

GLOBAL PAYMENTS API V2 CLIENT INTEGRATION GUIDE





Global Payments API Version 2 (GP2) Playbook

This document is designed to support onboarding for all new clients to GP2 within the JP Morgan API network. It provides comprehensive information about this API and includes instructions for every stage of the implementation process.

This includes:

- Navigating the Payment Developer Portal (PDP)
- Authentication and Security Requirements
- Formatting API Payloads for Different Payment Types for GP2
- Understanding Payment Statuses and Error Codes

By following this guide, both new clients and existing API users transitioning from older APIs to GP2 can efficiently complete their API onboarding, access payment information, and manage payment flows through simplified processes.

Table of Contents

This document is designed to support onboarding for all new clients to GP2 within the JP Morgan API network. It provides comprehensive information about this API and includes instructions for every stage of the implementation process.

1. Introduction.....	4
1.1 Overview	4
2. Navigating the Payments Developer Portal (PDP)	6
2.1 Overview	6
2.2 Products	6
2.3 Resources	8
2.3.1 API Reference Overview	8
2.3.2 Global Payments 2	8
2.4 How to Format an API Payment	11
2.4.3 Data Dictionary	12
3. Client Onboarding	14
3.1 Overview of Onboarding Process and Timelines	14
3.2 Client Onboarding & PDP Activation	15
3.3 Using the PDP to Exchange Certificates	17
3.4 API Authentication & Security	20
3.4.1 Overview of Certificates	20
3.4.2 Environment-Specific Credentials	21
3.4.3 How to Generate Certificates and Configure Callbacks	21
3.5 Overview of Testing Environments	22
4. Payment Statuses and Events.....	23
4.1 Payment Status & Sub-Status	23
4.2 Status Transition Flow	24
4.3 Applicable Statuses by Payment Type	25
4.4 Payment Events	27
4.5 Payload and Response Samples for Payment Initiation	28
4.6 Payload and Response Samples for Client Initiated Returns	34
5. Error Handling.....	35
5.1 Error Code Catalog	35
5.2 Types of Error Codes	35
5.3 Reading an Error Schema	35
5.4 Basic Debugging of Error Codes	36
6. Ancillary API compatibility.....	37
6.1 Before Initiating a Payment	37
6.2 Initiating a Payment	37
6.3 Other Payment APIs	38
7. Support & Troubleshooting.....	39
7.1 Best Practices	39
7.2 Duplicate Checks	39
7.3 API Support	39
8. Other Resources Coming Soon.....	40

1. Introduction

1.1 Overview

Global Payments API V2 (GP2), JPMorgan's latest Treasury Services API built on modern payments infrastructure, provides a single point of connectivity to initiate payments and track their status across all major payment rails. To simplify the client onboarding and integration experience, we offer different payment functionalities as part of GP2.

The API supports Payment Initiation and Client-Initiated Returns today as two key capabilities, available as separate endpoints.

Payment Initiation

The single payment in endpoint allows clients to initiate a single payment across multiple payment types. Using the same URL, clients can use the GET action to retrieve the latest status of the payment.

Payment Coverage

GP2 offers support for a variety of payment types across the regions we serve.

The table below provides detailed information by region and country, outlining the specific payment products available in each location.

Payment Type	Region	Country/ Branch Location
ACH	North America	US (Credit Transfers, Direct Debit, International ACH Transactions)
	Latin America	Chile (Credit Transfers only)
Wires	North America	US (PAIN 001, PACS 008, PACS 009) 1. PAIN.001 – Customer Credit Transfer Initiation
		2. PACS.008 – FI to FI Customer Credit Transfer
		3. PACS.009 – Financial Institution Credit Transfer
Kinexys (JPMorgan Blockchain)	North America	United States
	Europe, Middle East, and Africa	Luxembourg
		London
		Frankfurt
		Dublin
		Amsterdam
	Asia Pacific	Hong Kong
		Singapore
		Sydney
Push to Card	North America	US, Canada
Push to Wallet	North America	US (Paypal, Venmo)

GP2 API CLIENT INTEGRATION

Payment Type	Region	Country/ Branch Location
Zelle	North America	US
RTP	North America	US (TCH, FedNow)
		Canada (Interac E-Transfer)
	Europe, Middle East, and Africa	Eurozone (SEPA Instant) UK (FPS)
	Latin America	Brazil (PIX)
		Mexico (SPEI)
		Chile (Coelsa)*
RTP	Asia Pacific	Australia (NPP)
		Hong Kong (FPS)
		Malaysia (RPP)
		India (IMPS, UPI)*
		Singapore (FAST)
		Thailand (PromptPay)*

*Available in pilot phase and restricted availability

If you have further questions on coverage, please reach out to your respective Sales contact for further information.

Client Initiated Returns

A client-initiated return is defined as allowing JPMorgan's client to initiate a return against an incoming payment that was received into the account. This is offered as a separate endpoint from single payment initiation, but follows the same schema standards and responses as payment initiation.

If clients want a receipt of incoming payments (pay-ins) from the clearing network, they may use the [Payment Receipts API](#) (also known as Credit Confirmation) for webhooks.

The table below shows which regions support client initiated returns.

Payment Type	Region	Country
RTP	Latin America	Brazil*

* Available in pilot mode and restricted availability. Reach out to your Sales contact for more information.

2. Navigating the Payments Developer Portal (PDP*)

***Disclaimer:** *Not all APIs may be available in all locations; please visit the Payments Developer Portal for latest API offerings and/or contact your Sales Representative.*

2.1 Overview

The Payment Developer Portal (PDP) is JPMorgan's latest platform showcasing our payment APIs, providing all clients with detailed, self-service information on Payment APIs and enabling an interface to seamlessly manage their API onboarding experience.

This section is specifically focused on navigating the PDP as it relates to GP2, and does not cover the full functionality of the PDP platform.

The PDP is organized into two primary sections: Products and Resources.

- **Products Section:**

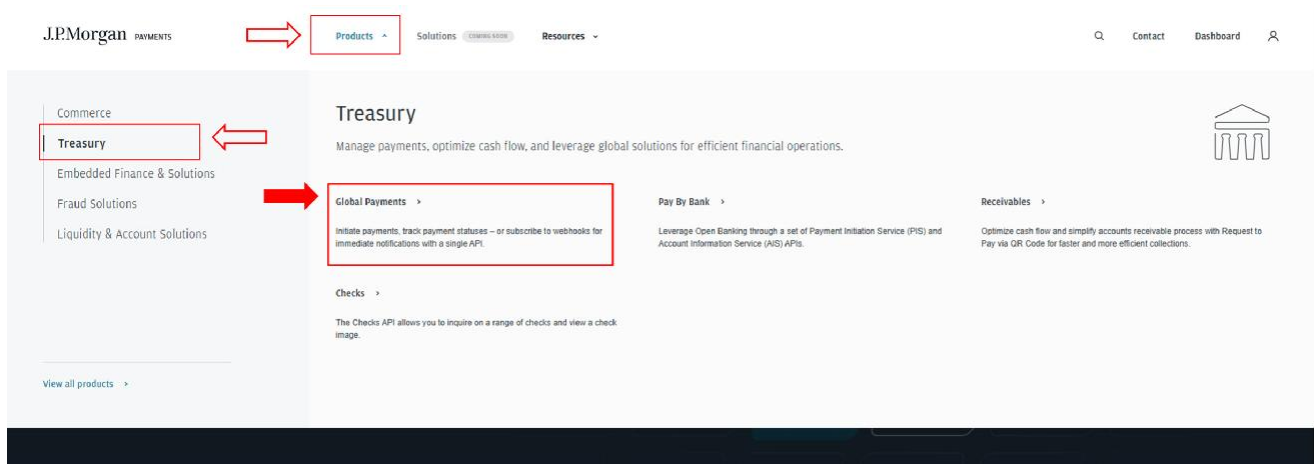
This area is intended for all users, especially corporate treasurers seeking information about JPMorgan's APIs and the complete taxonomy of APIs available across Commerce, Treasury, Accounts, and more. Here, users can explore business flows, use cases, payment limits, and service codes for all product types supported by GP2.Authentication and Security Requirements

- **Resources Section:**

Geared towards developers, this section provides direct access to authentication guides, API onboarding instructions, and the GP2 API specification with sample payloads.

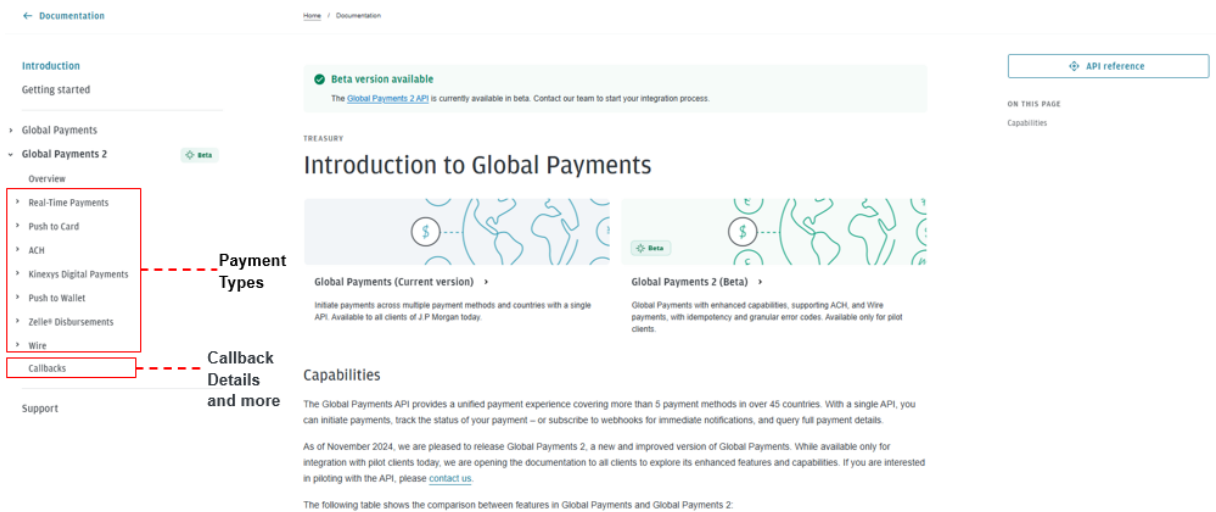
2.2 Products

To view all the product offerings for GP2, you will need to navigate to the [Payments Developer Portal \(PDP\)](#) → Select “Product” → Click “Treasury” → Select “Global Payments”



The “Global Payments” page shows both Global Payments V1 and V2. Starting February 2026, Global Payments V1 will be on the deprecation path.

Global Payments V2 (GP2) is the strategic unified payments API from 2026 onwards. The image below shows the navigation options available within GP2, highlighting where you can locate information on the supported payment types and callbacks.



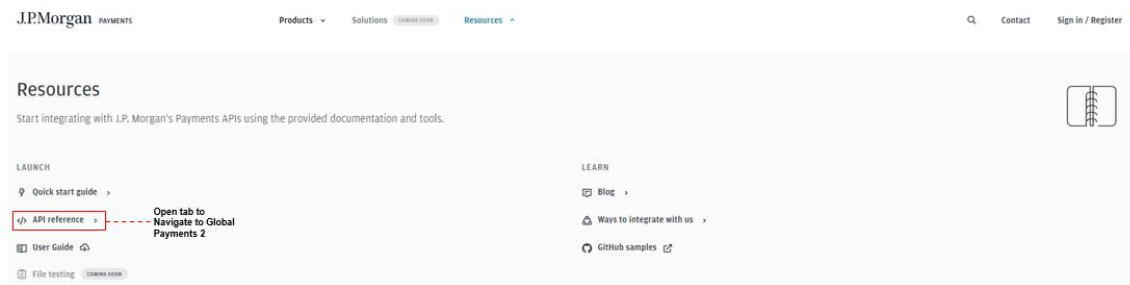
For each payment type, the following information is provided:

Page	Purpose & Usage
Overview	Use cases of the payment type, high level flows, and country availability
Payment Parameters	Provides country-specific requirements on formatting the API payment, split into Required fields/ payment parameters and Optional or Conditional Fields. Specifically for Real-Time Payments and ACH (coming soon), payment parameters on client-initiated returns are included here.
Resources	Additional important information related to each payment type, such as payment limits, response types, and purpose codes.
Initiate a Payment Request	Mock payload(s) to initiate a payment for each payment type. Multiple payloads might be provided for different use cases. Specifically for Real-Time Payments and ACH (coming soon), sample return payment requests can be found here.
Get Details of a Payment	Instructions to track the latest status of the payment with sample responses, and how to interpret them.

2.3 Resources

To view all the resource offerings for GP2, you will need to navigate to [Payments Developer Portal \(PDP\)](#) → Select “Resources” → Click “API Reference”

The image below shows how to navigate to the API Reference section on the Payments Developer Portal. By navigating through the "Resources" tab and selecting "API Reference", users can locate Global Payments 2 and related integration tools.



2.3.1 API Reference Overview

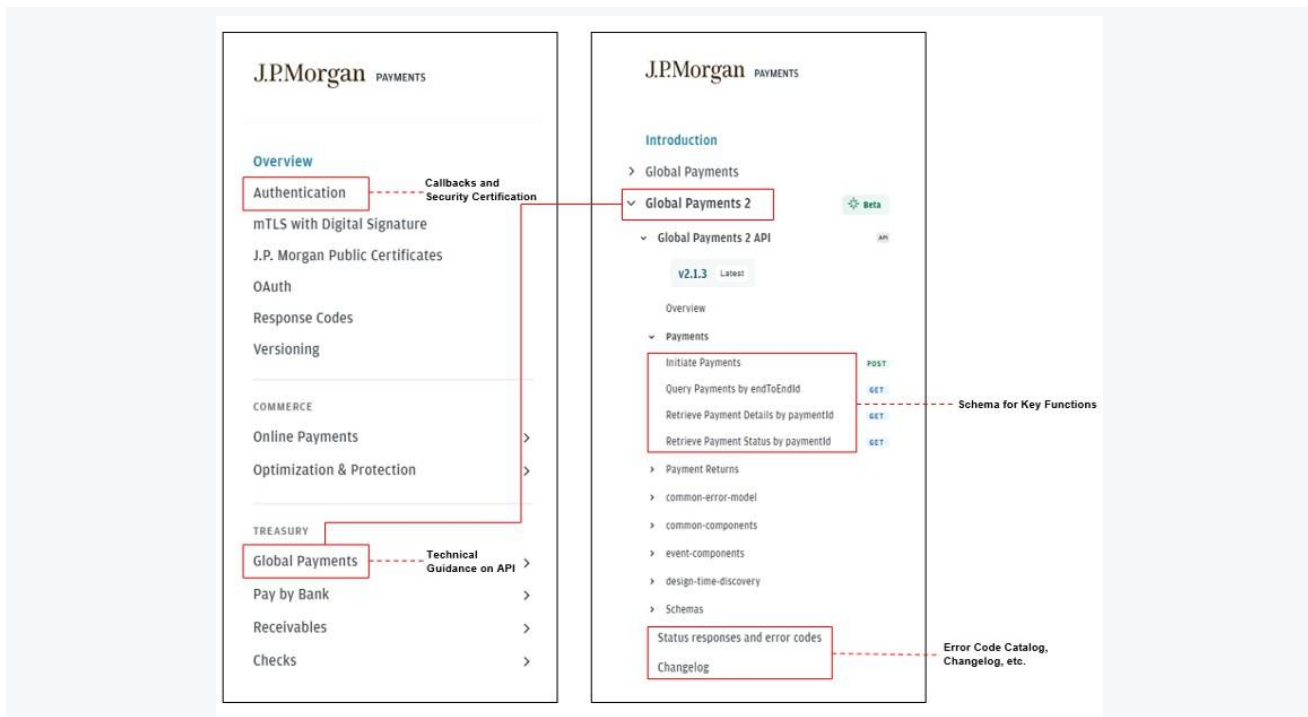
The API Reference section provides comprehensive resources and endpoint documentation, including detailed guides, code samples, and standardized response codes to support your integration journey.

Core Content:

- **Documentation:** Access business information of JPMorgan’s APIs, including step-by-step guides, technical explainers, and reference materials to get started quickly.
- **Response Codes:** Review standard conventions for API request success and error handling.
- **Versioning:** Understand our transparent and predictable versioning strategy to ensure long-term integration stability.
- **Featured APIs:** Discover our most popular APIs serving merchant and treasury use cases.
- **Browse by APIs:** Easily navigate through different APIs offered on the PDP.

2.3.2 Global Payments 2

The following section covers technical information about GP2. It is suitable for developers and any users looking to understand the technical aspects of the API. The image below shows you how to navigate to GP2 content from the API Reference section of the PDP.



Overview:

Allows you to download the API specifications in the format of a YAML file under “Download OAS” button. It includes critical information such as endpoints (paths), HTTP methods (GET, POST, etc.), request/response schemas, parameters, authentication details, and error codes.

This page also includes information and URLs for the following environments:

Environment	Purpose
Mock	Simulates API responses without backend logic; ideal for early development or testing integrations. Open to the public and available directly on the PDP or via the Mock endpoint.
Client Testing/ Sandbox	A safe, isolated environment with realistic data and behavior for client testing; used during initial phase of testing to validate client applications without affecting real data or users.
Production	The live environment serving real users and data; use this for actual business operations and end-user interactions.

Payments:

This endpoint pertains to single payment initiation. View information on the following 3 endpoints:

1. Initiate Payments
2. Query Payments by endToEndId or paymentId
3. Retrieve Payment by paymentId

For each of these endpoints, mock payloads and responses are available on the right hand side of the spec.

To view the schema for a 201 response (Payment Accepted & Created), a 200 response (duplicate payment), callbacks, and error responses, scroll down to the bottom of the page under ‘Initiate Payments’.

GP2 API CLIENT INTEGRATION

Payment Returns:

This endpoint pertains to client-initiated returns. View information on the following 2 endpoints:

1. (Initiate) Payment Returns
2. Retrieve Payment Return.

The Payment Returns endpoint shares the same 201 and 200 response as the Payments endpoint, as well as the same error code catalog.

Status Responses and Error Codes:

This section contains information about payment statuses, sub-statuses, and the new error code catalog. For more information about error codes, please refer to the following sections.

In GP2, we have introduced payment sub-statuses to provide more information about the current state of a payment.

Changelog:

Provides critical information around minor and major version upgrades, and when the changes were introduced. We only support testing on 1 version in the Sandbox/ client testing environment today, which will always be on the latest version of the API

2.4 How to Format an API Payment

As we offer 15+ unique payment methods on a single all-encompassing schema, we make it easy for you to format your payment based on the payment type and local clearing and regulatory requirements.

GP2 offers more than 400 parameters of information for you to fill in. Not all parameters are used or accepted for each payment type in each country. Please refer to the documentation below or on the PDP to verify that your payment instructions meet the formatting standards applicable to your country.

There are 3 options for you to obtain this information:

Resource	Where to Find It	What is it Good For
RTP	Product Section on the PDP	List of required and optional parameters by payment type and markets
Mock Payloads	API Reference under the Resources section	See sample payloads relevant to payment type and market
Data Dictionary	Personal or organization workspace after creating an account on the PDP	Similar information to Payment Parameters page, but in Excel format

2.4.1 Payment Parameters Deep Dive

Available for each payment type and market

- Displays the minimum required information needed to send a payment, as well as optional and conditional information
- Provides specific criteria the information needs to adhere to (if any), such as local purpose codes and maximum lengths
- Augmented with code snippets in CURL and JSON formats in the “How To” sections for each payment type

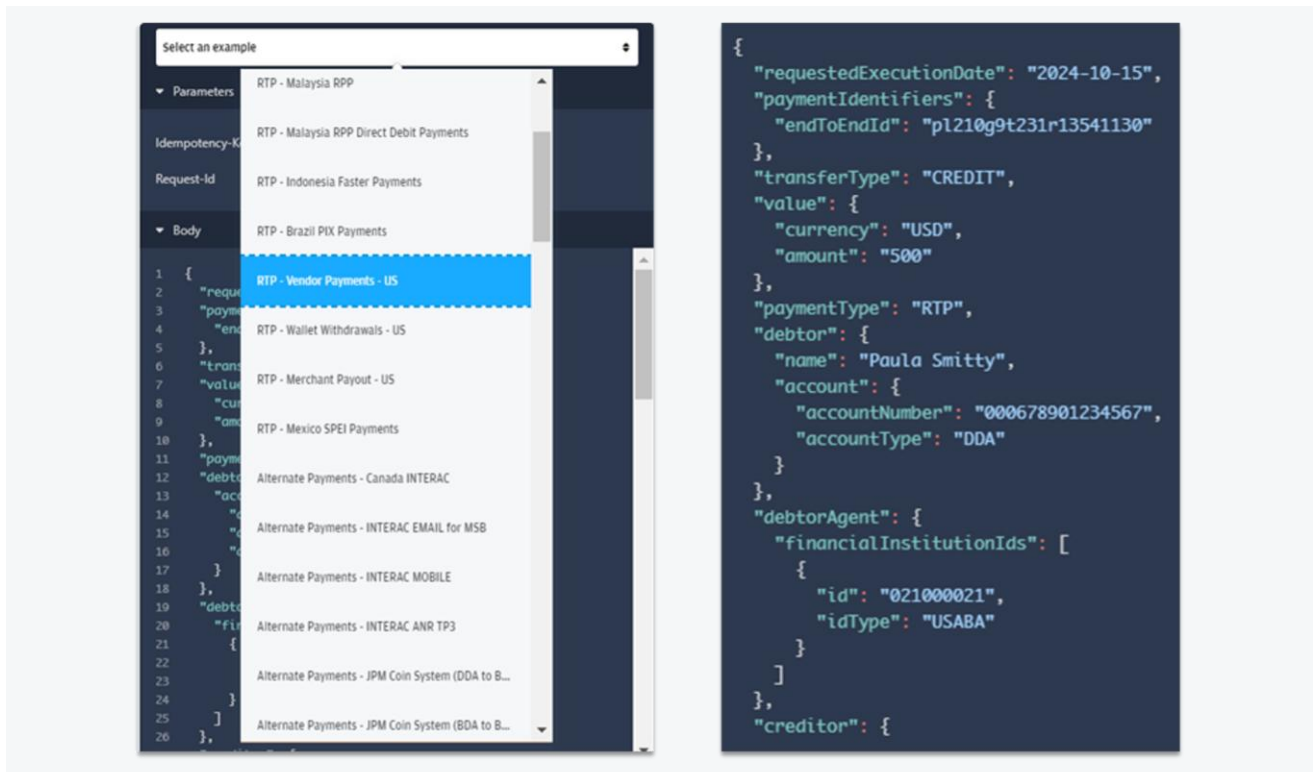
2.4.2 Mock Payloads

- Available for each payment type and market, and sometimes includes examples for specific use cases (e.g., vendor payments)
- Shows you how a properly formatted API payload might look like with mock party and account data
- Includes sample successful (201) and unsuccessful responses with corresponding error codes

Steps to View the Mock Payloads:

- To initiate a payment for any payment type, please refer to this link in the mock sample.

<https://developer.payments.jpmorgan.com/api/treasury/global-payments/global-payments-2/global-payments-2#/operations/createPayment>



2.4.3 Data Dictionary

The Data Dictionary provides an Excel sheet which is a supplement to the payment parameters pages and API specification on the Payments Developer Portal. Each product/market combination that is offered in the release of the GP2 API can be found in the subsequent tabs. Client can leverage this data dictionary as guide across all payment types.

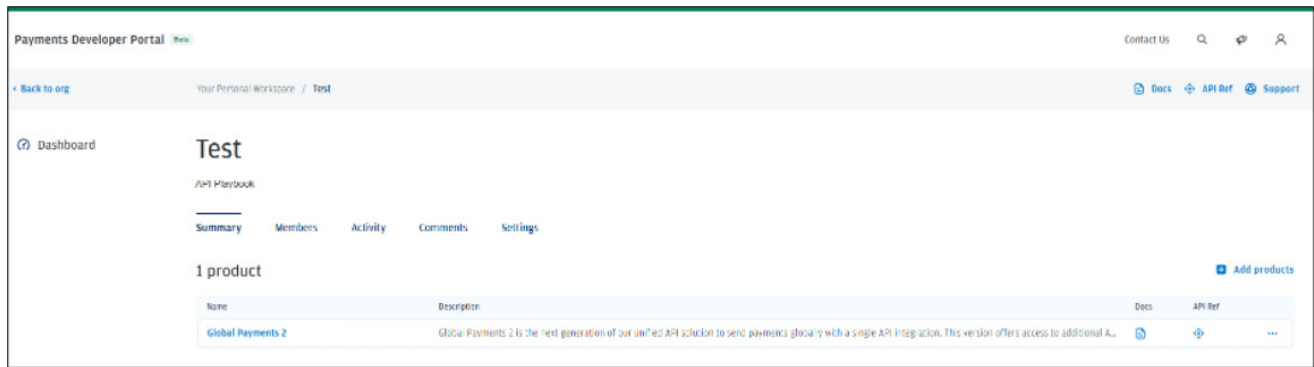
Below are steps to download the Data Dictionary from the PDP after you have created your PDP Account (See section 3 of this document):

1. Create Your Account on Payments Developer Portal (PDP)

- Go to the Payments Developer Portal (PDP)
- Register for a new account using your corporate credentials
- Complete any required verification steps

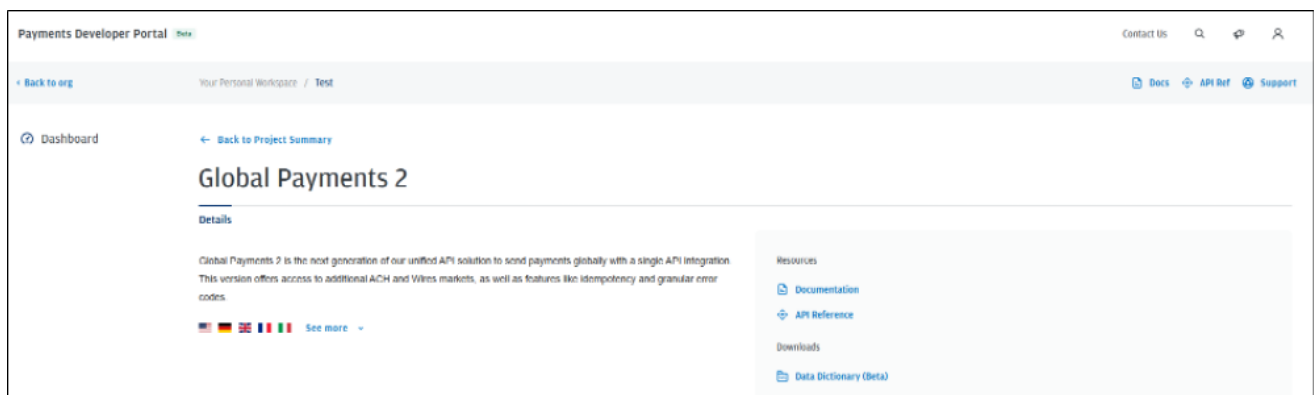
2. Add Your Product

- In your Personal or Organization Workspace, create a new Project
- When you're creating a project, you can select the option to add API Products
- Select "Global Payments 2"



3. Download the Data Dictionary

- On the Global Payments 2 page, look for the link labeled “Data Dictionary” under “Resources”
- You should see a download button or link for the data dictionary.
- Click “Download” to save the API GPV 2 Playbook Data Dictionary to your device



How to Use the Data Dictionary

1. **Instructions Tab:** Find step-by-step guidance on how to navigate the Data Dictionary and apply filters to locate the information you need
2. **Index Tab:** View a comprehensive list of payment types and supported countries available on GP2, along with directions on where to find each item within the Data Dictionary
3. **Payment Type Tab:** The Data Dictionary is organized by payment type. Select the relevant tab to review market-specific requirements for each payment method
 - *Note:* Always check the version of the specification supported by the Data Dictionary, as updates are released regularly
4. **Changelog Tab:** Displays the version history of the Data Dictionary and highlights updates from earlier documentation
 - The Data Dictionary is versioned according to its most recent publication date, which can be found in the Excel file name

3. Client Onboarding

3.1 Overview of Onboarding Process and Timelines

As GP2 uses a new onboarding process through the Payments Developer Portal (PDP), whether you are a new or existing client, you will need to follow the set-up steps below to onboard to the API.

Client Setup for GP2

Step	Task	Ownership	Estimated Duration (Days)	
			From	To
1	Client has to submit signed API Security Administrator Designation Form (SADF) for GP2 to JPMorgan	Client	2	3
2	Activation of client profile in the Payments Developer Portal (PDP)	JPMorgan	1	1
3	Client registers for the PDP and waits for JPMorgan account confirmation email. Meanwhile, client can review API specifications	Client + JPMorgan	1	5
4	Client to define and confirm the scope of payment methods to be added into your profile	Client + JPMorgan	1	1
5	Client to exchange Client Testing certificates with JPMorgan via the PDP	Client + JPMorgan	5	7
6	Configuration of client profile for GP2 for the Client Testing Environment (CTE), including addition of client testing accounts/ DDAs	JPMorgan	1	3
7	Client to confirm CTE connectivity is successfully in place	Client	1	3
8	Client testing occurs in the CTE	Client + JPMorgan	2	20
9	Client to sign off on results of Client Acceptance Testing (CAT)	Client + JPMorgan	1	2
10	Client to exchange Production certificates with JPMorgan via the PDP	Client + JPMorgan	1	7
11	Configuration of client profile for GP2 for the Production environment, including addition of client testing accounts/ DDAs	JPMorgan	1	3
12	Client to promote code to their Production environment	Client	2	5
13	Production Verification Testing (PVT) occurs	Client + JPMorgan	10	15
Total time			29	75

Addition of New Payment Types to GP2

One important change to highlight on GP2 compared to the earlier version is that clients have to be entitled to not just the API, but also specific payment types and countries they are interested in using. This is to ensure robust access policies for clients given the extensive global coverage of the API.

For example, if a client is set up to only use US RTP on GP2, but tries to send a SEPA Instant payment without any additional set up, will receive a 404 Unauthorized Error.

GP2 API CLIENT INTEGRATION

Clients already onboarded to GP2, who want to enable additional countries to an existing payment type, or enable more payment types to their profile, have to follow these steps.

Adding New Payment Types/ Countries for Existing Clients on GP2

Step	Task	Ownership	Estimated Duration (Days)	
			From	To
1	Client has to define and confirm the scope of payment methods to be integrated and added into your system.	Client + JPMorgan	1	1
2	Configuration of client profile for GP2 for the Client Testing Environment (CTE), including addition of client testing accounts/ DDAs	JPMorgan	1	3
3	Client testing occurs in the CTE	Client + JPMorgan	2	20
4	Client to sign off on results of Client Acceptance Testing (CAT)	Client + JPMorgan	1	2
5	Configuration of client profile for GP2 for the Production environment, including addition of client testing accounts/ DDAs	JPMorgan	1	3
6	Client to promote code to their Production environment	Client	2	5
7	Production Verification Testing occurs	Client + JPMorgan	10	15
Total time			18	49

Disclaimer: The above steps are not meant to be indicative for every client, but a standard set of steps that most clients can expect to follow. The actual steps and implementation period depends on the use cases of the client and the complexity of the implementation

3.2 Client Onboarding & PDP Activation

All new clients interested in onboarding to GP2 will have to complete and submit the Security Administrator Designation Form (SADF) shared by your Implementation Contacts to initiate the onboarding process.

The image below is a preview of what the SADF will look like.

J.P.MORGAN SECURITY ADMINISTRATOR DESIGNATION FORM (SADF)					V4.5.06.11.19
Name of Customer:		Customer ECID: (internal JPMC use only)		Address (Street):	
Customer(s) U.S. TIN (if applicable):		Address (City, State/County/District, ZIP/Postal Code, Country):			
Instructions: Please provide the information requested below to designate the Security Administrator(s) for your company for the indicated products. FOR NEW CUSTOMER IMPLEMENTATIONS OR FOR MODIFICATIONS: IF NO CHECKBOX IS SELECTED, THE NAMED INDIVIDUAL SHALL BE ADDED. Terms: The Customer hereby agrees to be bound by any Service Terms, Terms of Use or other agreement(s) between the Customer and JPMorgan Chase Bank, N.A. and any of its affiliates (the "Bank"), as applicable, applicable to the selected products (or any other products accessed through such selected products), the receipt of which is hereby acknowledged. Certain products are platform products, through which other products may be accessed. The designation of a Security Administrator for a platform product shall apply to all products accessed thereby, except to the extent a specific product is provided as a separate option below. If the Customer selects the JPMorgan Access Saudi Arabia Online product, the Customer specifically agrees to be bound by the JPMorgan Access Saudi Arabia Online Service Terms.					
Security Administrators Designated for the Following Products: ☐ J.P. Morgan Access® (Online and Mobile) Access Profile ID(s): _____ ☐ J.P. Morgan eServe™		☐ J.P. Morgan Host-to-Host/ (Partner ID(s): _____ File Transfer Services (FTSE ID(s): _____ ☒ J.P. Morgan Application Programming Interface (API) (Access Profile ID(s): _____		☐ ACH File Warehouse ☐ ACH Concentration Services ☐ ACH Inflows (Origin ID(s): _____ ☐ Global Trade Transactions (Trade Channel) ☐ JPMorgan Access Saudi Arabia Online ☐ J.P.Morgan Markets	
Sec Admin 1	Name: _____	Phone #: 312.914.8106	E-mail: _____	Signature: _____	
☒ Add ☐ Modify ☐ Delete	Street Address: _____	City: San Diego	State/County/District, ZIP/Postal Code, Country: _____		
Sec Admin 2	Name: _____	Phone #: 206.963.5211	E-mail: _____	Signature: _____	
☒ Add ☐ Modify ☐ Delete	Street Address: _____	City: San Diego	State/County/District, ZIP/Postal Code, Country: _____		
Sec Admin 3	Name: _____	Phone #: _____	E-mail: _____	Signature: _____	
☐ Add ☐ Modify ☐ Delete	Street Address: _____	City: _____	State/County/District, ZIP/Postal Code, Country: _____		
Sec Admin 4	Name: _____	Phone #: _____	E-mail: _____	Signature: _____	
☐ Add ☐ Modify ☐ Delete	Street Address: _____	City: _____	State/County/District, ZIP/Postal Code, Country: _____		
Sec Admin 5	Name: _____	Phone #: _____	E-mail: _____	Signature: _____	
☐ Add ☐ Modify ☐ Delete	Street Address: _____	City: _____	State/County/District, ZIP/Postal Code, Country: _____		
Sec Admin 6	Name: _____	Phone #: _____	E-mail: _____	Signature: _____	
☐ Add ☐ Modify ☐ Delete	Street Address: _____	City: _____	State/County/District, ZIP/Postal Code, Country: _____		
Note: For browser products requiring tokens, the Security Administrator whose information appears in the first Security Administrator block above will be responsible for receiving tokens. It is understood and agreed that each Security Administrator is authorized to receive, exchange and distribute on behalf of the Customer all Security Devices. Upon receipt of notice that setup is complete, the Security Administrators shall be responsible to verify that the requested service has been implemented or modified in accordance with the Customer's request, before allowing use by the Customer.					

Account Activation

Activating an account on the Payments Developer Portal is mandatory to use GP2, and you can do it in two ways.

Option 1: You will receive an invite in your mailbox to activate an account from the Payments Developer Portal.

Invitation to the J.P. Morgan Payments Developer Portal

J.P. Morgan Payments Developer Portal (no reply) <no-reply@jpmorgan.com>

To: _____

Retention Policy: JPMC_inbox_180 (6 months)

Expires: 4/7/2025

J.P.Morgan PAYMENTS

Activate your account

You have been invited to join the _____ organization on the J.P. Morgan Payments Developer Portal.

Activate your account by **10 October 2025** to gain access.

[ACTIVATE NOW](#)

Already have an account? Go to [Login](#)

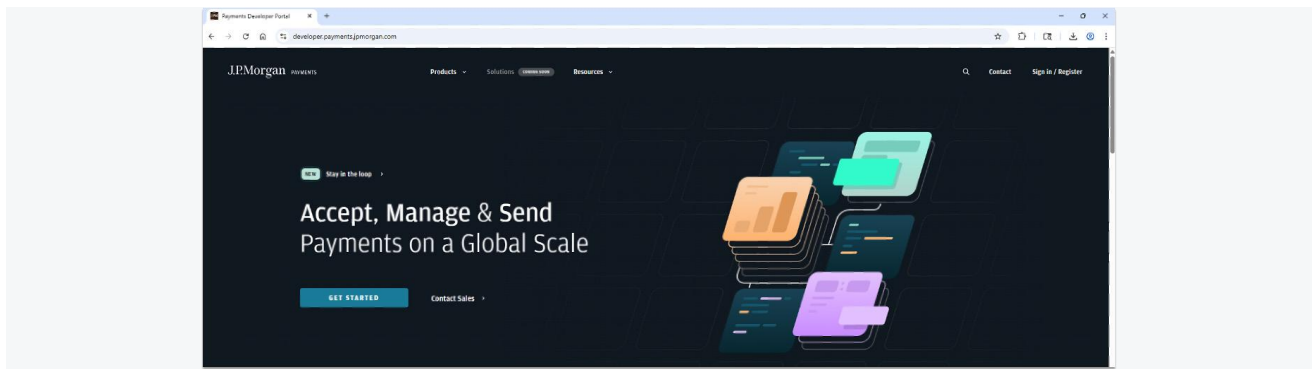
One platform. Unlimited possibilities.

The J.P. Morgan Payments Developer Portal provides you access to tools, documentation, and APIs that allow you to accept, manage, and send payments globally.

You're just a few steps away from unlocking the potential of payments on a global scale.

Option 2: Direct Access to the Payments Developer Portal

Visit the Payments Developer Portal at <https://developer.payments.jpmorgan.com> and create an account using the same email address provided on the SADF.



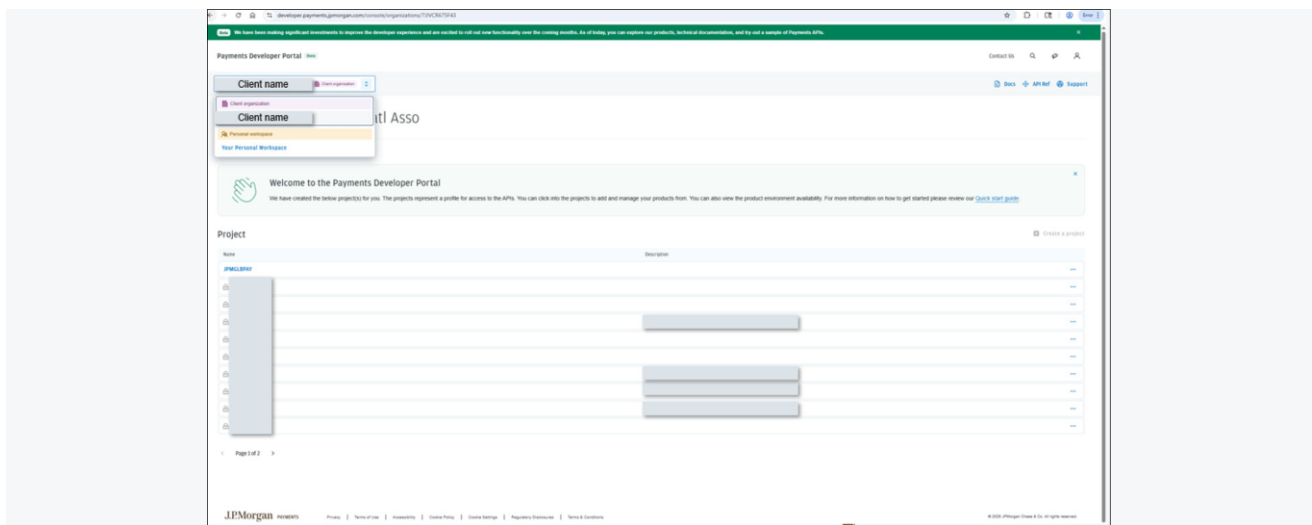
NOTE: Please ensure you sign up using the same email address listed on your SADF.

3.3 Using the PDP to Exchange Certificates

After your account is activated and you've logged in, select the Dashboard icon to open your Console. Here, you can manage your configurations and certificates.

You will have access to two workspaces:

- **Organization Workspace:** Shared with other users in your organization.
- **Personal Workspace:** A private area where you can experiment and test other APIs



After the profile activation, users will be able to access both their personal workspace and client organization view as pictured above. After the account activation, users will be able to access both their personal workspace and Organization Workspace as pictured above.

In your organization workspace, you can view what API Products your organization has been entitled to, and whether you have been authorized to do testing based on the environment type.

GP2 API CLIENT INTEGRATION

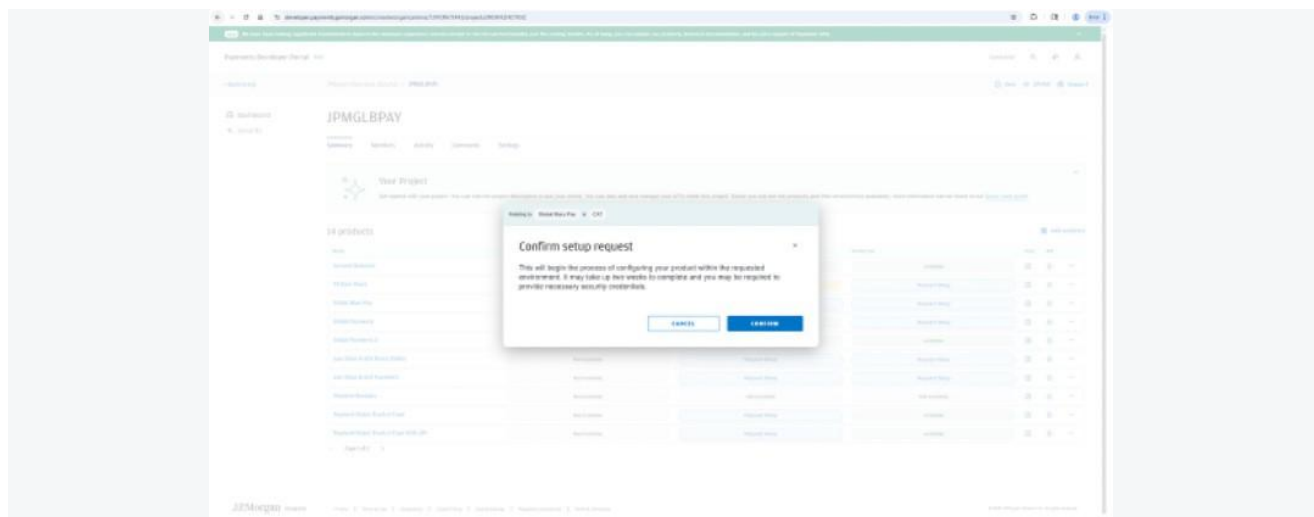
14 products						Add products
Name	Mock	Client Testing	Production	Docs	API	
Account Balances	Not Available	Available	Available			...
FX Rate Sheet	Not Available	Request Setup	Request Setup			...
Global Mass Pay	Not Available	Request Setup	Request Setup			...
Global Payments	Available	Available	Request Setup			...
Global Payments 2	Available	Available	Available			...
Low Value & ACH Direct Debits	Not Available	Request Setup	Request Setup			...
Low Value & ACH Payments	Not Available	Request Setup	Request Setup			...
Payment Receipts	Not Available	Not Available	Not Available			...
Payment Status Track-n-Trace	Not Available	Request Setup	Available			...
Payment Status Track-n-Trace With GPI	Not Available	Request Setup	Available			...

You can also view other team members part of the organization, and what API access rights they have (e.g., ability to upload certificates and manage membership).

4 members					Add members
Name	Email	Status	API Security	Access SA	
		✓ Active			...
		✓ Active			...
		✓ Active			...
		✓ Active			...

Requesting & Managing Certificate Setups

For APIs and environments that you are not yet authorized to access, you can request a set up, and your Implementations contact will be informed. Please view the next section for more information on Certificate and Credential Exchange.



When setup is complete, you'll have visibility into all certificates and their expiration dates across all environments.

Security
Manage your security credentials for access to Testing and Production environments. You need to maintain these settings to protect your users and product implementations. Take a look at our [Security Guide](#).

Mock **Client Testing** **Production**

Request

▼ **mTLS** ⓘ
Provide the public key certificate for the mTLS credential. A maximum of two certificates can share the same Common Name. [Add certificate](#)

Applied to: **Account Balances** **FX Rate Sheet** **Global Payments** **Global Payments 2** **Transaction Details**

Thumbprint	Status	Common Name	Expiry
377b714bccd103900018303820843fda08d876 ⓘ	✓ Active	0204cbar-mtls-ad.jpurchase.net	5 Feb 2026 6:59 PM EST
fbe60c48d91903e0daa552bc89a83baa29fe2435 ⓘ	✓ Active	020425cat-mtls-ad.jpurchase.net	3 Feb 2026 6:59 PM EST
3b919a1d07d6617d1098bec14besff754126d638 ⓘ	✓ Active	111806-mtls-ad.jpurchase.net	10 Dec 2025 6:59 PM EST

▼ **Digital Signature** ⓘ
Provide the Digital Signature Certificate to ensure the integrity and authenticity of the request. Add up to two certificates. [Add certificate](#)

Applied to: **Global Payments** **Global Payments 2**

Thumbprint	Status	Common Name	Expiry
eeb99fde4992f3f8bb17461cce7763ba171fbc3 ⓘ	✓ Active	111806-digsig-ad.jpurchase.net	10 Dec 2025 6:59 PM EST

If your certificate is expiring, you can easily add and renew your new certificate here.

Uploading Certificates

1. Log in to the Payments Developer Portal.
2. Navigate to the Security page within your project.
3. Select the appropriate environment tab (Client Testing or Production).
4. In the Request section, click “Add Security.”
5. Choose the certificate type (mTLS, Digital Signature, etc.).
6. Upload your certificate (drag & drop or Click “Add Certificate”
7. Verify the certificate is listed and active.

3.4 API Authentication & Security

3.4.1 Overview of Certificates

To ensure secure and reliable integration with JPMorgan's APIs, you must configure and manage several types of security credentials and certificates. These credentials are essential for authenticating your application, authorizing access, signing requests, encrypting sensitive data, and enabling secure callbacks.

JPMorgan's list of approved Certificate Authorities can be found on the PDP:

<https://developer.payments.jpmorgan.com/api/authentication>

1. Mutual Transport Layered Security (mTLS Certificate)

- Purpose: Authenticates your application's identity during API requests.
- Details: Issued by a JPMorgan-approved Certificate Authority (CA). Does not grant access permissions.
- Usage: Required for mutual TLS (mTLS) connections.

2. Digital Signature Certificate

- Purpose: Signs API requests (especially POST) for integrity and non-repudiation.
- Details: Uses asymmetric cryptography to verify the origin and integrity of requests.
- Usage: Required for APIs that mandate signed requests.

3. Callback Certificate

- Purpose: Authenticates JPMorgan when sending asynchronous event updates (callbacks) to your system.
- Details: Must be uploaded to the Payments Developer Portal.
- Usage: Required for products supporting callbacks.

4. Encryption Certificate

- Purpose: Encrypts sensitive data in API requests (e.g., PII).
- Details: Supports encryption at request or data level.
- Usage: Optional, but recommended for enhanced data protection.
- List Of Encryption Certificates are found here: <https://developer.payments.jpmorgan.com/api/certificates>

The table below showcases which certificates are necessary for GP2:

	Required for GP2?	Comments
mTLS	Required	
Digital Signature	Required	
Callback	Optional - Use if you would like to receive webhooks	Clients can also reuse their mTLS certificate for callbacks.
Encryption	Optional	

Reporting APIs (e.g., Balance, Transaction Details) generally do not require a Digital Signature, just an mTLS certificate.

3.4.2 Environment-Specific Credentials

Note that separate credentials are required for each environment. If you plan to conduct both Client Testing in our Client Test Environments, and Production Verification Testing in the Production environment, you will need to upload and manage certificates for each environment independently.

3.4.3 How to Generate Certificates and Configure Callbacks

Generating Certificates

1. Select a JPMorgan-approved Certificate Authority (CA).
2. Follow CA instructions to generate your certificate.
3. Ensure certificates are renewed before expiration to avoid service interruptions.

Configuring Callbacks

Adding Callback URL & Certificates

1. Go to the Global Payments screen, Security tab.
2. Select your environment.
3. Under Response, in the Callbacks section, click “Configure callbacks.”
4. Enter your callback URL.
5. Select or upload the required authentication certificate.
6. Optionally, upload an Encryption Certificate for added security.
7. Click “Configure callbacks.”
8. Confirm callback configuration is active.

3.5 Overview of Testing Environments

JPMorgan supports three client testing environments:

Type of Environment	URL	Used For:
Mock	https://api-mock.payments.jpmorgan.com/payment/v2	A self-contained space designed for global specification validation, connectivity testing, and response verification.
		No configuration or client setup is required to use this environment.
Sandbox	https://api-sandbox.payments.jpmorgan.com/payment/v2	The primary client testing platform.
		Captures callbacks, responses, and test connectivity.
		Requires client setup and configuration.
Production	https://api.payments.jpmorgan.com/payment/v2	Used for live traffic

We recommend that all clients test in Sandbox and Production before using the API in the production environment.

4. Payment Statuses and Events

GP2 provides status messages that are standardized across all supported payments. Statuses are returned in the callback, and appear when you use the GET endpoint to retrieve the latest status of your payment. Understanding what each status means help you track progress and identify the best course of action.

4.1 Payment Status & Sub-Status

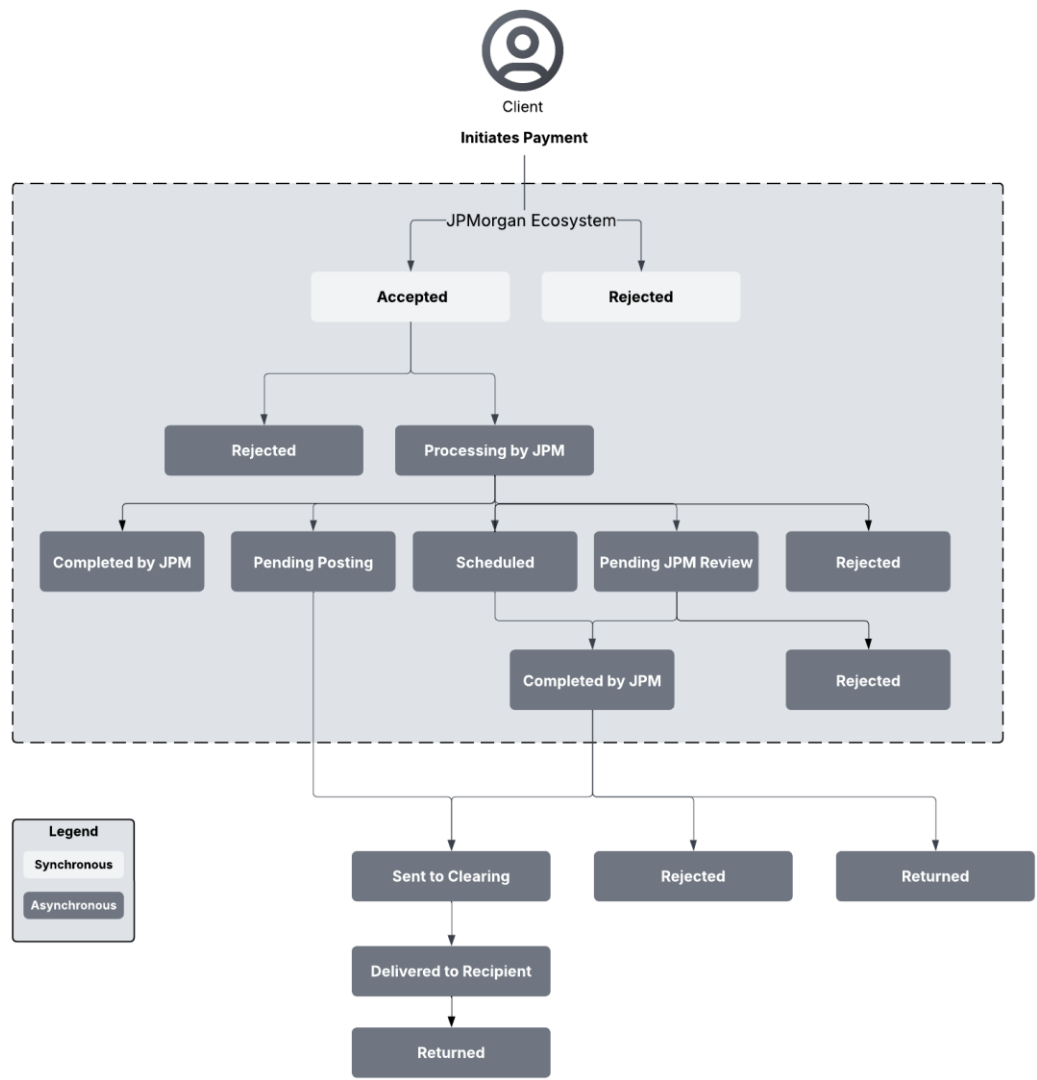
In GP2, we introduced sub-statuses to provide more granular information about your payment.

For additional information on status responses, please visit the PDP:

<https://developer.payments.jpmorgan.com/api/treasury/global-payments/global-payments-2/error-codes>

Status	Sub-Status	Description
ACCEPTED	ACCEPTED	The payment was accepted at the initiation layer.
PROCESSING	PROCESSING BY JPM	The payment is being processed by JPMorgan.
	PENDING COMPLIANCE REVIEW	Payment is under review of JPM Compliance.
	PENDING FRAUD REVIEW	Payment is on hold to review possible fraud.
	SCHEDULED	The payment is scheduled for future execution.
	PENDING POSTING	The payment was sent to an external party, such as a clearinghouse or beneficiary bank.
REJECTED	REJECTED	The payment was rejected.
	REJECTED BY JPM	The payment was rejected by JPMorgan.
COMPLETED	COMPLETED BY JPM	The payment was fully processed by JPMorgan and the necessary movement of money within JP Morgan accounts has occurred. It's no longer under the control of JPMorgan.
	SENT TO CLEARING	Payment Instruction has been sent to the clearing network.
	DELIVERED TO RECIPIENT	The payment was applied to the receiver's account.
RETURNED	RETURNED	The payment was returned by an external party, such as a clearinghouse or beneficiary bank.

4.2 Status Transition Flow



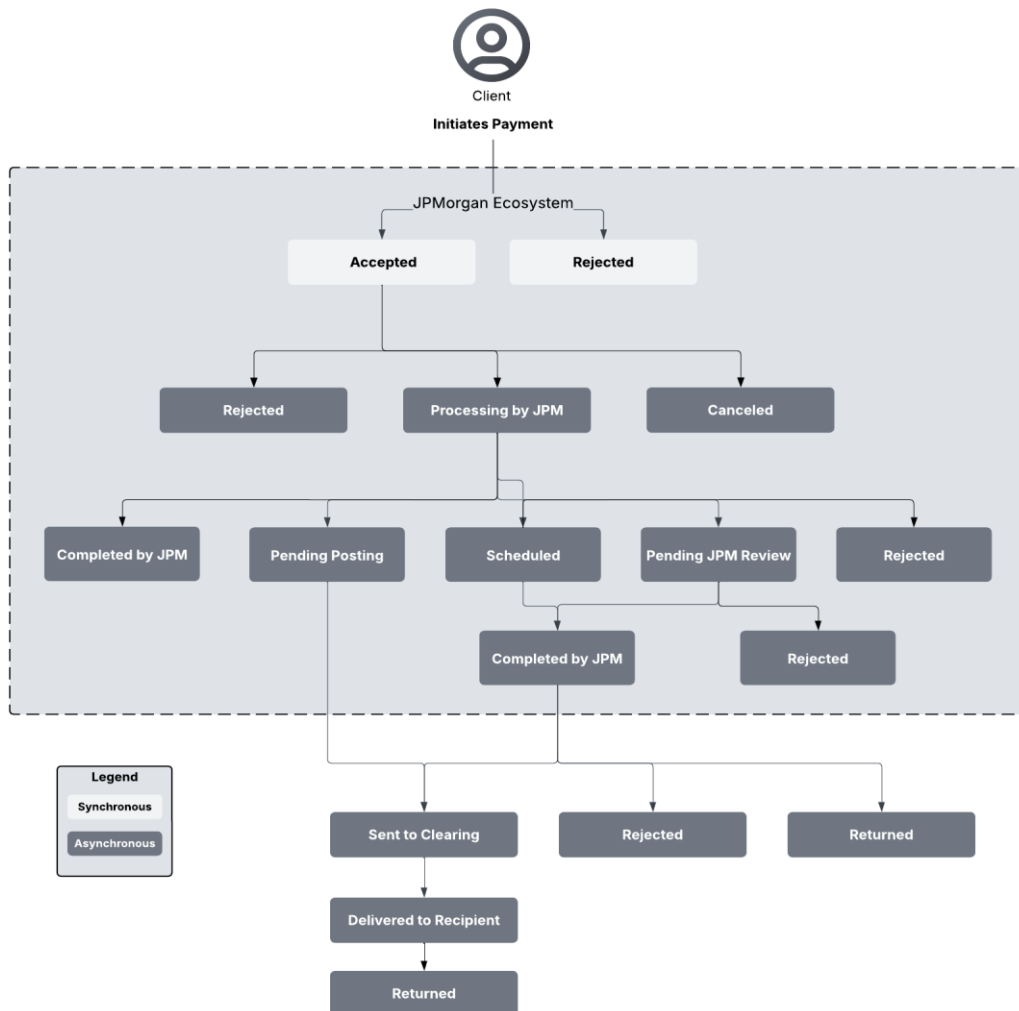
4.3 Applicable Statuses by Payment Type

Supported Statuses for Global RTP: Please find the list to the statuses and sub-statuses for all RTP market transitions in link attached [Global RTP Transactions Statuses](#)

Markets	Status	Sub-Status
Global RTP	ACCEPTED	ACCEPTED
Global RTP	PROCESSING	PENDING JPM REVIEW
Global RTP <i>*not applicable in US</i>	PROCESSING	SCHEDULED
Global RTP <i>*not applicable in US</i>	CANCELED	CANCELED
Global RTP	REJECTED	REJECTED
Global RTP	REJECTED	REJECTED BY JPM
Global RTP	COMPLETED	COMPLETED BY JPM
Hong Kong FPS and SEPA Instant only	COMPLETED	DELIVERED TO RECIPIENT
Global RTP <i>*not applicable in Chile</i>	RETURNED	RETURNED

Note: The table above is up to date as of: October 29, 2025.

Status Transitions For US ACH:



More supported statuses/status transitions for other payment types will be progressively added to this Integration Guide.

4.4 Payment Events

Callbacks and Webhooks

Callbacks and webhooks allow systems to send real-time notifications about status changes, removing the need for constant polling. Callback certificates serve as the documentation and authorization for setting up these notifications, while webhooks are the actual deliverables that transmit live event data between systems.

To receive these updates, clients must subscribe to our callbacks—without this subscription, users will not get automatic notifications and will have to rely on manual polling instead.

Cloud Events

Cloud Events offer a standardized way to describe event data in cloud-based environments. This is newly introduced in the GP2 callbacks and will eventually provide the capability for clients to subscribe to webhooks based on events that they care about (functionality coming soon via the PDP).

List of supported events today:

They align with our payment statuses, and in the future allow clients to selectively subscribe to callbacks with events that they are more interested in.

Status	Sub-Status	Payment Event
ACCEPTED	ACCEPTED	Payment.Accepted
PROCESSING	PROCESSING_BY_JPM	Payment.Accepted
PROCESSING	PENDING_JPM_REVIEW	Payment.Held
PROCESSING	SCHEDULED	Payment.Accepted
PROCESSING	PENDING_POSTING	Payment.Settlement.Sent
CANCELED	CANCELED	Payment.Canceled
REJECTED	REJECTED_BY_JPM	Payment.Rejected
REJECTED	REJECTED	Payment.Rejected
COMPLETED	COMPLETED_BY_JPM	Payment.Completed
COMPLETED	SENT_TO_CLEARING	Payment.Settlement.Sent
COMPLETED	DELIVERED_TO_RECIPIENT	Payment.Settlement.Completed
RETURNED	RETURNED	Payment.Returned

4.5 Payload and Response Samples for Payment Initiation

Below are common responses you will receive from the API and explanations of what certain parts of the schema mean.

1. Sample Payload on GP2 - Push to Wallet
2. Synchronous Response - Accepted & Created Payment
3. Synchronous Response - Duplicate payment (same endToEndId sent within 60 days)
4. Synchronous Responses - Duplicate payment (same idempotency key used within 24 hours)
5. Synchronous Response - Other Rejections
6. Asynchronous Response/ Webhook - Processing or Completed
7. Asynchronous Response/ Webhook - Payment Rejected
8. Get Status - Sample Schema

1. Sample Payload on GP2 – Push to Wallet

```
{
  "requestedExecutionDate": "2025-10-15",
  "paymentIdentifiers": {
    "endToEndId": "PUSHTOWALLET1234"
  },
  "transferType": "CREDIT",
  "value": {
    "currency": "USD",
    "amount": "100.01"
  },
  "paymentType": "PAYPAL",
  "debtor": {
    "name": "John Smith",
    "account": {
      "accountNumber": "083472915624308",
      "accountType": "DDA"
    }
  },
  "debtorAgent": {
    "financialInstitutionIds": [
      {
        "id": "CHASUS33",
        "idType": "BIC"
      }
    ]
  },
  "creditor": {
    "name": "JPMC",
    "account": {
      "alternateAccountIdentifiers": [
        {
          "identifier": "test123@email.com",
          "idType": "PROPRIETARY",
          "proprietarySchemeName": "EMAL"
        }
      ]
    },
    "postalAddress": {
      "postalCode": "10001",
      "country": "US"
    }
  },
  "paymentPurpose": {
    "purpose": {
      "proprietary": "GOODS"
    }
  },
  "remittanceInformation": {
    "unstructuredInformation": [
      {
        "text": "Sample remittance info"
      }
    ]
  }
}
```

The GP2 schema orders information in a hierarchical, logical format, including debtor/ creditor accounts, purpose codes and category purpose codes, and structured and unstructured remittance and tax information.

2. Synchronous Response – Accepted & Created Payment

```
{
  "paymentId": "1b2c3d4e-5f6a-7b8c-9d0e-f1a2b3c4d5e6",
  "paymentStatus": "ACCEPTED",
  "paymentSubStatus": "ACCEPTED",
  "statusUpdatedAt": "2025-10-15T18:48:57Z",
  "requestedExecutionDate": "2024-10-22",
  "paymentIdentifiers": {
    "endToEndId": " aBcDeFgHiJkLmNoP "
  },
  "transferType": "CREDIT",
  "paymentType": "RTP"
}
```

In GP2, we send a HTTP 201 response for an Accepted and Created payment, including a mandatory header (not included in this body sample) that shows you where you can get the latest details of this newly created payment resource.

3. Synchronous Response – Duplicate payment (same endToEndId within 60 days)

```
{
  "duplicateOf": {
    "paymentId": "1b2c3d4e-5f6a-7b8c-9d0e-f1a2b3c4d5e6",
    "paymentIdentifiers": {
      "endToEndId": "aBcDeFgHiJkLmNoP"
    }
  },
  "links": {
    "payment": "v2/payments/1b2c3d4e-5f6a-7b8c-9d0e-f1a2b3c4d5e6"
  },
  "reason": {
    "code": "11909",
    "location": "BODY",
    "message": "This is a business duplicate, refer to documentation."
  }
}
```

In GP2, we send a HTTP 200 response for a duplicate payment. The response clearly states that this is a duplicate payment, sharing the paymentId of the original payment that was accepted and created by the system. There is also a link where you can go to get the latest details of the original payment, before deciding whether to re-send your payment with a different endToEndId or leave the original payment as-is.

4. Synchronous Response – Duplicate payment (same idempotency key used within 24 hours)

```
{
  "title": "Idempotency Failure",
  "httpStatus": 422,
  "traceId": "00-00000000000000005ba75849d3ff8f2c-0ead1367b673c311-01",
  "context": [
    {
      "code": "10106",
      "message": "Idempotency Key must not be reused across different payloads of this operation"
    }
  ]
}
```

This error occurs when an idempotency key is reused for different request payloads in the same operation. To resolve it, ensure that each unique request uses a distinct idempotency key.

5. Synchronous Response – Other Rejections

```
{
  "title": "Forbidden",
  "httpStatus": 403,
  "traceId": "00-0000000000000000638c257dd60e6662-638c257dd60e6662-01",
  "context": [
    {
      "code": "14000",
      "message": "Security failure"
    }
  ]
}
```

This is a sample error that is triggered by our system when the payment fails our initial API checks. The next section covers different error scenarios in detail.

6. Asynchronous Response/ Webhook – Processing or Completed

```
{
  "specversion": "1.0.0",
  "id": "ec521d12-416e-4f48-a1b8-1d61e40146d2",
  "time": "2025-07-18T07:03:22.503+00:00",
  "type": "Payment.Completed",
  "source": "PaymentV2/PaymentToEndId=IMPS_0718123057",
  "dataschema": "urn:com.jpmorgan.payments/payment-event",
  "data": {
    "payments": [
      {
        "paymentId": "01981c56-0e48-7000-bfec-6fb5be1b3cc0",
        "requestedExecutionDate": "2025-01-06",
        "paymentStatus": "COMPLETED",
        "paymentSubStatus": "COMPLETED_BY_JPM",
        "statusUpdatedAt": "2025-07-18T07:03:22.503+00:00",
        "paymentIdentifiers": {
          "endToEndId": "IMPS_0718123057"
        },
        "paymentType": "RTP",
        "transferType": "CREDIT",
        "clearingSystem": {
          "reference": "D49KMSHY8GG2"
        }
      }
    ]
  }
}
```

- ① This is the Payment Event, part of the Cloud Event Specifications introduced in webhooks in GP2
- ② Provides the link to view the payment status
- ③ Payment status and sub-status
- ④ Depending on the payment type and clearing system, we might deliver the clearing system ID alongside the JPMorgan-assigned paymentId in the webhook.

7. Asynchronous Response/ Webhook – Payment Rejected

```

{
  "specversion": "1.0.0",
  "id": "25d712f7-3dd9-48f4-a69e-a3135e7ed9e5",
  "time": "2025-07-18T07:30:10.170+00:00",
  "type": "Payment.Rejected",
  "source": "payment/v2/payments?endToEndId=IMPS_0718120916",
  "dataschema": "urn:com.jpmorgan.payments/payment-event",
  "data": {
    "payments": [
      {
        "paymentId": "01981c42-3439-7000-87cc-52975776be03",
        "requestedExecutionDate": "2025-01-06",
        "paymentStatus": "REJECTED",
        "paymentSubStatus": "REJECTED",
        "statusUpdatedAt": "2025-07-18T07:30:10.170+00:00",
        "paymentIdentifiers": {
          "endToEndId": "IMPS_0718120916"
        },
        "paymentType": "RTP",
        "transferType": "CREDIT",
        "clearingSystem": {
          "reference": "519912266003"
        },
        "exceptions": [
          {
            "code": "11006",
            "message": "Account specified is blocked, prohibiting posting of transactions against it.",
            "location": "BODY",
            "additionalContext": [
              {
                "type": "ISO20022",
                "code": "AC06",
                "message": "Account specified is blocked, prohibiting posting of transactions against it"
              }
            ]
          }
        ]
      }
    ]
  }
}

```

Follows a similar format to the previous sample with regards to the payment event, status and sub-status. Compared to earlier versions of JPMorgan's APIs, GP2 offers more than 1 set of error codes, including ISO/ external codes as part of Additional Context. Further details on error codes can be found in Section 5 of this guide.

8. Get Status – Sample Schema

```
{
  "paymentId": "a1b2c3d4-e5f6-1234-abcd-abcdef123456",
  "requestedExecutionDate": "2025-01-06",
  "paymentStatus": "COMPLETED",
  "paymentSubStatus": "COMPLETED_BY_JPM",
  "statusUpdatedAt": "2025-07-18T07:03:19.214+00:00",
  "paymentIdentifiers": {
    "endToEndId": "INDIAIMPS1234"
  },
  "paymentType": "RTP",
  "transferType": "CREDIT",
  "clearingSystem": {
    "reference": "AB12CD34EF56"
  }
}
```

The structure is very similar to a callback in terms of required attributes and supporting the status and sub-status; it just does not include the Cloud Event specifications.

4.6 Payload and Response Samples for Client Initiated Returns

Below are common responses you will receive from the API for the Payment Returns endpoint.

1. Brazil RTP Returns – Full return
2. Brazil RTP Return – Partial return

1. Brazil RTP Returns – Full return

```
{
  "paymentType": "RTP",
  "originalPaymentIdentifiers": {
    "clearingSystemReference": "2QJ0B5XH320E059B117983652402Y5Q"
  },
  "paymentIdentifiers": {
    "endToEndId": "015520300215950001"
  },
  "chargeBearer": "DEBTOR",
  "country": "BR",
  "returnType": "FULL"
}
```

For returns, it is mandatory to specify at least one of the original payment identifiers such as bankReferenceNumber or clearingSystemReference or paymentId. If the client is issuing a full return, there is no need to specify the return amount.

2. Brazil RTP Returns – Partial return

```
{
  "paymentType": "RTP",
  "originalPaymentIdentifiers": {
    "clearingSystemReference": "185E2954302601583511865029340558"
  },
  "paymentIdentifiers": {
    "endToEndId": "K105250090305750052"
  },
  "chargeBearer": "DEBTOR",
  "country": "BR",
  "returnType": "PARTIAL",
  "value": {
    "amount": "30",
    "currency": "BRL"
  }
}
```

If the client is issuing a partial return, there is a need to specify the return amount.

The response for accepted, duplicate and rejected payments will follow the same format as the Payment endpoint in the previous section.

5. Error Handling

5.1 Error Code Catalog

Error codes identify the reason that a request results in an error. In the PDP, users are able to access a comprehensive list of tables that document and detail all the possible error codes and their descriptions for GP2.

We support standard HTTP Status Codes: 400, 401, 403, 404, 422, 429, 503.

For the full list of error codes, please visit the PDP: <https://developer.payments.jpmorgan.com/api/treasury/global-payments/global-payments-2/error-codes>

5.2 Types of Error Codes

In GP2, specially for **HTTP 400 Bad Request** Errors, we support 3 types of error codes. The Unified Code is always sent, and external/ clearing codes are sent on a case-by case basis under the “Additional Context” block.

- I. **Unified Codes:** 5-digit code proprietary code assigned by JPMorgan, that is granular to specific errors. By being fully numerical, these codes are easier for systems to parse, and align with industry standards.
- II. **ISO/ External Codes:** These codes are typically (but not always) in the ISO format, and might be preferred by companies more familiar with the ISO standard or want to be interoperable with other banks.
- III. **Clearing Network Code:** Codes that are assigned by the clearing network. This is sent only for US ACH today.

5.3 Reading an Error Schema

Below is a sample error schema that contains all 3 sets of codes. Note that most error samples will only contain the Unified Code and the ISO/ External Code.

US ACH Sample
<pre> { "paymentId": "842c11d0-dbf9-4ae9-969e-5f5802ad0fac", "requestedExecutionDate": "2025-10-28", "paymentStatus": "RETURNED", "paymentSubStatus": "RETURNED", "statusUpdatedAt": "2025-10-29T07:03:19.214+00:00", "paymentIdentifiers": { "endToEndId": "USACH1234" }, "paymentType": "ACH", "transferType": "CREDIT", "exceptions": [{ "code": "11001", "message": "Account number is invalid or missing", "additionalContext": [{ "code": "ACH1", "type": "EXTERNAL", "message": "Account number is invalid or missing" }, { "code": "C14", "type": "CLEARING_NACHA", "message": "Incorrect DFI Account Number. Please use 123456789" }] }] }</pre>

The **yellow section** is JPMorgan's proprietary 5-digit code. The full error code catalog can be found on the Payments Developer Portal.

The **green section** is the ISO or external code. If an ISO code is provided, the error description will follow the ISO 20022 External Code list.

The **blue section** is the clearing code and description that is directly provided by the clearing network.

5.4 Basic Debugging of Error Codes

This section is designed to help clients recognize and address frequent error codes that may arise when using JPMorgan APIs. The table equips clients with the context needed to identify the source of a problem and communicate more effectively with support teams if further assistance is required.

By outlining possible causes of each error, this table is intended to help clients better understand the issues they face, and organized in order of when this error might be triggered first.

Error Code	HTTP Code	Error	Potential Reasons	Suggested Actions
14000	401	Authentication Failure	- Security certificates expiration - Accessing a service or account with required authorization	- Check that your security certificates are up to date/not expired - Confirm that your account has the necessary permissions
10199	403	Signature Verification Failure	- Failure to verify digital signature - JWS format required - Certificates not configured - Unsupported algorithm used	- Ensure your digital signature is correctly configured and valid - Check that your request uses the JWS format - Verify that all necessary certificates are set up - Consult support team
10199	422	Invalid Data	- Failure to decrypt the request payload - Encryption algorithm not supported - No certificates configured - Algorithm not supported	- Verify that the algorithm you are using is supported by the system - Check that your request payload is correctly encrypted and uses a supported encryption algorithm
10107	409	Concurrent request failure	The same payment is being sent twice at the same time to our systems.	- Check that you are not submitting the same payment request more than once at the same time - Wait for a confirmation response from our system before resubmitting your payment
10106	422	Idempotency Failure	The idempotency key might have been re-used within a 24-hour period.	Try resending your payment with a different idempotency key.
14000	403	Authorization Failure	- Insufficient account permissions (e.g., not set up for GP2) - Incorrect account details (e.g., debtor account not set up for client or production testing) - Other accesses are not provisioned	- Confirm that your account has the correct permissions for this event - Reach out to your Technical Implementations Contact to ensure API profile is properly configured
15000	401 or 403	System Errors	Unspecified system error.	- Wait 15 minutes and try again later - If the issue persists, contact support
12999	503	System Unavailable	The API system is currently unavailable.	- Wait 15 minutes and try again later - If the issue persists, contact support

6. Ancillary API compatibility

We acknowledge that GP2 is just one part of your overall payments journey. This section of the guide showcases complementary APIs designed to work alongside GP2, aiming to help clients build a more complete and efficient payments ecosystem.

6.1 Before Initiating a Payment

i. Account Validation Services:

Account Validation Services offer a secure and efficient solution for verifying bank account details, individuals, and businesses across multiple data sources. By validating new payee information and screening the identity of users, vendors, and suppliers, these services help prevent payment fraud and mitigate the risk of funds being redirected to unauthorized parties.

This ensures reliable transactions and supports your business's risk management and compliance needs.

Please find more information here: <https://developer.payments.jpmorgan.com/docs/fraud-solutions/validation-services>

ii. Platform Availability Communication Management (PACMan):

Platform Availability Communication Management (PACMan) is designed to keep your business informed about the status and availability of critical APIs and partner banks. PACMan delivers timely notifications and updates on both planned and unplanned outages, helping you anticipate and manage downtime with confidence.

PACMan provides real-time access to critical information, enabling proactive incident management and minimizing operational downtime. Enhancements to this API are underway for 2026, please stay tuned for upcoming changes.

Please find more information here: <https://developer.payments.jpmorgan.com/docs/treasury/pacman/doc>

6.2 Initiating a Payment

iii. Account Balances:

The Account Balances API enables you to securely retrieve both current and historical bank account balances, providing the settled cash amount in your accounts at the time of each API request. In addition to balance information, the API delivers detailed data within its response, supporting customized integration and reporting to meet your business needs.

This API is designed to enhance your financial visibility and operational efficiency, while accommodating various use cases including sweep accounts and event-based triggers.

This API may be subject to occasional outages and is not always available 24/7.

Please find more information here: <https://developer.payments.jpmorgan.com/docs/liquidity-account-solutions/account-balances/doc>

6.3 Other Payment APIs

iv. **Payments Receipts/Credit Confirmation API**

By integrating the Payment Receipts Credit Confirmations webhook, clients and users will receive immediate notifications each time your accounts are credited. This solution streamlines the reconciliation processes and ensures not only timely, but also accurate visibility into incoming payments, removing the need for manual verification.

Please find more information here: <https://developer.payments.jpmorgan.com/api/treasury/payment-receipts/doc>

v. **Request for Payment API:**

The Request for Payment (RFP) API enables businesses to securely and efficiently request real-time, guaranteed payments directly from their customers through the RTP® Network. By integrating with customers' desktop or mobile banking applications, the API facilitates seamless payment experiences with end-to-end encryption, ensuring both convenience and security.

With the RFP API, organizations can initiate payment requests, track the status of those requests, and receive instant notifications when payments are completed—empowering faster collections and supporting a new era of real-time receivables

Please find more information here: <https://developer.payments.jpmorgan.com/docs/treasury/request-for-payment/doc>

vi. **Global Mass Pay:**

Global Mass Pay is an advanced API solution that enables businesses to efficiently execute cross-border, cross-currency, and single-debit ACH payments from a single account. By providing direct access to low-value, local clearing systems, Global Mass Pay streamlines payment processes and enhances operational efficiency.

This cost-effective service empowers organizations to manage international payments seamlessly, ensuring reliable access to local clearing networks and supporting business growth in global markets.

Please find more information here: <https://developer.payments.jpmorgan.com/docs/treasury/global-mass-pay/doc>

7. Support & Troubleshooting

7.1 Best Practices

- **Documentation:** Full integration guide, troubleshooting steps, and FAQs are available on the PDP as a supplement to this Guide.
- **API Versioning:** Use the latest API version published on the PDP, and refer to the Changelog for backward compatible changes.
- **Use /Jose and not /Json** on the payment header when initiating a payment.
- **Rate Limiting:** Adhere to agreed upon rate limits to avoid API failure.

7.2 Duplicate Checks

Ensuring a payment is not erroneously processed twice is one of the top priorities of our APIs. We perform various checks in GP2 to ensure this.

Idempotency Check: This is performed by the API Gateway against the idempotency key that is inserted in the payload header. The idempotency key is an optional attribute for clients who want to avail of that option, and can be reused after 24 hours. With an idempotency failure, you will receive a HTTP 422 error with the error code 10106 as part of the synchronous response.

Business Validation Check: This check performed by our internal systems before the payment gets formally accepted against the endToEndId of the payload. Generally, clients are not allowed to use the same endToEndId within 60 days of submitting the original payment. With a business validation failure, you will receive a HTTP 200 duplicate response with a response code 11909.

Further Checks: In the final stage of payment processing before the payment gets sent to clearing, we perform further checks against other payload attributes. If a payment is flagged as duplicate in this stage, you will receive a HTTP 400 error and error codes including 11507 (AM05), 10104 (DUPL) or 11544 (BE23). Please refer to the error description for more information.

To see how responses from our API will look like in these various duplicate scenarios, please refer to Section 4.5 of this guide, or to the Payments Developer Portal: <https://developer.payments.jpmorgan.com/api/treasury/global-payments/overview#idempotency-logic>.

7.3 API Support

- Raise a request on the PDP: <https://developer.payments.jpmorgan.com/contact/support>
- Send an email to the API Support Team: api.service.support@jpmorgan.com. Supported languages are English, Portuguese, Mandarin Chinese, and Spanish.

8. Other Resources Coming Soon

We are working to expand our support materials. Please check back in the future for a Testing Playbook that will serve as a second volume to this guide.

FOR INSTITUTIONAL & PROFESSIONAL CLIENTS ONLY – NOT INTENDED FOR RETAIL CUSTOMER USE

This material was prepared exclusively for the benefit and internal use of the J.P. Morgan client to whom it is directly addressed (including such client's subsidiaries, the "Company") in order to assist the Company in evaluating a possible transaction(s) and does not carry any right of disclosure to any other party. In preparing this material, we have relied upon and assumed, without independent verification, the accuracy and completeness of all information available from public sources or which was provided to us by or on behalf of the Company or which was otherwise reviewed by us. This material is for discussion purposes only and is incomplete without reference to the other briefings provided by J.P. Morgan. Neither this material nor any of its contents may be disclosed or used for any other purpose without the prior written consent of J.P. Morgan.

J.P. Morgan, JPMorganChase, Chase, Chase Merchant Services, and Chase Payment Solutions are marketing names for certain businesses of JPMorganChase and its subsidiaries worldwide (collectively, "JPMorganChase"). Products or services may be marketed and/or provided by commercial banks such as JPMorgan Chase Bank, N.A., securities or other non-banking affiliates or other JPMorganChase entities. JPMorganChase contact persons may be employees or officers of any of the foregoing entities and the terms "J.P. Morgan", "JPMorganChase", "Chase", "Chase Merchant Services" and "Chase Payment Solutions" if and as used herein include as applicable all such employees or officers and/or entities irrespective of marketing name(s) used. Nothing in this material is a solicitation by JPMorganChase of any product or service which would be unlawful under applicable laws or regulations.

Investments or strategies discussed herein may not be suitable for all investors. Neither J.P. Morgan nor any of its directors, officers, employees or agents shall incur in any responsibility or liability whatsoever to the Company or any other party with respect to the contents of any matters referred herein, or discussed as a result of, this material. This material is not intended to provide, and should not be relied on for, accounting, legal or tax advice or investment recommendations. Please consult your own tax, legal, accounting or investment advisor concerning such matters.

Not all products and services are available in all geographic areas. Eligibility for particular products and services is subject to final determination by JPMorganChase and or its affiliates. This material does not constitute a commitment by any JPMorganChase entity to extend or arrange credit or to provide any other products or services and J.P. Morgan reserves the right to withdraw at any time. All products and services are subject to applicable laws, regulations, and applicable approvals and notifications. The Company should examine the specific restrictions and limitations under the laws of its own jurisdiction that may be applicable to the Company due to its nature or to the products and services referred herein.

Any mentions of third-party trademarks, brand names, products and services are for referential purposes only and any mention thereof is not meant to imply any sponsorship, endorsement, or affiliation.

Notwithstanding anything to the contrary, the statements in this material are not intended to be legally binding. Any products, services, terms or other matters described herein (other than in respect of confidentiality) are subject to, and superseded by, the terms of separate legally binding documentation and/or are subject to change without notice.

Changes to Interbank Offered Rates (IBORs) and other benchmark rates: Certain interest rate benchmarks are, or may in the future become, subject to ongoing international, national and other regulatory guidance, reform and proposals for reform. For more information, please consult: <https://www.jpmorgan.com/global/disclosures/interbank-offered-rates>.

JPMorgan Chase Bank, N.A. Member FDIC. Deposits held in non-U.S. branches are not FDIC insured. Non-deposit products are not FDIC insured.

JPMorgan Chase Bank, N.A., organized under the laws of U.S.A. with limited liability.

© 2026 JPMorgan Chase & Co. All Rights Reserved.