

# BlackLine SAP Core

## External API configuration

Valid from version 2102

**Prepared By:** BlackLine Support

**Release Date:** 2021-02-25

**Document Version:** 2.1

**DISCLAIMER.** The information in this document is for general guidance only. In no event will BlackLine or the partners or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information in this document.

**The contents of this document are confidential; for internal use by BlackLine customers, partners and staff only.**

## Contents

1.	Revision History .....	2
2.	Overview .....	3
3.	Process flow .....	3
4.	Message Flow .....	4
5.	Prerequisites .....	5
6.	Preparation .....	7
6.1	Setup API user.....	7
6.2	Get SSL certificate.....	8
7.	Setup .....	10
7.1	Logical File (optional) .....	10
7.2	Upload SSL Certificate .....	12
7.3	Create HTTP destinations.....	15
7.4	Generate API configuration.....	18
7.5	Individual maintenance .....	20
8.	Test .....	23
9.	Troubleshooting.....	25

## 1. Revision History

Version	Date	Writer/Editor	Description/Notes
1.0	15-05-2020	Arjan Aalbers	Initial for release EC2005.00.00 from SAP Technology group
1.1	17-08-2020	Guido Buitendijk	Removed Release version from the first page, and added the compatible Release S2009 to par.4
1.2	18-08-2020	Arjan Aalbers	Updates for Logical File and pre-req Firewall + DNS
1.3			Changes in par.6.3
2.0	19-01-2021	Arjan Aalbers	rewrite for EC2102 release
2.1	25-02-2021	Arjan Aalbers	Update certificate upload added currency rates api for v2105

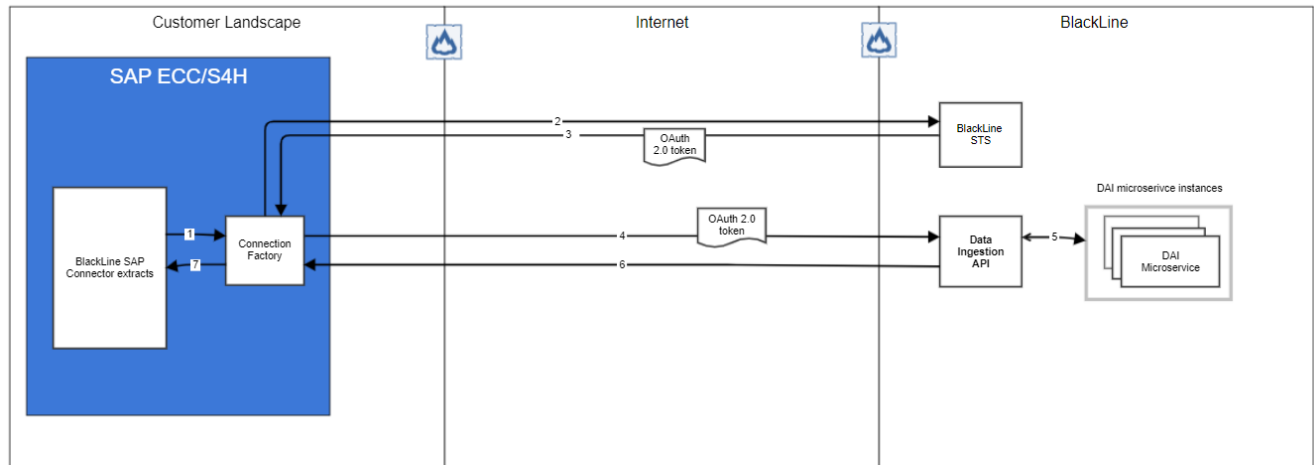
[Intentionally Left Blank]

## 2. Overview

This document explains how to setup the API access from the Customer SAP system to the BlackLine Cloud API's. It is meant for Implementation Consultants.

## 3. Process flow

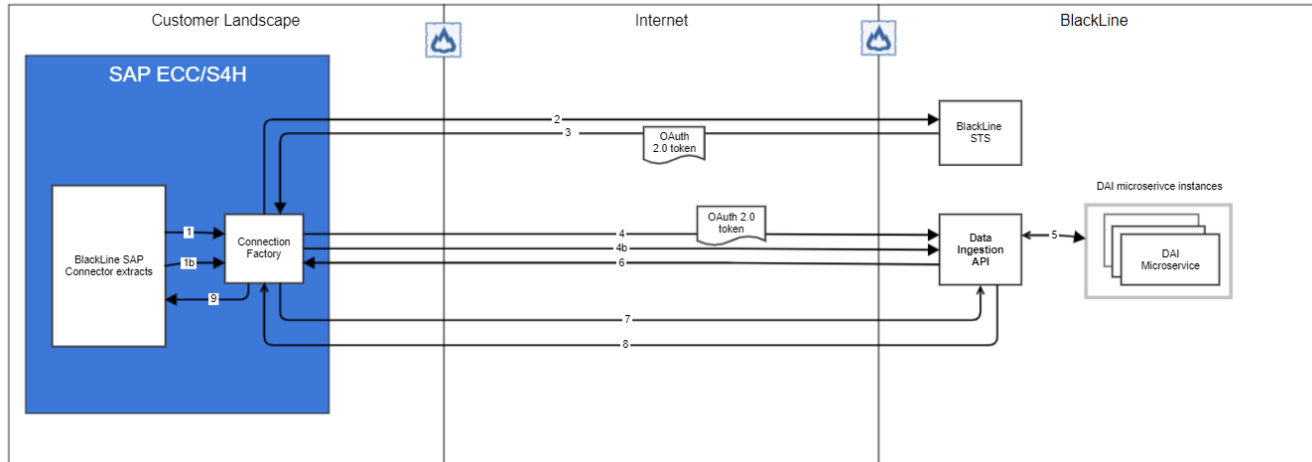
This process flow is from the SAP customer landscape point of view. The processing within BlackLine has been simplified.



Step	Description
1	The SAP Connector query the data and send result to the Connection factory
2	The connector presents API key to BlackLine STS to authenticate via HTTPS POST
3	BlackLine STS validates API key and returns an OAuth 2.0 token to the Connection Factory. This token is valid for the duration of the token's TTL (time-to-live) and can be used for subsequent communication with the BlackLine Data Ingestion API.
4	The Connection Factory executes an HTTPS POST/PUT/GET operation passing the OAuth 2.0 token inserted into the authorization header of the request.
5	The Data Ingestion API hands the payload over for processing. An ImportID is generated
6	The result HTTP 202 Accepted + ImportID is returned in the response
7	The Connection Factory reports the result to SAP Connector Extract program for logging

## 4. Message Flow

This process flow is from the SAP customer landscape point of view. The processing within BlackLine has been simplified.



Step	Description
1	The SAP Connector extract program queries the data in SAP and send result to the Connection factory
1b	For Open Items and Transactions, the body is split into chunks of 50 MB and multiple calls to the Connection Factory are made
2	With the First call the connector presents API key to BlackLine STS to authenticate via HTTPS POST
3	BlackLine STS validates API key and returns an OAuth 2.0 token to the Connection Factory. This token is reused for calls 4, 4b and 7. If the token expires in the meanwhile, a new token will be fetched
4	The Connection Factory executes an HTTPS POST/PUT/GET operation passing the OAuth 2.0 token inserted into the authorization header of the request.
4b	For the Transaction Matching API (Data source) multiple call must be made if the payload exceeds 50MB
5	The Data Ingestion API hands the payload over for processing. An ImportID is generated
6	The result HTTP 202 Accepted + ImportID is returned in the response
7	The Connection Factory queries the Status of the import via the Status API using the ImportID. If the returned status (8) = PENDING or SYSTEM INFORMATION , the connection factory waits for 2 seconds and tries again with a maximum of 10 tries.
8	The status API return the import status: SUCCESS, SUCCESSFULLY COMPLETED, DATA_ERROR, PENDING or SYSTEM INFORMATION
9	The import status is returned to the SAP Connector extract program

## 5. Prerequisites

- Check with the Network team or SAP Basis team in your organization that a Firewall must allow traffic from your SAP system to the BlackLine Instance on Port 443
- Check with the Network team or SAP Basis team in your organization that the target host (**{environment}.api.blackline.com**) can be resolved to an IP address from your SAP server. This might need a change to your DNS or host file configuration.
- SAP Connector version EC2005.00 or S2009.00 or higher is installed on the customer system.
- BLG version 2102 is installed on the customer system.
- An SAP user is available with SAP\_ALL or the following authorizations:
  - transaction SM59
  - transaction STRUSTSSO2
  - transaction /BLG/EC\_MAINT\_ECON
  - transaction FILE when the customer has a Runtime Database License or has a SolEx contract
- The BlackLine Implementation Consultant has provided for your BlackLine instance:
  - The API and Token endpoint URL
  - The Client ID (token server logon user)
  - The Client Secret (token server logon password)
  - The Client Guid

[Example on next page]

**From:** BlackLine - Do Not Reply <[donotreply@blackline.com](mailto:donotreply@blackline.com)>

**Date:** 8 May 2020 at 18:34:50 CEST

**To:** .....

**Subject:** Case # 00269443: API - Enable All API has been updated.

\*\*\* CASE UPDATE ALERT \*\*\*

Company: Blackline, Inc.  
Case: 00xxxxxx: API - Enable All API  
BlackLine Owner: .....

Case Comment: Hello,  
The reporting, task, dataingestion, and the matching API has been enabled to  
<https://xyz.us2.blackline.com>

Below are the connection information for Reporting, and Dataingestion.

Dataingestion is for dataingestion, matching, and task.  
Regards

.....

Reporting API info:

\*\*\*\*\*  
Environment = US2  
ClientID = my\_bl\_user  
Client Secret = 1Q3.6;!EsL#u  
Scope = ReportsAPI instance\_6610EFC3-2F5C-4E82-BB96-D8442CFA5946  
URL to request token = [https://my\\_bl.api.blackline.com/authorize/connect/token](https://my_bl.api.blackline.com/authorize/connect/token)  
\*\*\*\*\*

Dataingestion API Info:

\*\*\*\*\*  
Environment = US2  
ClientID = my\_bl\_user  
Client Secret = 1Q3.6;!EsL#u  
Scope = DataIngestionAPI instance\_BE772D9-890A-4710-96E10-3F6CEB98BB  
URL to request token = [https://my\\_bl.api.blackline.com/authorize/connect/token](https://my_bl.api.blackline.com/authorize/connect/token)  
\*\*\*\*\*

Click on the link to access the case: <https://blackline.my.salesforce.com/.....>

Sincerely, The BlackLine Support Team



The world's most trusted solution for Finance Controls and Automation.

## 6. Preparation

### 6.1 Setup API user

- Go to the user admin grid on your BlackLine instance and create an API user

- Note the Login ID (example api\_user)
- Generate the API key for that user and copy the Guid for later use

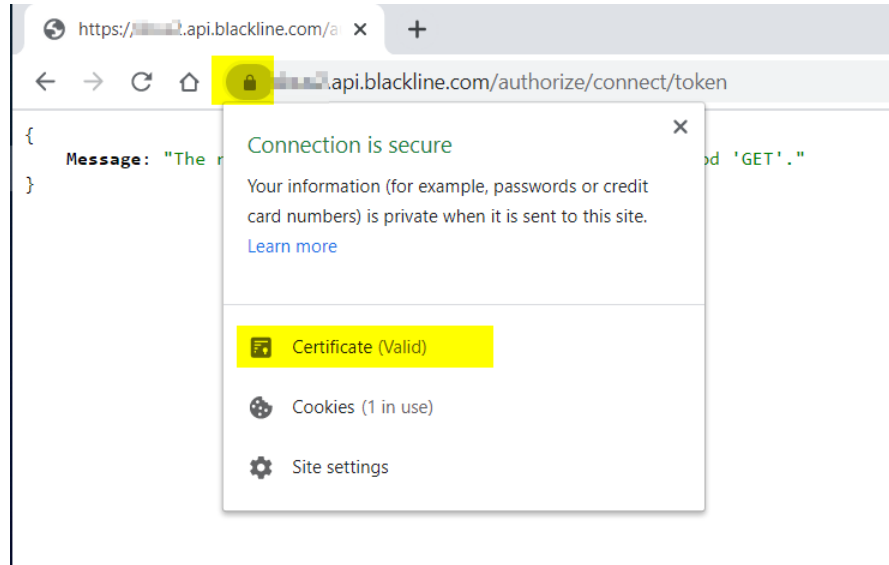
- Assign the correct API authorizations in Authorized Roles  
Apart from the API Access option also check the boxes for the domains in which this user must upload data

Authorized Roles										
Role	Account	Consolidations	Journal Document	Match	Task	Variance Analysis	Intercompany	Insights	Enhanced Reporting	Compliance
Preparer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Approver	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reviewer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Financial Reviewer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Account Reviewer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Financial Manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Account Manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Internal Auditor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Executive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CFO	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
External Auditor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Local Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Business Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Consultant	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
API Access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

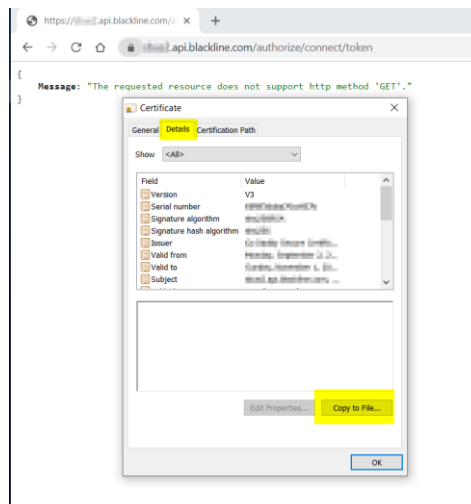
## 6.2 Get SSL certificate

*Note: It's recommended to use Chrome or Microsoft Edge for this step. The screenshots below are made with the Chrome browser.*

- The SSL client certificate of the BlackLine webserver must be installed on the SAP system. To obtain the certificate, open a browser and enter the token endpoint url (<https://{environment}.api.blackline.com/authorize/connect/token>)  
Or  
<https://{environment}.api.blackline.com/sts/diagnostics/status> ). (Applies to the new APIgee framework hosted on Google Cloud Platform GCP)  
Ignore the error message and click on the lock icon to see the certificate details.

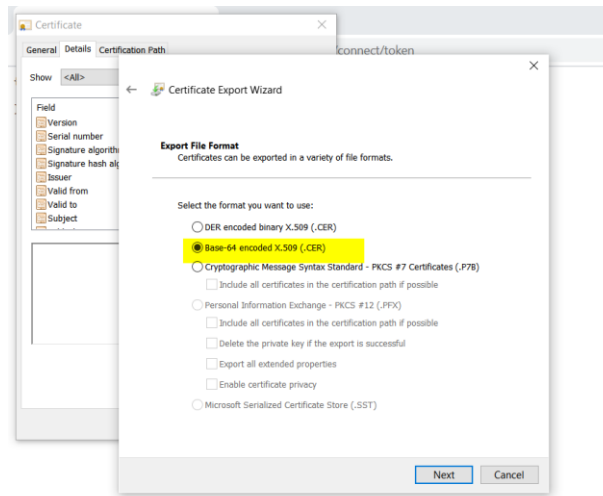


- Click on "Certificate (Valid)" to display the certificate details and switch to the "Details" tab

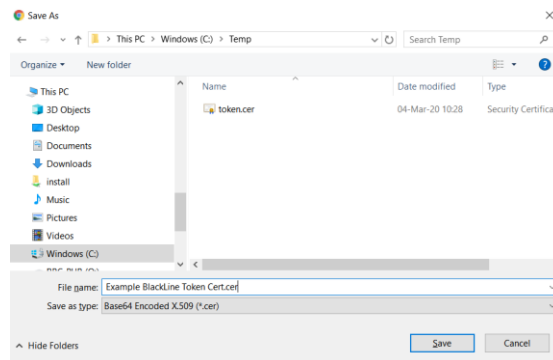




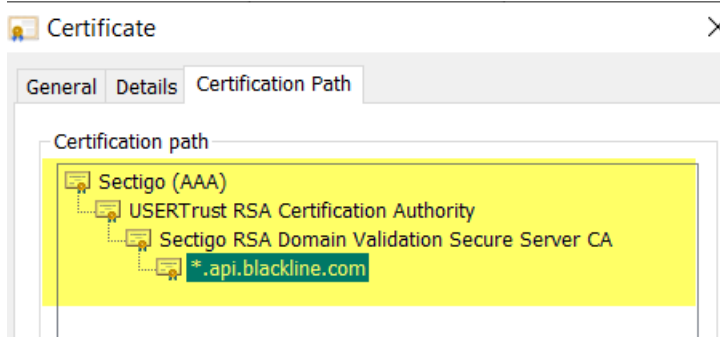
- Use the "Copy to File..." option to export the certificate as "Base-64 Encoded X.509 (.cer)"



- Save the file to your local PC for later use.



- Repeat this for the whole certificate chain.



In this example 4 certificates must be downloaded.

## 7. Setup

### 7.1 Logical File (optional)

In case of "Runtime Database License" the configuration is not stored in Database tables but in a configuration file on the SAP application server. For this the Logical File and Path must be configured. **For all other licenses, skip chapter 6.1.**

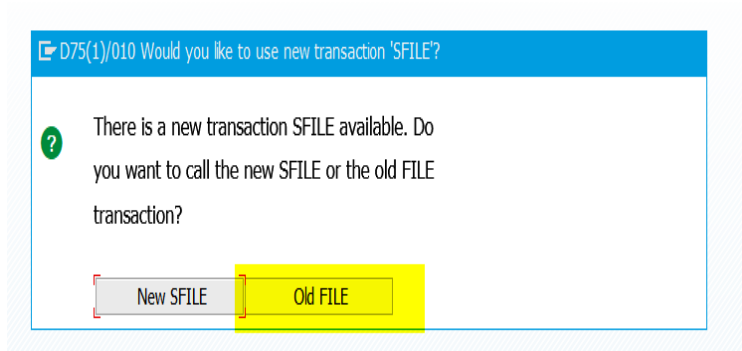
- Start transaction /BLG/EC\_MAINT\_ECON  
If you get an error message:

**"Logical file '/BLG/EC\_CON\_CONFIG\_FILE' p1 'ConfigHeader' validation failed. Please check trx FILE"**  
Or

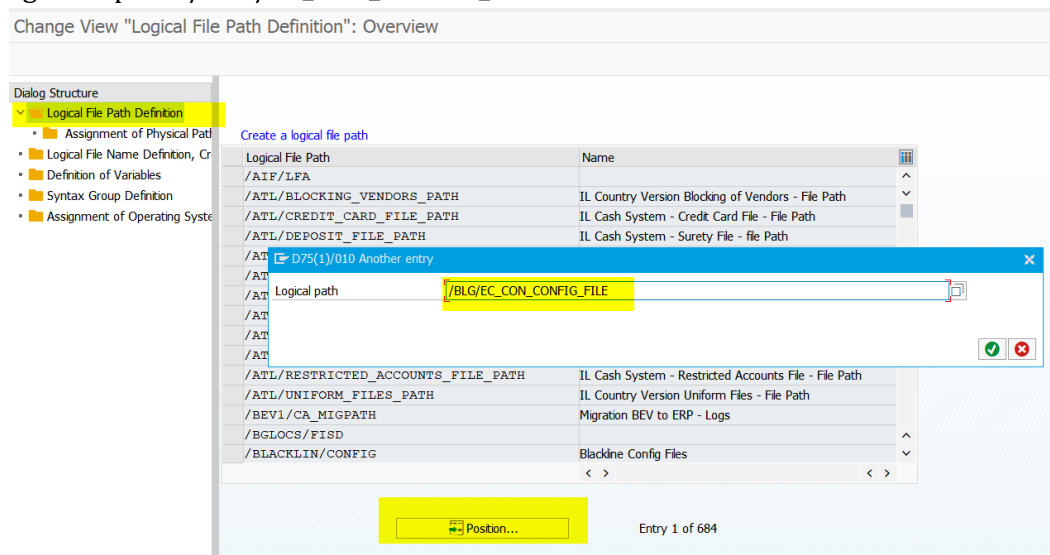
**"Please maintain logical path '/BLG/EC\_CON\_CONFIG\_FILE' for storage of config files"**

Then continue with the following, else **skip chapter 6.1**

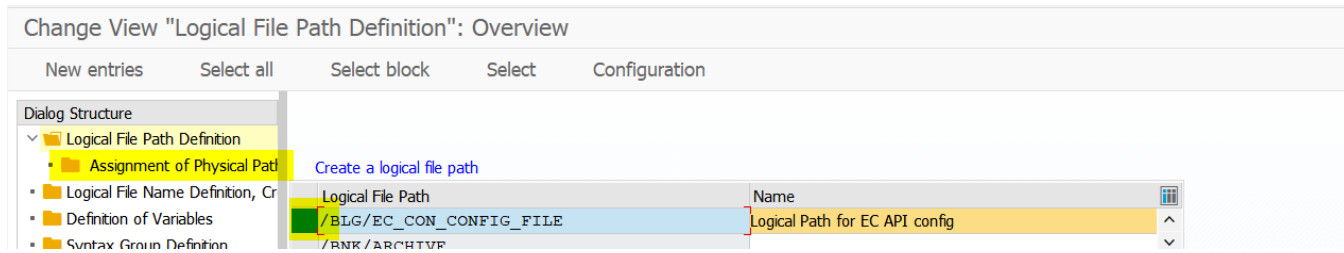
- Start transaction FILE
  - On newer SAP systems you might get the question to choose between the new SFILE and the old FILE transaction. Choose in this case for the Old FILE option.



- Select node "Logical File Path Definition" + position to navigate to path "/BLG/EC\_CON\_CONFIG\_FILE"

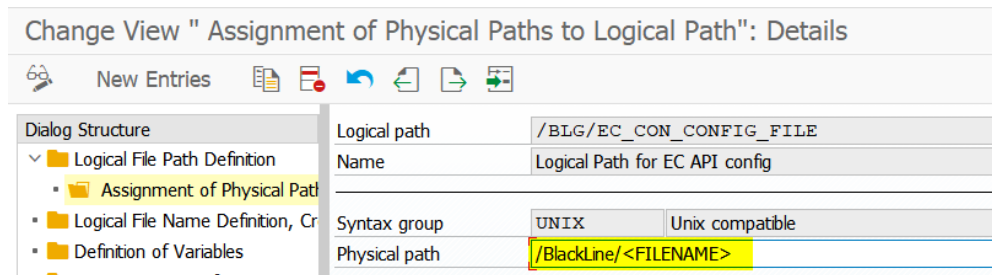


- Select the entry and create a new entry for "Assignment of Physical Paths to Logical Path".



- According to your OS (Windows, Unix,... ), choose a suitable folder and use "<FILENAME>" as the placeholder.

Example for Unix:



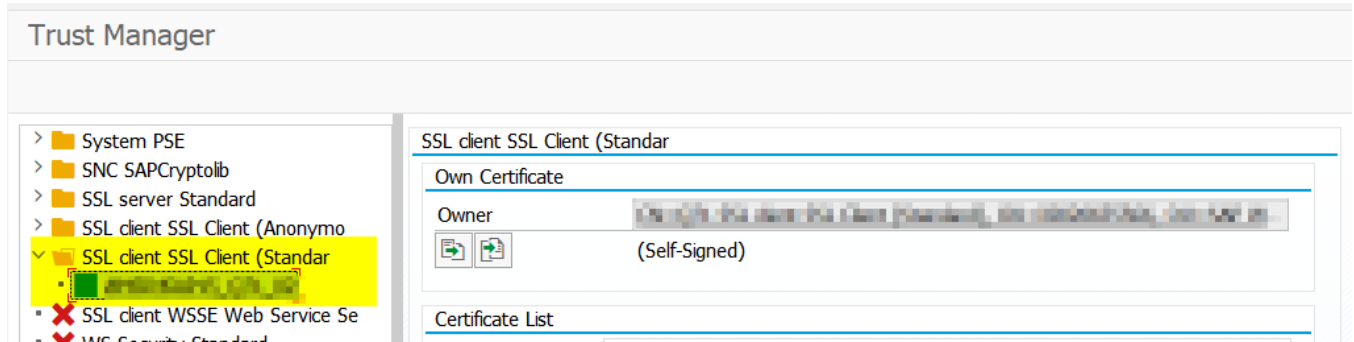
Picture 7-1

- Save your entry and assign a workbench request when prompted.

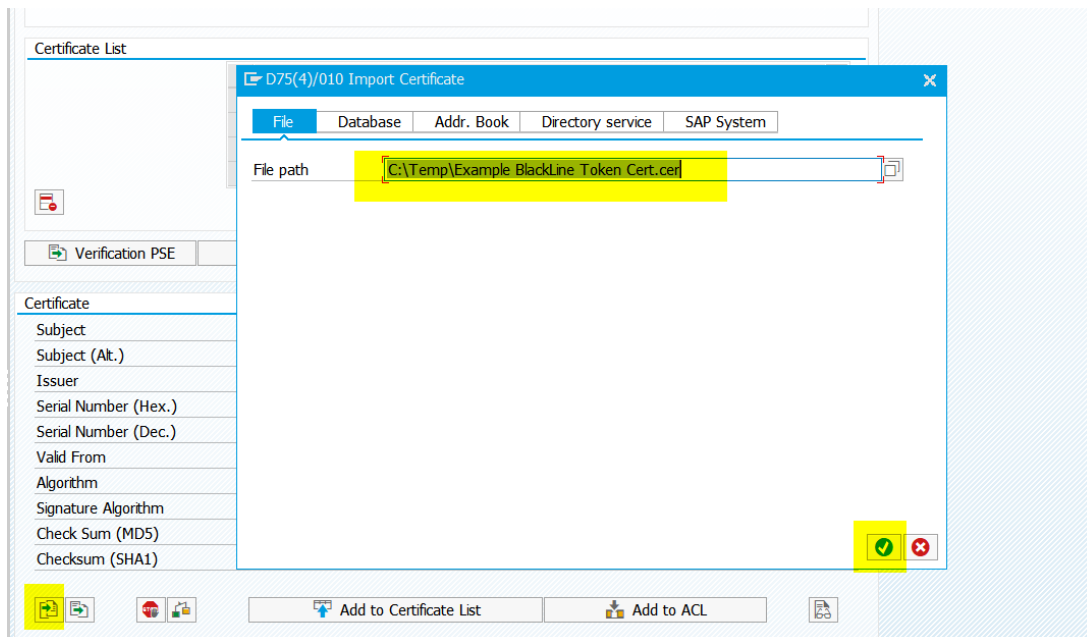
## 7.2 Upload SSL Certificate

For https traffic to the BlackLine API and Token endpoint the client certificate must be uploaded in SAP.

- Start transaction STRUST or STRUSTSSO2
- Switch to change mode when needed and open Folder "SSL client SSL Client (Standard)" and select your SAP instance  
(You can also use a custom defined PSE to store the Blackline Certificates)



- Use the import button to upload the .cer file downloaded in the Preparation step



Use the "add to Certificate List" to add the certificate to the list.

### Certificate List

Subject
<a href="#">CN=api.blackline.com, OU=Domain Control Validated</a>
<a href="#">CN=api.blackline.com, OU=Domain Control Validated</a>

Verification PSE
 Password

---

### Certificate

Subject	CN= <a href="#">api.blackline.com</a> , OU=Domain Control Validated		
Subject (Alt.)	dNSName= <a href="#">www.api.blackline.com</a> , dNSName= <a href="#">api.blackline.com</a>		
Issuer	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repositor...		
Serial Number (Hex.)	<a href="#">F0A F0A F0A F0A F0A F0A F0A F0A</a>		
Serial Number (Dec.)	<a href="#">17744812977777777777</a>		
Valid From	02.09.2019 13:02:26	to	01.11.2020 16:28:05
Algorithm	RSA	Key Strength	2048
Signature Algorithm	RSA+SHA256		
Check Sum (MD5)	<a href="#">6C B4 B5 D3 E1 C8 F5 B5 B5 B5 D3 E1 F4 B4 D3 E1</a>		
Checksum (SHA1)	<a href="#">E1 F5 B5 B5 C8 D3 E1 F5 B5 B5 B5 C8 D3 E1 F5 B5 B5</a>		

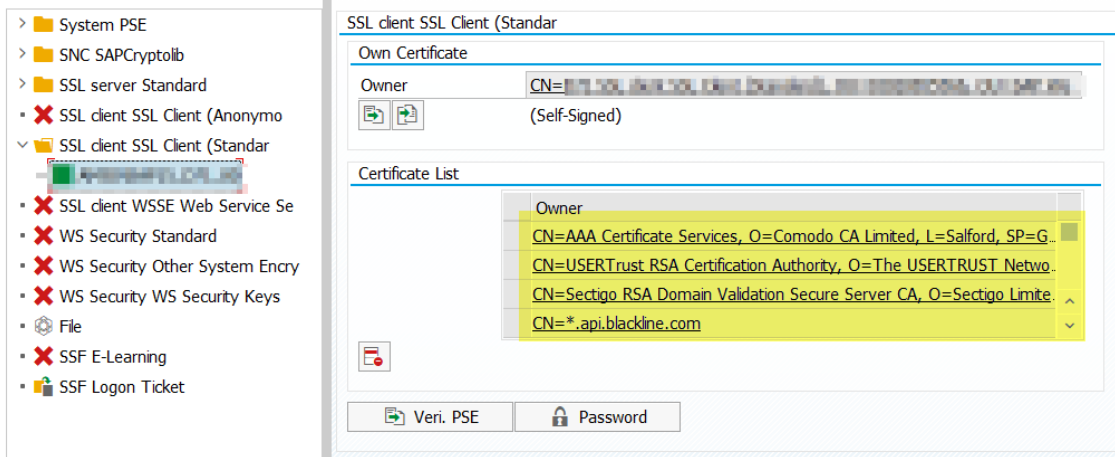
Add to Certificate List
 Add to ACL

- Save

The screenshot shows the 'Certificate List' window in Windows. The 'Own Certificate' tab is selected, displaying a single certificate. The 'Subject' field is highlighted in yellow and contains the text 'CN=api.blackline.com, OU=Domain Control Validated'. The 'Issuer' field is also highlighted in yellow and contains the text 'CN=api.blackline.com, OU=Domain Control Validated'. The 'Expiration Date' field is highlighted in yellow and contains the text '12/31/2024'. The 'Issued On' field is highlighted in yellow and contains the text '12/31/2024'. The 'Trust issuer certificates' checkbox is unchecked. The 'Certificate List' tab is also visible, showing a list of certificates. The 'Verification PSE' and 'Password' buttons are at the bottom.

- Repeat the upload for the other certificates in the chain.  
In this example 4 certificates in total are added to the certificate list

#### Trust Manager



## 7.3 Create HTTP destinations

Use transaction SM59 to create 2 HTTP destinations:

### 7.3.1 HTTP Destination for OAUTH

- Enter a name for the HTTP destination. For example: BL\_OAUTH\_[PROD/SANDB/TEST/...]  
Choose type = G
- Enter a description (1) and press enter

Ignore the message “HTTP connections may not be secure”

RFC Destination BL\_OAUTH\_PROD

Connection Test

RFC Destination: BL\_OAUTH\_PROD

Connection Type: G HTTP Connection to External Serv

Description: Prod: Get Oauth tokens for Blackline API's

- From the Url to request token copy the hostname (without https:// or suffixes) into Target Host
- Leave the Service No. empty
- Enter rest of the url into the field Path Prefix

Administration Technical Settings Logon & Security Special Options

Target System Settings

Target Host: my\_bl.api.blackline.com

Service No.:

Path Prefix: /authorize/connect/token

- Switch to the Logon and Security Tab
- Switch to Basic Authentication
- Use the ClientID provide in the email for User
- Use Client Secret provide in the email as Password

Administration Technical Settings Logon & Security Special Options

Logon Procedure

Logon with User

☐ Do Not Use a User

☒ Basic Authentication

User: my\_bl\_user

PW Status: changed

Password: \*\*\*\*\*

- Set SSL to active and select the Certificate list containing the uploaded BlackLine Certificates - DFAULT SSL Client (Standard)

The screenshot shows the 'Security Options' configuration window. It has a title bar 'Security Options' and a sub-header 'Status of Secure Protocol'. Below this, there are two radio buttons: 'Inactive' and 'Active', with 'Active' selected. To the right of the radio buttons is a dropdown menu labeled 'SSL Certificate' with the value 'DFAULT SSL Client (Standard)' and a 'Cert. List' button. Below this is a section titled 'Authorization for Destination' with an empty text input field.

- Switch to the Special Options Tab
- Set HTTP 1.1 active
- Set Compression to Active(depends on Mime Type)
- Set Compressed response to Yes
- Set Accept Cookies to Yes (All)
- SAVE the HTTP destination

The screenshot shows the 'Special Options' configuration window. It has a title bar 'Special Options' and a sub-header 'HTTP Setting'. Below this, there are three sections: 'Status of HTTP Version' with radio buttons for 'HTTP 1.0' and 'HTTP 1.1' (selected); 'Compression Status' with radio buttons for 'Inactive', 'Active (Depends on MIME Type)' (selected), and 'Active (Whole Document)'; and 'Status of Compressed Response' with radio buttons for 'Yes' (selected) and 'No'. Below these is a section titled 'HTTP Cookies' with a sub-header 'Type of Cookies Acceptance'. It contains a radio button for 'Accept Cookies' with options 'No', 'Yes (All)' (selected), 'Input Prompt', and 'Trigger Event'.



## 7.3.2 HTTP Destination for API

- Enter a name for the HTTP destination. For example: BL\_API\_[PROD/SANDB/TEST/...]
- Choose type = G
- Enter a description (1) and press enter  
Ignore the message "HTTP connections may not be secure"
- From the Url to request token copy the hostname (without https:// or suffixes) into Target Host
- Leave the Service No. empty
- Leave Path Prefix **empty**

**RFC Destination**

Connection Test

RFC Destination: BL\_API\_PROD

Connection Type: G HTTP Connection to External Serv

Description: Prod: Blackline API's

Target System Settings

Target Host: my\_bl.api.blackline.com

Service No.:

Path Prefix:

- Switch to the Logon and Security tab
- Choose logon – Do not use a User
- Set SSL to active and select the Certificate list containing the uploaded BlackLine Certificates - DFAULT SSL Client (Standard)

Administration Technical Settings **Logon & Security** Special Options

Logon Procedure

Logon with User

☒ Do Not Use a User

☐ Basic Authentication

User:

PW Status: is initial

Logon with Ticket

☒ Do Not Send Logon Ticket

☐ Send Logon Ticket Without Ref. to a Target System

☐ Send Assertion Ticket for Dedicated Target System

System ID: Client:

Security Options

Status of Secure Protocol

SSL: ☐ Inactive ☒ Active

SSL Certificate: DFAULT SSL Client (Standard) Cert. List

- Switch to the Special Options Tab
- Set HTTP 1.1 active
- Set Compression to **InActive**
- Set Compressed response to Yes
- Set Accept Cookies to Yes (All)
- SAVE the HTTP destination

The screenshot shows the 'Special Options' tab in the SAP Connector configuration interface. It contains three main sections: 'HTTP Setting', 'Compression Status', and 'HTTP Cookies'. In the 'HTTP Setting' section, 'HTTP Version' is set to 'HTTP 1.1'. In the 'Compression Status' section, 'Compression' is set to 'Inactive'. In the 'HTTP Cookies' section, 'Accept Cookies' is set to 'Yes (All)'.

## 7.4 Generate API configuration

- Start transaction /BLG/EC\_MAINT\_ECON and switch to change mode
- Use "Generate all API config" to start the wizard
- Choose Data Ingestion Wizard in the popup, leave "With OAuth 2.0 support" checked.

The screenshot shows the 'Generate all API config' wizard in the SAP Connector configuration interface. The wizard is titled 'D75(1)/010 Select the wizard'. It has two options: 'Data Ingestion wizard' (selected) and 'Journals Documents wizard'. The 'With OAuth 2.0 support' checkbox is checked. The wizard is displayed over a background showing the 'API Configuration' table and the 'New Configuration' button.

Enter a Prefix to generate unique names

- Choose the HTTP destination for API create before (6.3.2)
- Choose the HTTP destination for Oauth token created before (6.3.1)
- Enter the user created in the user admin grid
- Enter the generated API key from the user admin grid
- Enter the API Scope provided in the Email

D75(1)/010 Wizard: Generate all API configuration entries

\*\*\*\*\* This wizard will generate the API configuration \*\*\*\*\*

Enter a prefix to ensure unique names.  
(De)Select the API's from the list below

Prefix:

HTTP Conn. API:

HTTP Conn. OAUTH:

User Name:

API key:

API Scope:

Checkbox	Logical Name	Ext API	Ext Service Type	API type	Description
<input type="checkbox"/>	<Prefix>_BL_DAI_CRR		API	BL_DAI_CRR	BlackLine DAI Currency Rates

- Select all the API's needed for your integration with BlackLine

D75(1)/010 Wizard: Generate all API configuration entries

\*\*\*\*\* This wizard will generate the API configuration \*\*\*\*\*

Enter a prefix to ensure unique names.  
(De)Select the API's from the list below

Prefix:

HTTP Conn. API:

HTTP Conn. OAUTH:

User Name:

API key:

API Scope:

Checkbox	Logical Name	Ext API	Ext Service Type	API type	Description
<input type="checkbox"/>	<Prefix>_BL_DAI_CRR		API	BL_DAI_CRR	BlackLine DAI Currency Rates
<input checked="" type="checkbox"/>	<Prefix>_BL_DAI_DS		API	BL_DAI_DS	BlackLine DAI Data Sources
<input type="checkbox"/>	<Prefix>_BL_DAI_ERR		API	BL_DAI_ERR	BlackLine Retrieve import status errors
<input checked="" type="checkbox"/>	<Prefix>_BL_DAI_GL		API	BL_DAI_GL	BlackLine DAI Accounts
<input type="checkbox"/>	<Prefix>_BL_DAI_ITM		API	BL_DAI_ITM	BlackLine DAI Items
<input checked="" type="checkbox"/>	<Prefix>_BL_DAI_MCB		API	BL_DAI_MCB	BlackLine DAI Multi Currency Balances
<input checked="" type="checkbox"/>	<Prefix>_BL_DAI_SBL		API	BL_DAI_SBL	BlackLine DAI Subledger
<input checked="" type="checkbox"/>	<Prefix>_BL_DAI_STS		API	BL_DAI_STS	BlackLine DAI Status
<input type="checkbox"/>	<Prefix>_BL_DAI_TAC		API	BL_DAI_TAC	BlackLine DAI Tasks Auto Certify
<input type="checkbox"/>	<Prefix>_BL_DAI_TDP		API	BL_DAI_TDP	BlackLine DAI Tasks dependencies
<input type="checkbox"/>	<Prefix>_BL_DAI_TSK		API	BL_DAI_TSK	BlackLine DAI Tasks
<input type="checkbox"/>	<Prefix>_BL_DAI_TUD		API	BL_DAI_TUD	BlackLine DAI Tasks update description
<input checked="" type="checkbox"/>	<Prefix>_BL_DAI_OAUTH_TOKEN	OAuth_TOKEN			BlackLine DAI OAuth Token

- Recommended selection is:
  - BL\_DAI\_DS BlackLine DAI Data Sources
  - BL\_DAI\_GL BlackLine DAI Accounts
  - BL\_DAI\_MCB BlackLine DAI Multi Currency Balances
  - BL\_DAI\_SBL BlackLine DAI Subledger
  - BL\_DAI\_STS Blackline DAI Status
  - BL\_DAI\_CRR Blackline DAI Currency Rates (for version v2105 and higher)
- Note: The API's *BlackLine DAI Status* and *BlackLine DAI OAuth Token* will always be generated, regardless of the checkbox.

The result should look like this:

Change: Overview of External Connections

Display/Change Upload Client SSL Certificate Generate all API config

API Configuration

Chan...	Delete	T...	Logical Name	Ext API	Ext Srv ...	API type	Description
			PROD_BL_DAI_DS	API	BL_DAI_DS	BlackLine DAI Data Sources - API Configuration for server: xxxx	
			PROD_BL_DAI_GL	API	BL_DAI_GL	BlackLine DAI Accounts - API Configuration for server: xxxx	
			PROD_BL_DAI_MCB	API	BL_DAI_MCB	BlackLine DAI Multi currency balances - API Configuration for server: xxxx	
			PROD_BL_DAI_SBL	API	BL_DAI_SBL	BlackLine DAI Subledgers - API Configuration for server: xxxx	
			PROD_BL_DAI_STS	API	BL_DAI_STS	BlackLine DAI status query - API Configuration for server: xxxx	

OAuth Token Configuration

Chan...	Delete	Logical Name	Ext API	Ext Service Type	Description
		PROD_BL_DAI_OAUTH_TOKEN		OAUTH_TOKEN	BlackLine OAuth Configuration for server: xxxx

## 7.5 Individual maintenance

The wizard is convenient to generate all configuration in a single step.

You can also view, edit and create individual API – or Authentication configuration

### Example 1: manual creation of an API configuration

- On the main screen (in change mode) choose “new configuration”

Change: Overview of External Connections

Display/Change Upload Client SSL Certificate Generate all API config

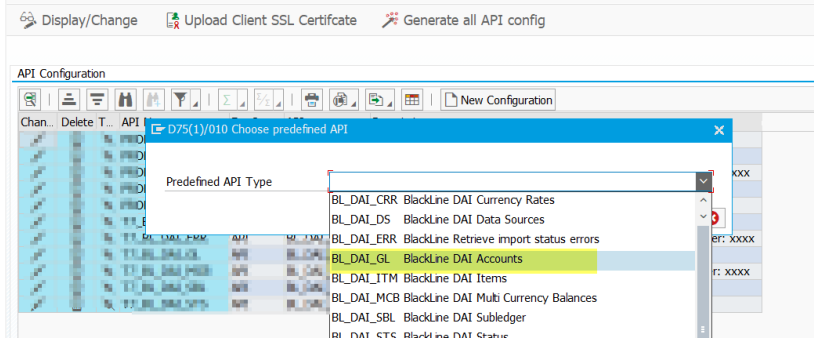
API Configuration

New Configuration

New

Chan...	Delete	T...	API Name	Ext Srv ...	API type	Description
			PROD_BL_DAI_DS	API	BL_DAI_DS	BlackLine DAI Data Sources - API Configuration for server: xxxx
			PROD_BL_DAI_GL	API	BL_DAI_GL	BlackLine DAI Accounts - API Configuration for server: xxxx
			PROD_BL_DAI_MCB	API	BL_DAI_MCB	BlackLine DAI Multi currency balances - API Configuration for server: xxxx
			PROD_BL_DAI_SBL	API	BL_DAI_SBL	BlackLine DAI Subledgers - API Configuration for server: xxxx
			PROD_BL_DAI_STS	API	BL_DAI_STS	BlackLine DAI status query - API Configuration for server: xxxx
			TT_BL_DAI_DS	API	BL_DAI_DS	BlackLine DAI Data Sources - API Configuration for server: xxxx

- Choose the predefined API Type in type popup ( in this example “Accounts” )



- API Detail Screen

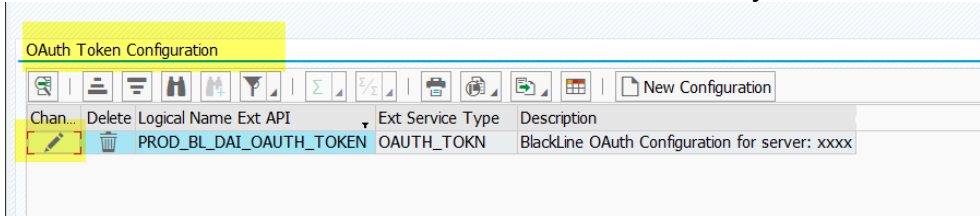
The screenshot shows the 'Maintain API Configuration' screen. It includes sections for 'Header', 'Connection details', 'OAuth Details', and 'API Import Status'. Numbered callouts (1-13) point to specific fields and actions: 1. Logical Name Ext API, 2. Description, 3. HTTP Connection, 4. URL Path, 5. Http Method, 6. Content type, 7. Auth. Method, 8. API Scope, 9. API Response is Binary, 10. OAuth Configuration, 11. Import Status API, 12. Check Configuration, and 13. Save/Cancel button.

- Configuration name
  - Fill out with a logical name
- Description
  - Add a meaning full description
- Http Connection
  - choose the connection configured in step 7.3.2
- Path – endpoint of the API
- Method used to call the API
- Content type
- Authentication method
- API Scope
  - Fill out the correct Guid provided to you
- Response is Binary
- OAuth Configuration
  - Select the OAuth configuration
- Import Status API
  - Select the API to retrieve the Job status
- Check configuration
  - Checks if all the mandatory fields are filled
- Save/Cancel

## Example 2: Changing the OAuth configuration

You can change the OAuth configuration, when for example the API key has expired and needs to be regenerated and must be updated in SAP.

1. On the main screen select the edit button for the OAuth entry



2. The fields on the Details screen

Maintain OAUTH Token Configuration

Check Configuration Show Passwords

Header

Token Name	PROD_BI_DAI_OAUTH_TOKEN
Description	BlackLine OAuth Configuration for server: Prod (Demo)

Connection details

HTTP Connection BL\_OAUTH\_PROD Display Connection

Host Name t7.api.blackline.corp

URL Path /authorize/connect/token

Http Method POST

OAuth Grant Type password

User Name api\_user

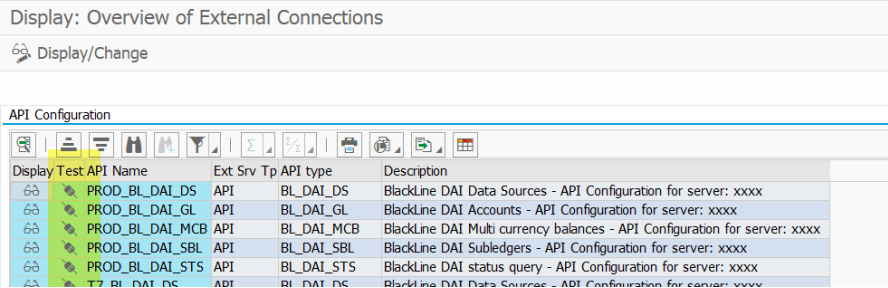
API key 6acb096cbdb2df3e8986484f6b0ba189

1. Configuration name
2. Description
3. HTTP destination configured in step 7.3.1
4. Method used to call the Token Service
5. Type of Grant
6. Logon id of the user created in the user admin grid (See chapter 6.1)
7. API key (re-)generated in the user admin grid
8. Hide/Show API key
9. Check configuration - Checks if all the mandatory fields are filled
10. Save/Cancel

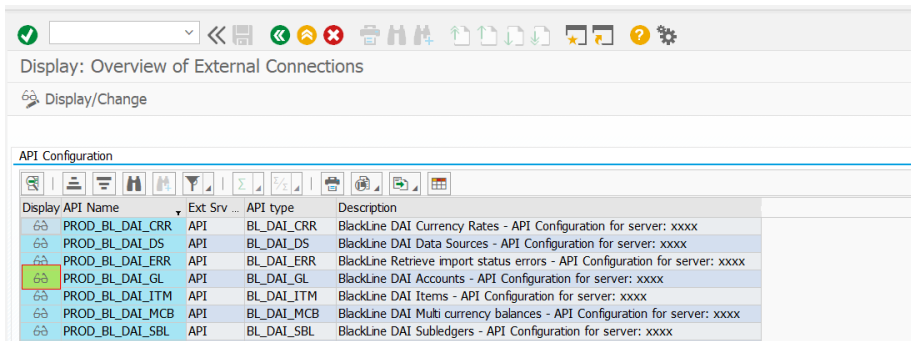
## 8. Test

After generating the API configuration, you can test if connection to API's end point works.  
The connection test works from the main screen or in display mode from the API detail screen

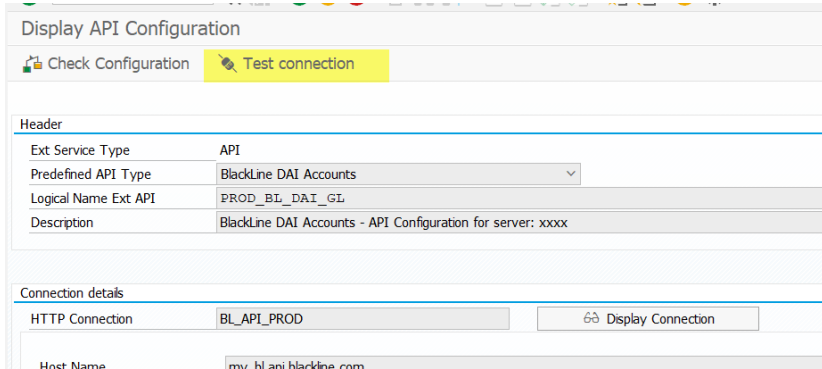
- Main Screen:



- Or Open one of the API detail screen by pressing the display icon



- Use the “Test Connection button”



- The test will call first the OAuth service to get a token  
Secondly a call is made to the API using invalid data. This prevents that actual postings are made via the API's  
An error message "invalid\_format" can be expected.

Service Call Logging	
Technical Information          Help	
Overview	Nu...
Start Testing API with invalid format	1
*****	1
- HTTP connection : BL_TOKEN_...	1
- Host : api.blacklinecorp	1
- Path : /authorize/connect/token	1
- User : D73API	1
- API key : 0608...	1
- Scope : DataIngestionAPI instance_BEA772D9-890A-4710-9...	1
- Getting Configuration for API BL_DAI_GL	1
- Getting Configuration for oauth BL_DAI_OAUTH_TOKEN	1
- Getting OAUTH Token	1
- OAuth Token Received	1
- HTTP connection : BL_API_...	1
- Host : api.blacklinecorp	1
- Path : /dataingestion/accounts?message-version=5	1
- Authorization : Bearer 527335de3a59e...	1
- Calling Service BL_DAI_GL	1
- error : invalid_format	1
- Response: 400 Bad Request	1
- {"error":"invalid_format"}	1
*****	1
- Response {"error":"invalid_format"} is expected. Connected	1

- Some API's use import parameters in the URL. In a popup you can enter a value for this parameter

Display API Configuration
 

Check Configuration
 Test connection

Header
 

Ext Service Type	API
Predefined API Type	BlackLine DAI Status
Logical Name Ext API	BL_DAI_STS
Description	BlackLine DAI status query - API Configuration for server: xxxx

Connection details
 

HTTP Connection	BL_API_...	Display Connection
Host Name	api.blacklinecorp	
URL Path	/dataingestion/status/<import_id>	
Http Method	GET	

API
 

BlackLine DAI Status
 

D75(2)/010 Fill in the URL parameters
 

Parameter 1	import_id	Value 1	10
Parameter 2		Value 2	



## 9. Troubleshooting

Common errors:

- SSL error- Most Likely an uploaded certificate has expired.
  - Please check STRUSTSS02 for the validity of the BlackLine certificates
- Failed to get OAUTH Token: 400 Bad Request - invalid grant - Authentication failed.  
The API key has expired or entered incorrectly into the SAP OAUTH configuration
  - Generate a new key in the BlackLine user admin grid and copy into the SAP OAUTH configuration
  - Make sure the user can also do has the roles to upload the data in the specific domain

Potential error codes:

Status Code	Error Code	Description
400	invalid client	SM59 -> Token service destination -> password(client secret) invalid
400	invalid grant + authentication failed	API key is invalid. Go to BLC user admin grid and regenerate new key or username is invalid
400	invalid grant	- grant_type must be "password" - API key not valid/has expired
400	invalid scope	check scope is correct filled in the API configuration
400	version_required	User has not supplied an import version
400	version_not_supported	The version supplied by the user is not supported
400	no_data	User has not supplied any data for import
400	invalid_format	The data was send is in the wrong format.
401	unauthorized	The token request was send with wrong credentials
401	unauthorized	Authentication failed due to invalid authentication credentials
403	Forbidden	Authorization failed due to insufficient permissions The user in the BlackLine Cloud instance has insufficient API authorizations
404	Not Found	Check host/url/path in SM59 destination
405	method not allowed	Check API uses POST or PUT
429		User has made more requests per second than the allowed threshold
500	Internal Server error	Server has encountered an internal error and cannot complete the request.
500	Native SSL error	The TLS version on older ABAP systems might be too low. Use tls 1.2
500	SSL Peer Certificate untrusted	Check STRUSTSS02 if the BlackLine Certificates are uploaded correctly and still valid
503	Service Unavailable	The web server is currently unavailable