
Clearstream API Developer Guide

November 2022

Change log

3 June 2021	First draft
10 September 2021	SSL extraction details added
29 September 2021	Rework for Preview
11 November 2021	First version for publication
25 November 2021	Rebranding
8 February 2022	Simplification of DBP integration
3 June 2022	Clarifications on API onboarding + Additional troubleshooting & support sections
20 June 2022	Removal of DBP user ID references, SSL cert/keys scripts clarified
23 August 2022	Clarifications on API onboarding + November certificate changes for API consumers
23 September 2022	Support page improvements
4 November 2022	Rework for November 2022 API roll-out
15 November 2022	Adding additional information on CA certificates

Introduction

This developer guide provides an overview on how to discover and integrate with Clearstream APIs as well as how to access and use the Clearstream API setup. The current infrastructure is powered by:

- Deutsche Börse Digital Business Platform (DBP) – The API developer platform and catalogue
- Clearstream XACT – The Clearstream customer facing web platform
- Clearstream API Platform – The API component of Xact

This guide is targeted at developers as well as technical project managers and software architects interested in building systems using Clearstream APIs. This guide assumes a basic understanding of various API related topics such as HTTP, REST, OAuth2.0, mutual TLS, etc.

It must be noted that due to the sensitive nature of financial APIs, Clearstream APIs require additional setup steps which are detailed in the “Pre-requisites” chapter of this document.

The “Example code” section provides a script based example which illustrates how to build using Clearstream APIs. OpenAPI specifications are always published to the digital business platform in their most recent version. Some APIs reference additional documentation through their description.

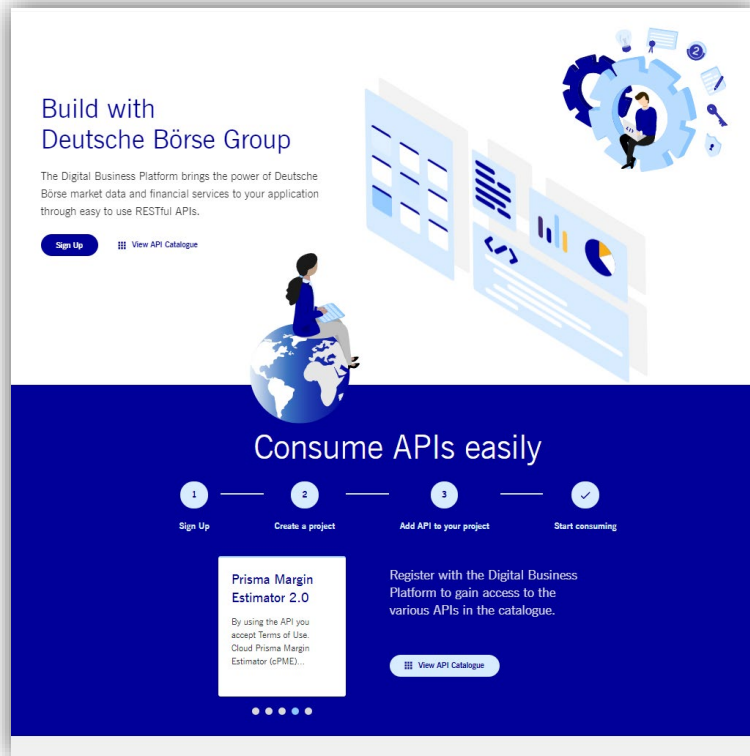
Table of Contents

Change log	ii
Introduction.....	1
Table of Contents	2
Pre-requisites	3
Digital Business Platform	3
Xact Web Portal.....	4
Xact Web Portal subscription & MT599 API onboarding messages.....	4
Step 1 - Xact API consumer creation.....	5
Step 2 - Xact API consumer creation.....	6
Getting Started.....	7
Clearstream OCAPI Playground.....	7
Certificate Chains, Certificate Authorities (CAs), Truststores & more.....	8
Getting an OAuth2.0 Bearer Token (access_token)	9
Accessing the Playground API	10
Troubleshooting.....	11
1) I cannot get my OAuth2.0 client to work. How does the support page work?	11
2) How do I convert the Xact API consumer PEM files to P12 files?.....	12
3) When requesting a bearer token (access_token), HTTP 4xx errors (client-errors) are returned	12
4) Using curl I am unable to retrieve an access_token and I get SSL/TLS errors.	13
5) Mutual TLS is not part of the OAuth2.0 spec and is not supported by my library	13
6) How to troubleshoot and/or debug with CURL commands	13
How to get development support from Clearstream?.....	14
Example code.....	16
Bash/CURL	16

Pre-requisites

Digital Business Platform

To browse through the Clearstream API catalogue developers must consult the digital business platform (DBP). <https://console.developer.deutsche-boerse.com>.



This platform serves as a DBG-wide API inventory and presents all available Clearstream APIs, their descriptions, points of contact as well as Swagger / OpenAPI specifications.¹

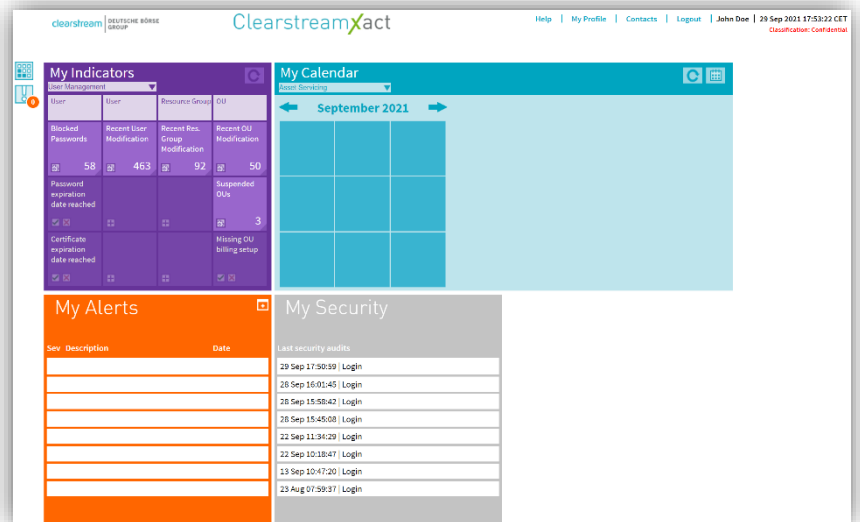
¹ Please note that for the pre-production / UAT / OCCT environment (<https://api-t2s-test.clearstream.com/>), a staging deployment of the DBP is available under: <https://console.cstest.dbpapi.com>
Clearstream API Developer Guide
Clearstream Banking S.A

Xact Web Portal

This section presents the required Xact Web Portal setup as well as the API consumer credentials setup mandatory for any successful API call.

Xact Web Portal subscription & MT599 API onboarding messages

Xact Web Portal is a web-based, connectivity channel offering online access to a variety of post-trade services and more. In addition, Xact Web Portal provides access management for Clearstream APIs published on the Digital Business Platform. By design, Clearstream APIs are treated as business resources and are therefore protected by fine grained user access control mechanisms and API credentials.



Existing Xact Web Portal customers must send an **MT599 SWIFT** message to the Clearstream address **CEDELULLXXX, (ATTN: PRGConnect)** to enable the Clearstream API service for their Organisation Unit (OU). In this message, a request for one or more specific API resources can be included. As a minimum, the Clearstream API Playground should be requested for an initial onboarding in production.

The full list of available API resources, including descriptions, is available in the public [DBP API Catalogue](#)

The below example shows the required format of this MT599 SWIFT message. Please make sure that the message contains only SWIFT compliant characters!

```
ATTN: PRGConnect
SUBJECT: Clearstream APIs
Please add the Clearstream API service
and link the Clearstream API Playground resource
to our Xact OU xxxxxx
Contact details: John Doe, john.doe(at)xxxxxx.xyz, 00123456789
```

For customers that already have the Clearstream API service added in their OU, the following shortened MT599 message can be used instead of the above:

```
ATTN: PRGConnect
SUBJECT: Clearstream APIs
Please link the <API-NAME-FROM-DBP-CATALOGUE> API resource
to our Xact OU xxxxxx
Contact details: John Doe, john.doe(at)xxxxxx.xyz, 00123456789
```

Future customers as well as other interested parties are advised to contact the Clearstream Connectivity Helpdesk directly for additional information about how to setup. (connect@clearstream.com).

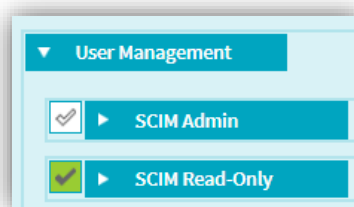
Step 1 - Xact API consumer creation

API consumer credentials can be created by following the standard Xact Web Portal user creation procedure². The user type must be set to “API Consumer”³. In the first step of the API consumer creation, the grants of the technical user are configured:

Service name	Property name	Category	Updatable by	Value
User Management	Smart Card	Credentials Types	All Types of Admin Users	Allowed
User Management	Software Key Store	Credentials Types	All Types of Admin Users	Allowed
User Management	User Mgt N-Eyes Principle	N-Eyes	All Types of Admin Users	2 eyes
User Management	User Time Zone	System	All Types of Admin Users	CET
User Management	Preferred Language	Session	All Types of Admin Users	English
Clearstream APIs	DBP User Id	DBP	All Types of Admin Users	164c0fc3-340e-4f56-80e4-6a7ccaaacc34

In the grant-selection component, an API consumer can be granted one or more Clearstream APIs.

In addition to this general coarse-grained API access, depending on the API it might be necessary to grant specific fine-grained roles. For example, for most user management API calls to succeed, the SCIM Admin or SCIM Read-Only roles are required in addition to the Xact Web Portal User Management API role.



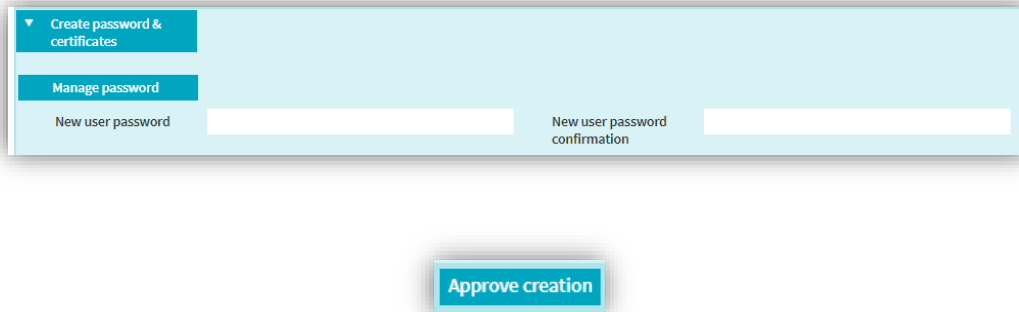
However, some APIs (such as the Clearstream API playground) do not need additional fine-grained access management. The DBP documentation describes which API endpoint offers which roles and how they can be used.

² See: <https://www.clearstream.com/resource/blob/1311454/6a3813957a058c3138ba6fcdeb6dde71/xactusermanual-en-data.pdf>

³ Xact Web Portal OUs need to be granted access to the Clearstream API service and must be configured with at least two valid administrators to create “API Consumer” users.

Step 2 - Xact API consumer creation

The second step of the API Consumer creation deals with credential generation. After submitting the future API consumer password, private keys will be locally generated in the browser for which certificates (that is, CSRs) are then generated and returned. This results in the download of two PEM files containing certificates and keys.



▼ Create password & certificates

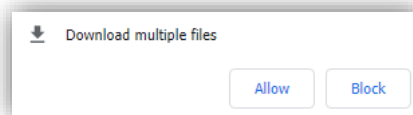
Manage password

New user password

New user password confirmation

Approve creation

Your browser might prevent the simultaneous download the 2 PEM files. In this case the download needs to be confirmed. Google Chrome shows the below pop-up:



2 PEM files will be downloaded containing the:

- ✓ Signing certificate and key
- ✓ **SSL (TLS) certificate and key**

The naming convention of the files is "**ocapi- $\{$ USERID $\}$ - $\{$ TYPE $\}$.pem**". The more important file is the SSL file as it allows establishing a mutual TLS connection with <https://api.clearstream.com> and retrieving OAuth 2.0 tokens as described in the next section.

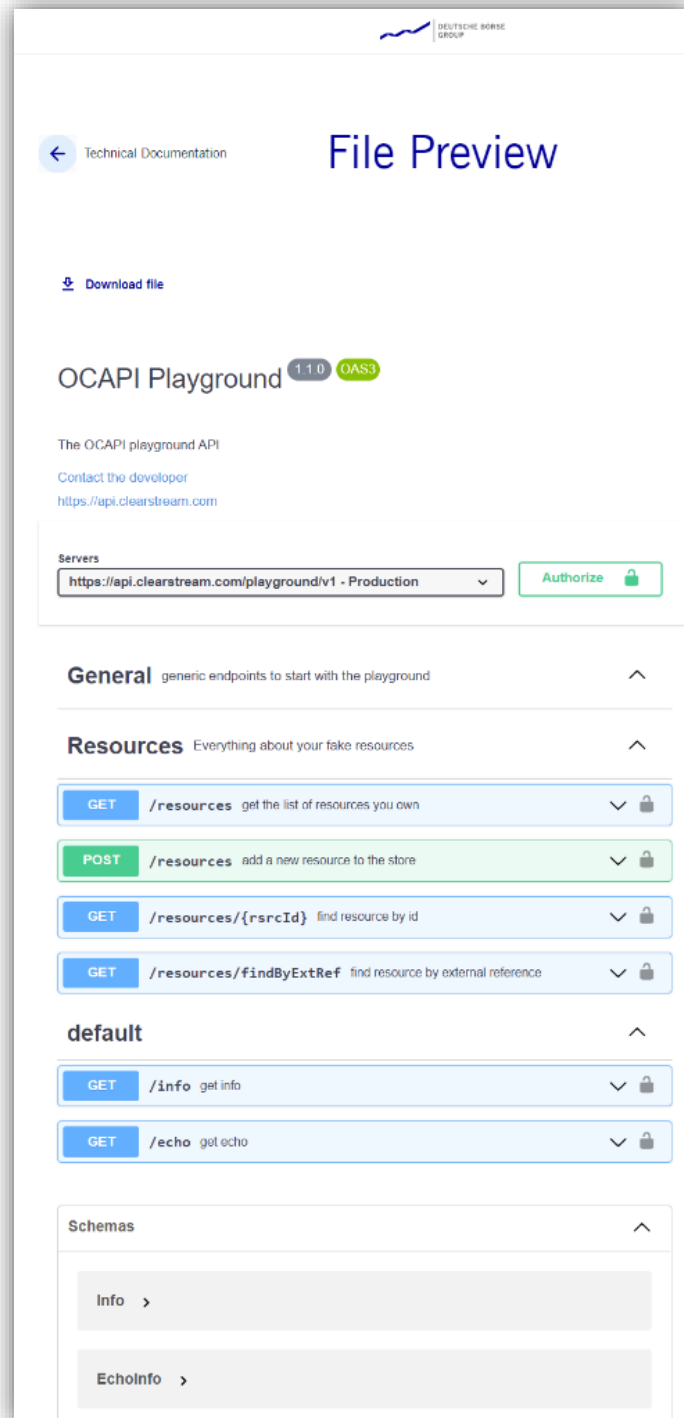


Note: Your certificates will expire after 2 years and need to be replaced beforehand. Xact Web Portal OU administrators can view the certificate expiry date in the credential details screen of the API consumers.

Getting Started

Clearstream OCAPI Playground

It is recommended to start with the “[Clearstream OCAPI Playground](#)” which offers a variety of synthetic endpoints and is provided free of charge. The OpenAPI specification of this API is available on the DBP portal under the “Technical Documentation” tab.



Certificate Chains, Certificate Authorities (CAs), Truststores & more...

To securely communicate with the Clearstream API Platform it is mandatory to add the necessary CA Certificates into your certificate authority chain or truststore.

Running in "insecure mode" without proper the certificate authority chain or truststore defined is not supported. Additionally, any form of certificate pinning is not supported. This includes adding Clearstream server certificates to the truststore.

Note: Clearstream reserves the right to update API server certificates at any point in time with no prior announcement.

Server CA Certificates

You can download the server CA certificates using the following link or using the API support page:

→ <https://api.clearstream.com/server-cert-cacerts.pem>

The **DigiCert** root and sub certificate inside this file must be present for API client use cases:

- For curl, it is sufficient to provide this the above file using the "--cacert" parameter
- For Java, the certificates from the above file should be added to a P12 or JKS truststore which is then referenced / used in the client HTTPS code.

Client CA Certificates

Note: This section can be ignored in most cases.

The Clearstream API Platform uses mutual TLS for all API calls. As a result, certificates are issued to API consumers during the API consumer creation. If you need to validate the certificate chain of the API consumer certificate, then the client CA certificates are available using the below download link.

→ <https://api.clearstream.com/client-cert-cacerts.pem>

The verification of the client certificate is not necessary for most use cases. For example, curl trusts client certificates and keys without having the full certificate chain.

Getting an OAuth2.0 Bearer Token (access_token)

Before calling the “playground” API, an OAuth2.0 bearer token needs to be requested from the Xact authorisation and authentication server. Xact has implemented the OAuth 2.0 resource owner credentials flow⁴ but has hardened it by enforcing a strict mutual TLS connection (SSL certificate/key) in addition to a consumer/user password.⁵

To request an OAuth 2.0 access token the mutual TLS curl commands below can be used. Please note that the variables in the below snippet need to be initialised correctly. When requesting a token, the desired scopes need to be specified.

```
curl
--cert ${SSL_PEM}
--cacert ${CA_PEM}
--data "grant_type=password"
--data "scope=allow ocapi-playground-v1"
--data "username=${USERNAME}"
--data "password=${LOGIN_PASSWORD}"
https://api.clearstream.com/authmanager/oauth2/access_token)
```

Running the above command yields a JSON response containing the **JWT access_token**, the granted scopes as well as a refresh token.

```
{
  "access_token": "eyJ0eXAiOiJKV1QiLCJ...",
  "refresh_token": "eyJ0eXAiOiJKV1QiLC...",
  "scope": "allow ocapi-playground-v1",
  "token_type": "Bearer",
  "expires_in": 3599
}
```

The basic authentication header required for the OAuth 2.0 client identification is not required by the Clearstream API infrastructure as clients are instead identified through their mutual TLS and consumer/user login password credentials sent via form data. However, setting this OAuth 2.0 basic-auth header to any random placeholder value is allowed and will simply be ignored by the Clearstream API infrastructure⁶.

⁴ Sometimes referred to as the OAuth2.0 password flow

⁵ Furthermore, an underlying authentication algorithm paired with a scope validator ensure the validity of any token requests before tokens are issued. Finally, the Clearstream API configuration comes with coarse grained access control to API endpoints based on the token scopes that have been granted.

⁶ For example, if your OAuth 2.0 library requires you to specify a client ID and password

Accessing the Playground API

Once a valid bearer token (access_token) has been obtained, calling API endpoints is straight forward but still requires a mutual TLS connection.

```
curl
--cert ${SSL_PEM}
--cacert ${CA_PEM} \
--header 'Authorization: Bearer ${ACCESS_TOKEN}'
https://api.clearstream.com/playground/v1/info
```

For the above playground info endpoint, the following JSON response is returned.

```
{
  "info_str": "Welcome to OCAPI Playground API ... ",
  "version": "1.221101XP.12"
}
```

Note:

- A full curl based Bash example is provided in the "Example Code" chapter.
- In case of errors, more information can be found in the "Troubleshooting" section of this document.

Troubleshooting

1) I cannot get my OAuth2.0 client to work. How does the support page work?

If there are problems with your OAuth2.0 client, please consult the [Clearstream API support](#) page which provides a working web client. (See screenshot below)

Analysing the network traffic between this web client and the Clearstream API platform with your Browser's development tools is recommended to understand how API calls should be performed. To use this client, the API consumer must be granted access to at least the Clearstream API Playground as detailed in the "Pre-Requisite" chapter.

The SSL certificate and key from the Xact credentials P12 must be imported into the browser. To convert your PEM files to P12 files for import into your browser or operating system, please use the [Clearstream API credential support page](#).

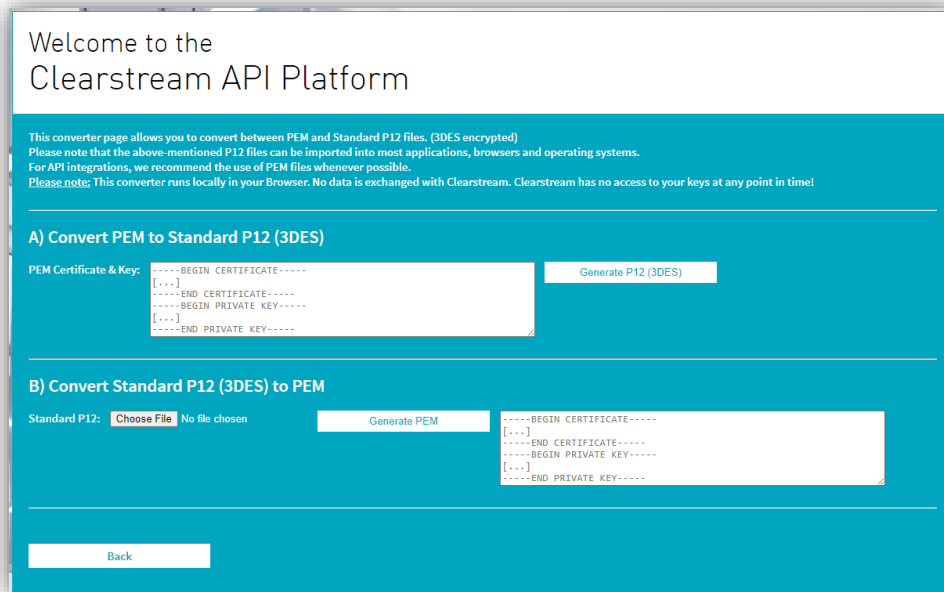
Finally the support page also provides the download links for the server and client CACerts.

The screenshot shows a web client interface for the Clearstream API Platform. The page has a white header with the text "Welcome to the Clearstream API Platform". Below the header is a teal background area containing instructions and form fields. The instructions state: "This page allows testing API access using Xact API consumer credentials (v4.2211XP.14)", followed by three bullet points: "- API access must be granted to the API consumer in Xact", "- You must import your SSL client certificate in your browser (Mandatory mutual TLS)", and "- Refer to the API credential support page to convert between PEM and P12 files". A note at the bottom of the instructions says "- Only if required download Server-CACerts here. (Download Client-CACerts here)".

The form fields are organized into two columns. The left column contains: "Token Server:" with the value "https://api.clearstream.com"; "Token Endpoint:" with the value "/authmanager/oauth2/access_token"; "API Consumer ID:" (empty); "Password:" (empty); "Scopes:" with the value "allow ocapi-playground-v1"; a "Request Access Token" button; "Token type:" (empty); "Access Token:" (empty); "Refresh Token:" (empty); "Token scopes:" (empty); "Token expiry:" (empty); and a "Back" button. The right column contains: "Clearstream APIs are documented in the DBG Digital Business Platform API catalogue" (with a link); "API Server:" with the value "https://api.clearstream.com"; "API Endpoint:" with the value "/playground/v1/info"; "Query params:" (empty); "Method:" with a dropdown menu set to "GET"; "Request headers:" with the value "Content-type: application/json; charset=UTF-8"; "Request body:" (empty); and a "Call API Endpoint" button.

2) How do I convert the Xact API consumer PEM files to P12 files?

To import your certificates and keys into your browser or operating system it might be necessary to convert the PEM files to P12 files. For this the [Clearstream API credential support page](#) provides a converter which allows going from PEM to P12 and vice-versa. This converter is also helpful to generate P12 files for easy integration with Java applications supporting only the P12 format.

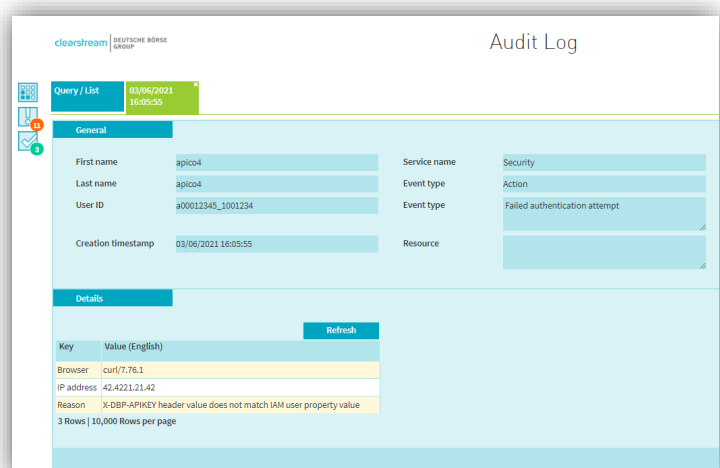
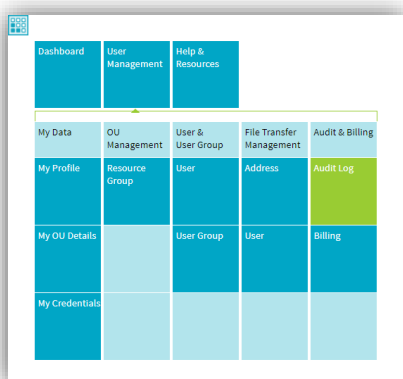


3) When requesting a bearer token (access_token), HTTP 4xx errors (client-errors) are returned

Please make sure your request goes through <https://api.clearstream.com> or the equivalent API portal for test environments. Any OAuth requests sent to <https://xact.clearstream.com> will be rejected.

When requesting a bearer token via <https://api.clearstream.com>, valid scopes must be specified. If invalid scopes are requested, then the bad request error response will contain a list of valid scopes. If this does not solve your issue, please continue with the next troubleshooting step.

If any of the other parameters in the token request is incorrect, a 403 Forbidden error is returned by the authorisation server. Details on what exactly has led to the error can be viewed in the audit log of the Xact OU. This feature is only available to granted Xact OU administrators.



4) Using curl I am unable to retrieve an access_token and I get SSL/TLS errors.

Certain older versions of curl are not supported by the Clearstream API infrastructure. Please try upgrading curl to a more recent version.

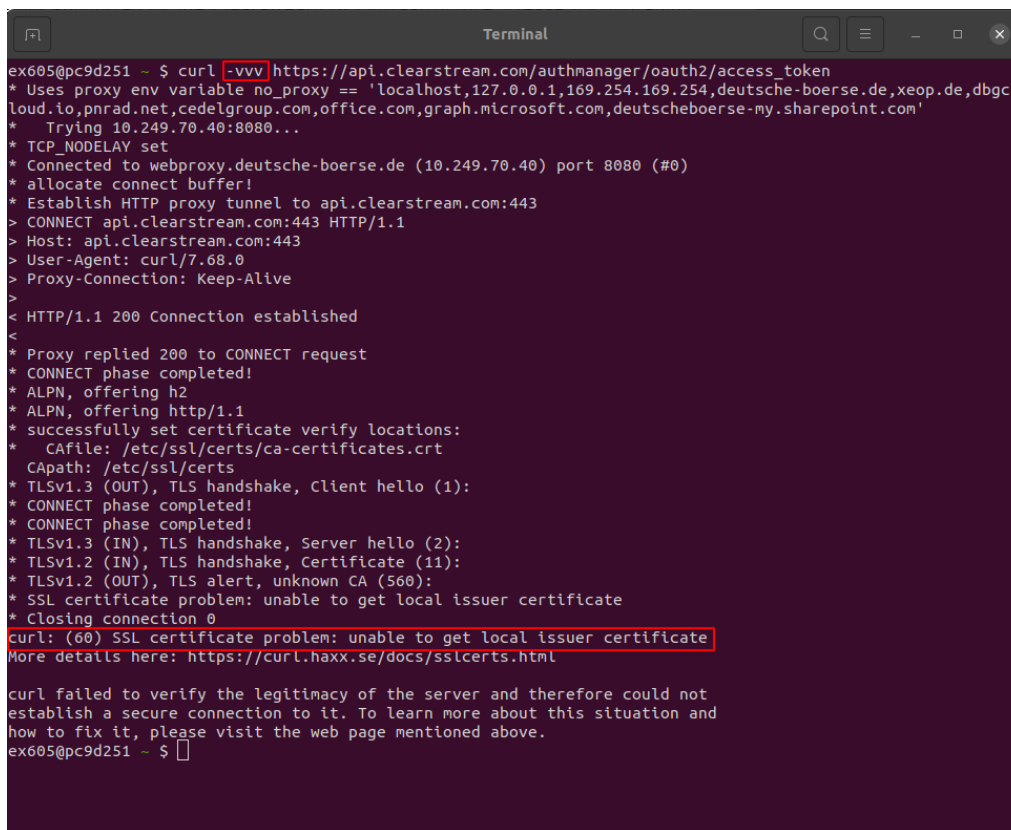
5) Mutual TLS is not part of the OAuth2.0 spec and is not supported by my library

The current OAuth2.0 specification does not deal with mutual TLS. If you need to use a specific library which does not support mutual TLS, and you are not able to modify the HTTP connection accordingly, then we recommend installing a proxy in between your client and our infrastructure. This proxy should then wrap the libraries one-way TLS into mutual TLS (two-way) before contacting the Clearstream API infrastructure.

6) How to troubleshoot and/or debug with curl commands

When using curl commands to troubleshoot or debug API connectivity issues it is important to use the verbose mode. In this mode additional debug information is provided which is often necessary to fully understand the underlying issue.

The **below invalid example** illustrates how a verbose curl command (-vvv option) shows a successful proxy connection followed by a SSL error caused by the fact that no client certificate was specified.



```
ex605@pc9d251 ~ $ curl -vvv https://api.clearstream.com/authmanager/oauth2/access_token
* Uses proxy env variable no_proxy == 'localhost,127.0.0.1,169.254.169.254,deutsche-boerse.de,xeop.de,dbgc
loud.io,pnrad.net,cedelgroup.com,office.com,graph.microsoft.com,deutscheboerse-my.sharepoint.com'
* Trying 10.249.70.40:8080...
* TCP_NODELAY set
* Connected to webproxy.deutsche-boerse.de (10.249.70.40) port 8080 (#0)
* allocate connect buffer!
* Establish HTTP proxy tunnel to api.clearstream.com:443
> CONNECT api.clearstream.com:443 HTTP/1.1
> Host: api.clearstream.com:443
> User-Agent: curl/7.68.0
> Proxy-Connection: Keep-Alive
>
< HTTP/1.1 200 Connection established
<
* Proxy replied 200 to CONNECT request
* CONNECT phase completed!
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: /etc/ssl/certs
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* CONNECT phase completed!
* CONNECT phase completed!
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS alert, unknown CA (560):
* SSL certificate problem: unable to get local issuer certificate
* Closing connection 0
curl: (60) SSL certificate problem: unable to get local issuer certificate
More details here: https://curl.haxx.se/docs/sslcerts.html

curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.
ex605@pc9d251 ~ $
```

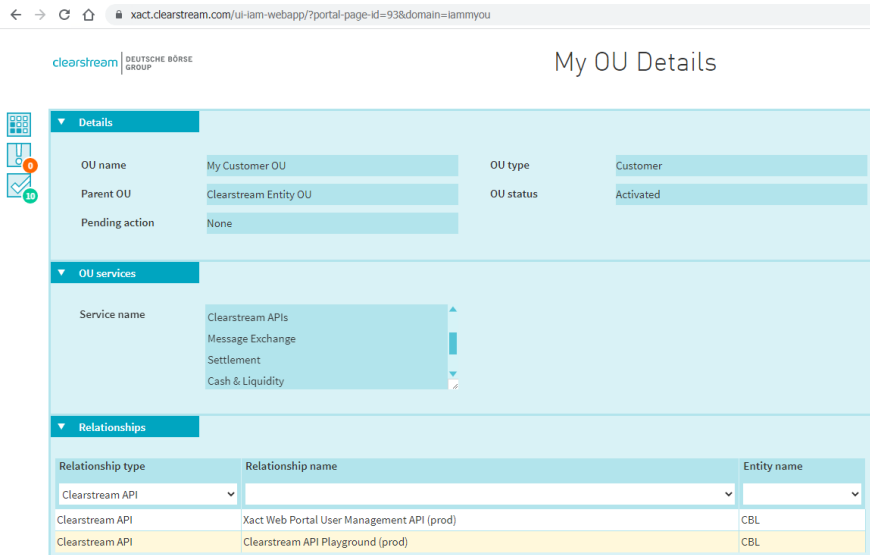
Please note that a **correct** working example including all required parameters would look like this:

```
curl
--cert ocapi-a000012345_00012345-ssl.pem
--cacert ocapi-a000012345_00012345-cacert.pem
--data "grant_type=password"
--data "scope=allow ocapi-playground-v1"
--data "username=a000012345_00012345"
--data "password=*****" https://api.clearstream.com/authmanager/oauth2/access_token
```

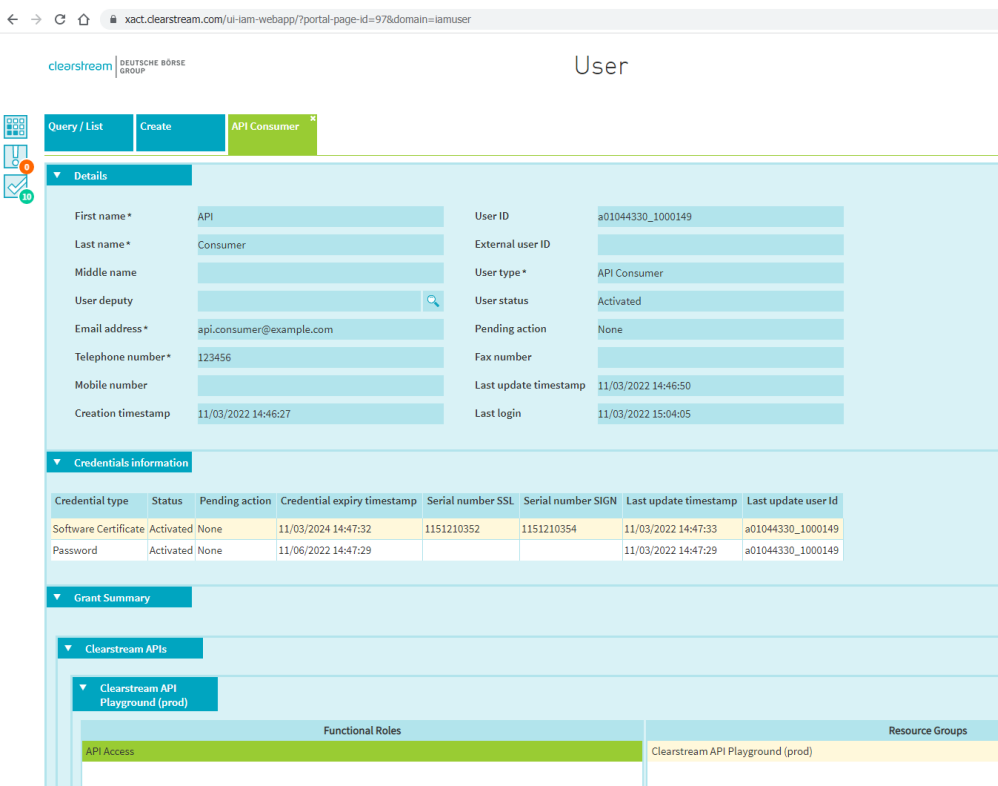
How to get development support from Clearstream?

If the above troubleshooting steps did not solve your issue and **before contacting** connect@clearstream.com for additional help, please run through the following checklist.

- 1) Visit “My OU Details” and check that the Clearstream API service is granted to your OU. Check that you have at least one Clearstream API resource linked in the Relationships of your OU.



- 2) Check that your API consumer user has valid credentials in Xact Web Portal. Check that at least one API resource such as the Clearstream API playground is assigned to the API Consumer user.



- 3) With the SSL key and certificate perform a curl command against https://api.clearstream.com/authmanager/oauth2/access_token to obtain an access token. In this curl command check that all required information is provided including the grant_type, scope, username and password. A complete example is available in the "Getting an OAuth2.0 Bearer Token (access_token)" section
- 4) With the SSL key and certificate perform a curl command against <https://api.clearstream.com/playground/v1/info> to ensure the obtained access token is working correctly.
- 5) With the SSL key and certificate perform a curl command against the Clearstream API you are trying to use. In case of errors please ensure that the correct scope was specified in step 3.

If the above checklist did not reveal the problem, please communicate at which step your issue occurs and additionally **you must provide the following debugging information:**

- Timestamps of when you encountered the issue
- The command history in case you execute curl or scripting commands (verbose mode – see troubleshooting section)
- Code snippets illustrating your API usage
- HTTP requests and responses send/receive to/from the Clearstream API platform

Example code

This section provides a scripting-based example for illustration purposes. Clearstream Banking does not take any responsibility in case of issues, problems or damages caused by the example code below.

Clearstream Banking encourages developers to always follow best practices and to perform regular penetration tests for any systems integrating with the Clearstream API platform.

Bash/curl

```
#!/usr/bin/env bash

# Script dependencies (tools you need to have installed to run this script
# 1) curl - recent version of curl (Old versions cause issues. E.g. 7.47.0 does not work)
# 2) jq - json parser for bash
echo " -----"
echo " -- Demo: Accessing the Clearstream API Playground with bash/curl --"
echo " -----"

# >>>> PRODUCTION <<<<
# ENVIRONMENT='https://api.clearstream.com'
# SSL_PEM='keystores/ocapi-a00012345_0012345-ssl.pem'
# CA_PEM='keystores/ocapi-a00012345_0012345-cacert.pem'
# USERNAME='a00012345_0012345'
# LOGIN_PASSWORD='*****'

# >>>> PRE-PRODUCTION (OCCT) <<<<
ENVIRONMENT='https://api-t2s-test.clearstream.com'
SSL_PEM='keystores/ocapi-stb2_01014172_1000000-ssl.pem'
CA_PEM='keystores/ocapi-stb2_01014172_1000000-cacert.pem'
USERNAME='stb2_01014172_1000000'
LOGIN_PASSWORD='*****'

# -----
echo "ENVIRONMENT=${ENVIRONMENT}"
echo "SSL_PEM=${SSL_PEM}"
echo "CA_PEM=${CA_PEM}"
echo "USERNAME=${USERNAME}"
echo "LOGIN_PASSWORD=${LOGIN_PASSWORD}"

echo $'\n>> 1) Request access token from authorization server'
ACCESS_TOKEN_RESP_CALL=$(curl \
  --cert ${SSL_PEM} \
  --cacert ${CA_PEM} \
  --data "grant_type=password" \
  --data "scope=allow ocapi-playground-v1" \
  --data "username=${USERNAME}" \
  --data "password=${LOGIN_PASSWORD}" \
  ${ENVIRONMENT}/authmanager/oauth2/access_token)

echo $'\n\n>> 2) Parse access token from response'
ACCESS_TOKEN=$(echo $ACCESS_TOKEN_RESP_CALL | jq -r .access_token)

# https://console.developer.deutsche-boerse.com/apis/9993a0e6-d53a-4bf9-94d4-73e4da49f6dd/technical-documentation
echo $'\n\n>> 3) Access Playground API with access_token'
curl \
  --cert ${SSL_PEM} \
  --cacert ${CA_PEM} \
  --header "Authorization: Bearer ${ACCESS_TOKEN}" \
  ${ENVIRONMENT}/playground/v1/echo?value=Hello%20World"

echo $'\n\n'
```