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.

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.

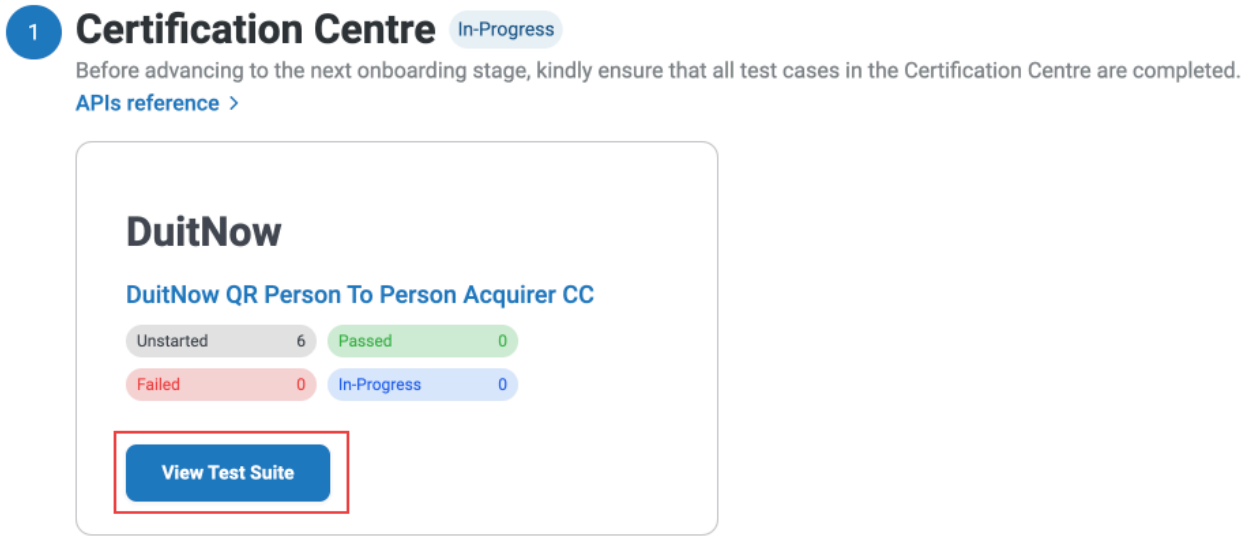
Obtaining Your API Keys

INFO

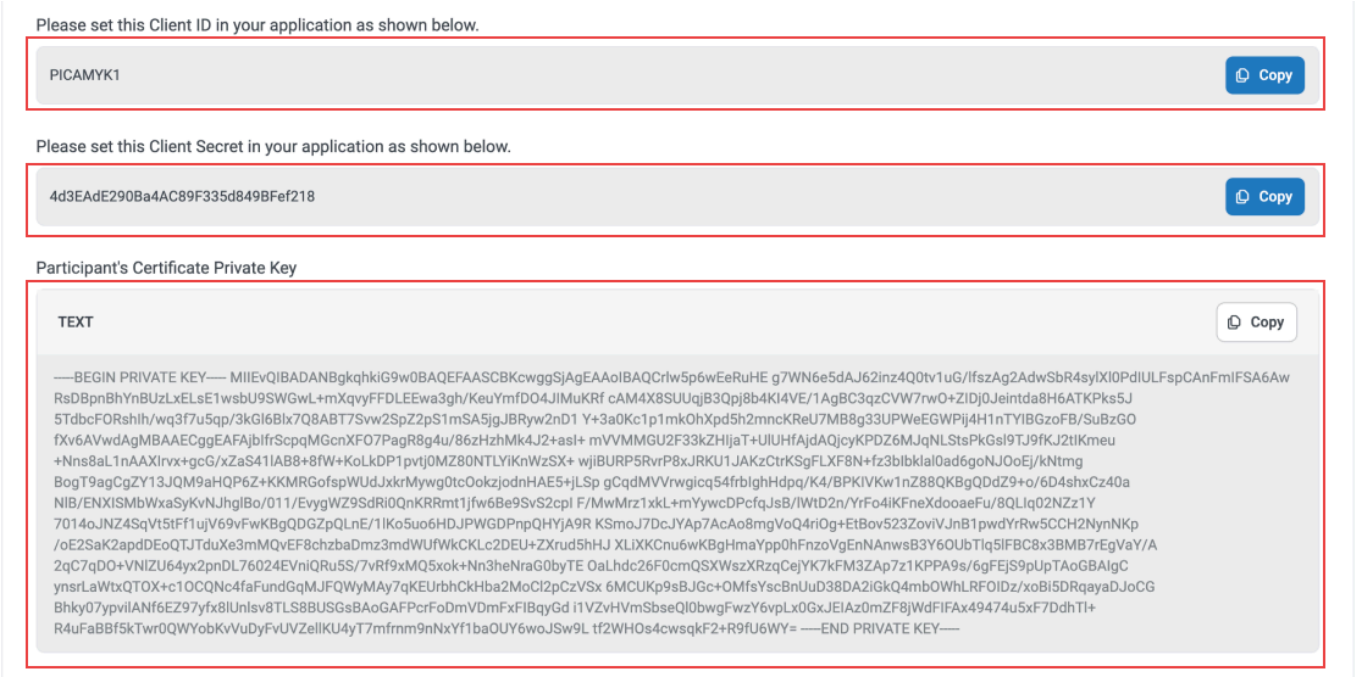
Depending on the stages of onboarding, the process of obtaining your API keys will be different. Please refer to the guide below on how to obtain your *Client ID* and *Client Secret* values.

Certification Centre | System Verification | Production

Step 1: Click the button “View Test Suite” access to test suite



Step 2: Step 2: Scroll to the section “Please set this Client ID in your application as shown below”



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.

1. Generate or obtain your `client_id` and `client_secret` values from Developer Portal.

2. Call Authentication API to generate access token.

INFO

Please be aware of the differences in the URL for each environment.

Certification Centre | System Verification | Production

```
curl --location
'https://certification.api.developer.inet.paynet.my/v1/picasso-
guard/auth/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_id=**yourClientId**' \
--data-urlencode 'client_secret=**yourClientSecret**'
```

3. Below is an example of the response that you should expect.

```
{
    "access_token":
"eyJraWQiOiJmMGFlYjYyYzZhM2M0MmQ4YjA0N2Y4MmQ2NmY5NTA2OCIsImFsZyI6IlJTMjU2In0.eyJ
wWZmiQLQ4LgE2xPbp3feliCP4NmMMPr4FK95sIgPrEZpCr-2qqStBrN4DNaYWWLtlXnuCg31aD1934Zj
    "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' \
// highlight-next-line
--header 'Authorization: Bearer
eyJraWQiOiJmMGFlYjYyYzZhM2M0MmQ4YjA0N2Y4MmQ2NmY5NTA2OCIsImFsZyI6IlJTMjU2In0.eyJz
wWZmiQLQ4LgE2xPbp3feliCP4NmMMPr4FK95sIgPrEZpCr-2qqStBrN4DNaYWWLtlXnuCg31aD1934Zj
--data-raw '{
    <Sample Body>
}'
```