services, cardholders receive funds directly on the account linked to their card. In the Visa network, OCT sends payments via a 'push' mechanism specifically over the VisaNet electronic payments network to specific card-based account holders. In turn, payments are credited into those cardholder's accounts. **Cross River benefits**: Through our Card Rails and Merchant Acquiring product, Cross River enables partners to originate push payments to debit cards, resulting in a dramatic reduction in processing time. The wait for transaction approval drops from days to literally minutes, providing cardholders with access to their funds almost instantly.
ODFI	**Originating Depository Financial Institution** This term is used in connection with ACH Network (ACH). In the ACH flow, the ODFI acts as the interface between the Federal Reserve or ACH network and the originator of the transaction.
OFAC	The **US Office of Foreign Assets Control** is responsible for administration and enforcement of economic and trade sanctions for the US Treasury Department. OFAC maintains several lists of persons who are blocked under OFAC sanctions. US banks are required to check the OFAC lists every time a

Term	Description
	customer comes to open an account.
Originator	Use to describe the person who is initiating a transaction. **Example** Each originator can have many profiles from which they originate transactions.
Payment	A payment is a type of transaction in which funds are sent.
Payment rail	A payment rail is the method by which funds are transferred from one account to another. Examples of rails include ACH, RTP, and wires. **Example** Depending on the rail type, funding results might be immediate or take up to a few days
PCI	Payment card industry **data security standard**
PCC	Procurement Credit Card
RDFI	Receiving depository financial institution (RDFI) is a financial institution qualified to receive ACH (Automated Clearing House) entries. These institutions should abide by the NACHA (National Automated Clearing House Association) Rules. The RDFI interlinks the Receiver's account with the Cards Association network.
Recipient	Use to describe the consumer or entity who receives the funds. **Example** The recipient receives funds immediately in their account.
RPPS	Remote Payment and Presentment Service (RPPS) is an electronic payment processing and presentment hub used by Mastercard. It includes routing and settlement within 24 hours, risk management procedures, and automatic editing of customer accounts.
RTP	**Real Time Payments.** The RTP domain integrates payments between banks through "The Clearing House". An RTP payment is near instant. Within a matter of seconds, the money will be in the receiver account.
SBA	**US Small Business Association**
Sender	Use to describe the person or entity who sends the funds

Term	Description
	Example The sender's bank will charge the sender a fee for the payment order.
Servicing partner	Refers to the partnership between a borrower and the partner who is servicing their loan.
Subledger	An alias to a master account which can also be used to classify a specific amount within the master account balance
TCH	**The Clearing House** (TCH) is a private banking association and payments company owned by 24 of the largest banks.
Transaction	The movement of funds from one account to another or an account to a fund
W2 form	Wage and tax statement form

Further information: **US Treasury Dept. Glossary**

8. Disclaimer

All Cross River (the Bank) software and systems, and the information and materials contained or made available in this site are provided on an "as-is", "as available" basis without warranty of any kind. Neither Cross River nor any of its current or future affiliates or subsidiaries or the employees, successors or assigns of it or its affiliates or subsidiaries make any warranties regarding the use, operation or performance of software and systems utilized, or to the content of material set forth herein, whether express or implied, and the Bank and affiliates or subsidiaries or the employees, successors or assigns of it or its affiliates or subsidiaries expressly disclaim all implied warranties, including any warranty of merchantability or fitness for a particular purpose.

The Bank has no liability with respect to any software or system or for any inaccurate or incomplete information or claims that may result from reliance on such information contained herein. Neither the Bank nor any of its affiliates or subsidiaries or the employees, successors or assigns of it or its affiliates or subsidiaries shall be liable for, and hereby expressly disclaim any, liabilities and warranties with respect to other third-party components of material contained herein.