

API Keys

Overview

PayNet's API Gateway utilises OAuth 2.0 and requires an access token to be passed in each request for authentication. Before your application can generate an access token and make requests to PayNet APIs, you will need to generate API keys for your application.

INFO

We are in the midst of updating all our APIs to support OAuth2.0. Please refer to the respective API product reference to find out which authentication method is being supported currently.

Generating your API Keys

To generate your application's API keys, you will need to register your application in the [PayNet Developer Portal](#). Once registered, you will be provided a *Client ID* and *Client Secret* key pair for your application to be used in the Development environment.

Field	Description
Client ID	Similar to how a username identifies a user, the Client ID identifies the application that is making the API call.
Client Secret	Similar to how a password proves a user is who they say are, the Client Secret is used to validate the identity of the application that is making the API call.

INFO

API Keys for Production environment are generated immediately, but will still need to be approved for access before your application can go live. Once your Production access request has been reviewed, you will be notified on whether access has been approved or denied.

Managing your API Keys

In the Developer Portal there are 3 possible actions for managing your API keys:

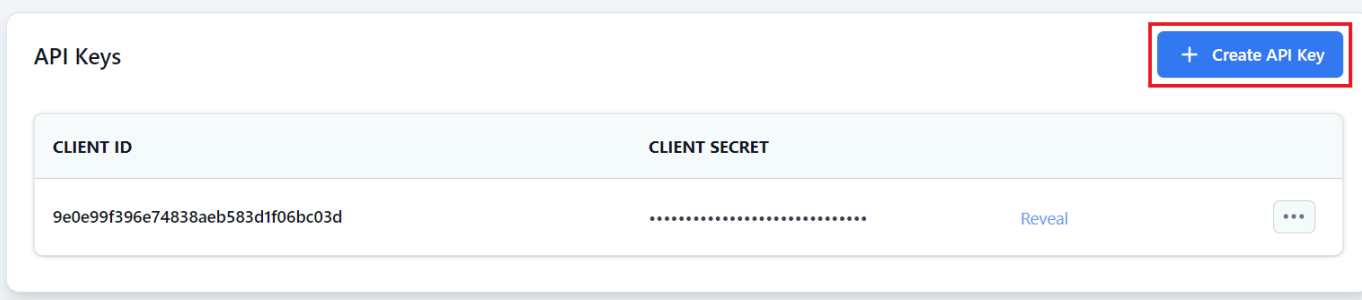
Create an API Key

Renew an API Key

Revoke an API Key

Create an API Key

Step 1: Click **Create API Key**.



The screenshot shows the 'API Keys' management interface. At the top right, there is a blue button labeled '+ Create API Key' which is highlighted with a red rectangular box. Below this is a table with two columns: 'CLIENT ID' and 'CLIENT SECRET'. The table contains one row with the following data:

CLIENT ID	CLIENT SECRET
9e0e99f396e74838aeb583d1f06bc03d Reveal

On the far right of the table row, there is a small grey button with three dots (⋮).

Step 2: Click **Confirm**.

Create API Key

Are you sure you want to create new API key?

CancelConfirm

Step 3: The newly created API key pair will be listed.

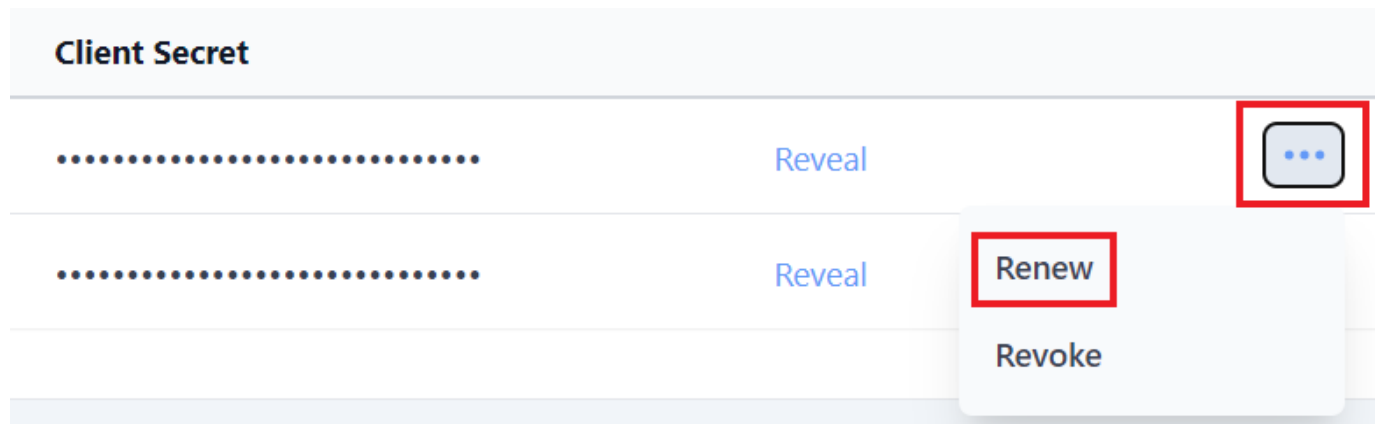
API Keys

+ Create API Key

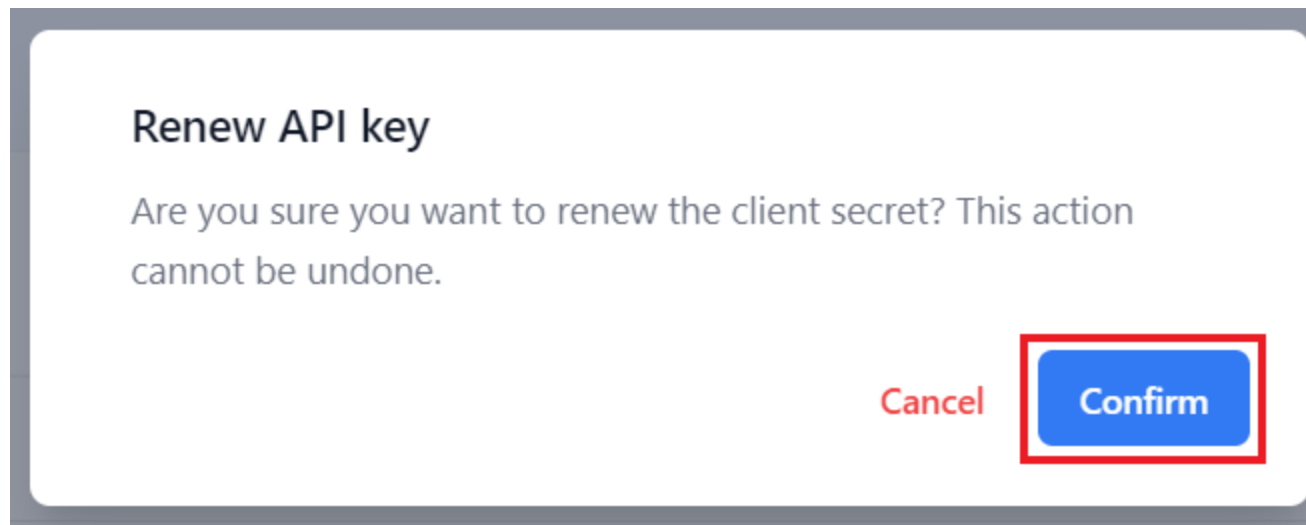
CLIENT ID	CLIENT SECRET	
9e0e99f396e74838aeb583d1f06bc03d	Reveal ...
fd65ae2dcc764bdbabcca60b663ffa4e	Reveal ...

Renew an API Key

Step 1: Click the three dots ... next to the key you want to renew and click **Renew**.



Step 2: Click **Confirm**.



Revoke an API Key

Step 1: Click the three dots  next to the key you want to renew and click **Revoke**.

Client Secret	
.....	Reveal
.....	Reveal

Renew

Revoke

Step 2: Click **Confirm**.

Revoke API key

Are you sure you want to revoke the API key? This action will immediately delete key from database and cannot be undone.

Cancel

Confirm

Using the API Keys

The assigned *Client ID* and *Client Secret* keys are to be passed to the [OAuth 2.0 API](#) endpoint to generate an access token. On successful request, an access token will be returned which can subsequently be used to make requests to PayNet's APIs. The access token should be re-generated by the application once expired.

How It Works

Once you have received the *Client ID* and *Client Secret* from Developer Portal, you may trigger API calls to our OAuth 2.0 resource server for token issuance. A Bearer token will be created and you embed that token inside the `Authorization` header for subsequent API calls.

Generate `client_id` and `client_secret` from Developer Portal.

Call Authentication API to generate access token.

Sample Request:

cURL

```
curl --location --request POST 'https://sandbox.api.paynet.my/auth/token' \
--header 'Accept: application/json' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=<client_id>' \
--data-urlencode 'client_secret=<client_secret>' \
--data-urlencode 'grant_type=client_credentials'
```



Sample Response:

```
{
  "access_token":
    "eyJraWQiOiJmMGFIYjYyYzZhM2M0MmQ4YjA0N2Y4MmQ2NmY5NTA2OCIsImFsZyI6IjR0bm90bnQ4LgE2xPbp3feliCP4NmMMP4FK95slgPrEZpCr-2qqStBrN4DNaYWWLtlXnuCg31aD1934Zjq-T_
    "token_type": "bearer",
    "scope": "rpp:merchant",
    "expires_in": 86400
}
```



Append `access_token` from response field into `Authorization` field of API request.

```
curl --location -g --request PUT 'https://api_domain' \
--header 'Authorization: Bearer
eyJraWQiOiJmMGFIYjYyYzZhM2M0MmQ4YjA0N2Y4MmQ2NmY5NTA2OCIsImFsZyI6IjI0IiwiaXN0eWZldW
wWZmiQLQ4LgE2xPbp3feliCP4NmMMP4FK95slgPrEZpCr-2qqStBrN4DNaYWWLtlXnuCg31aD1934Zjq-T_
--data-raw '{
  <Sample Body>
}'
```