



PUBLIC

SAP Business Network for Logistics Integration Suite Configurations

Table of Contents

1	Overview.....	3
2	Integration Package - SAP Business Network for Logistics Connectivity-Integration Suite Configuration...	4
3	How to import SAP BN4L Connectivity: Integration Suite configuration	5
4	Setup Inbound Connection to SAP LBN	6
	4.1 Setup connection between backend and your SAP Cloud Integration	6
	4.1.1 Configurations in your backend SAP system	6
	4.1.2 Configurations in your SAP Cloud Integration	6
	4.2 Setup connection between your SAP Cloud Integration and SAP LBN	10
	4.2.1 Configurations in your SAP Cloud Integration	10
	4.2.2 Configurations in your SAP LBN	11
	4.3 Configure 'Inbound to Network' iflow from the Package	12
5	Setup Outbound Connection from LBN to your CPI.....	13
	5.1 Setup connection between SAP LBN and your SAP Cloud Integration	13
	5.1.1 Configurations in LBN	13
	5.2 Setup connection between your SAP Cloud Integration and your backend SAP system.....	15
	5.2.1 Capturing destination detail in value mapping artifact	15
	5.2.2 Configure 'Outbound from Network' iflow from the package	16
6	Note.....	17

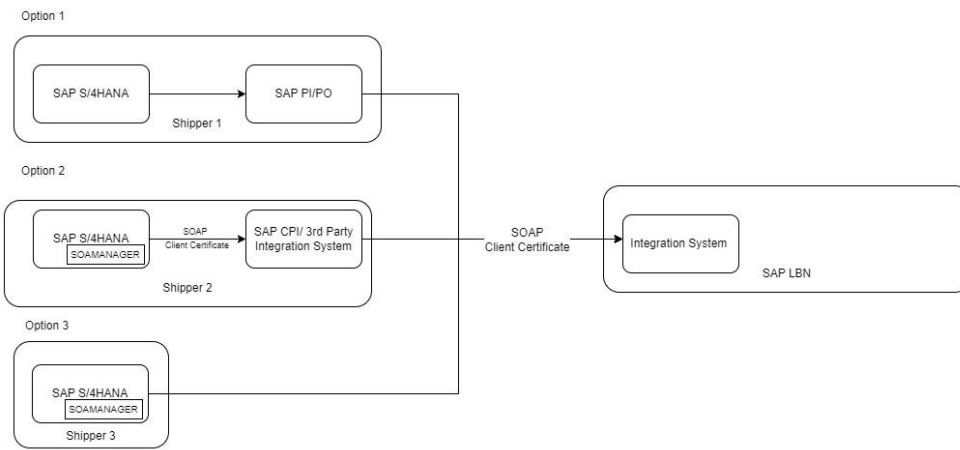
There are multiple ways to achieve connectivity between SAP Business Network for Logistics and customer's backend SAP system. One such way is using SAP Cloud Integration, provided customer has a valid license. To do so, certain integration artifacts need to be developed that enables connectivity and routing of messages between your backend system and SAP Business Network for Logistics (LBN). To make this easier, a standard integration package is made available to customers.

The SAP Business Network for Logistics Connectivity Integration Suite facilitates integration between SAP S/4Hana system or TM systems and the Logistics Business Network (LBN) through SAP Cloud Integration. It offers two pre-configured integration flows for Inbound to Network and Outbound from Network scenarios. This package can be imported into the tenant for configuring certificates, routing, logging, and authentication, ensuring streamlined logistics connectivity.

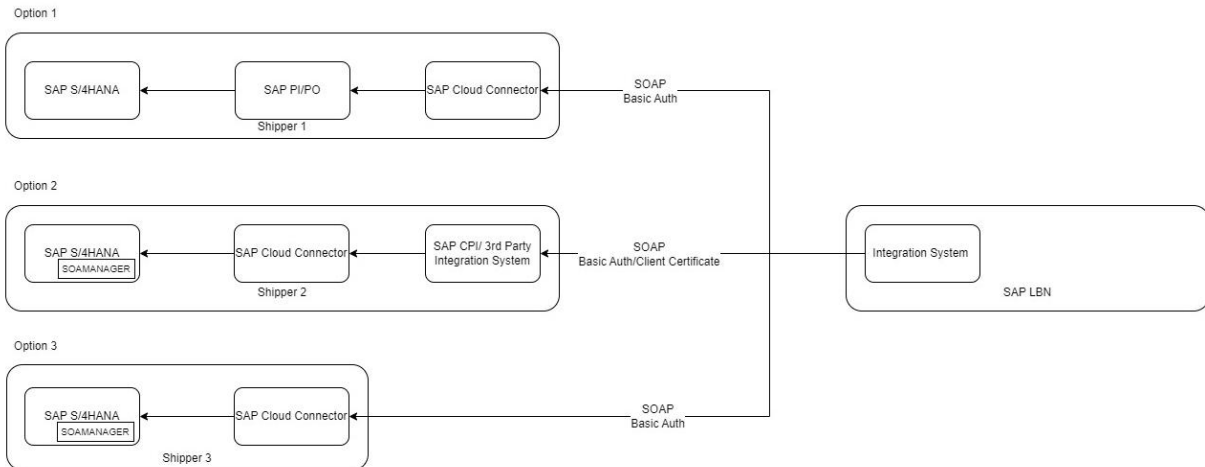
1 Overview

The following diagram depicts the various integration possibilities between SAP LBN and customer's backend system for inbound and outbound communications.

Inbound to SAP LBN



Outbound from SAP LBN



- **Option 1** - SAP Process Integration /Process Orchestration as an intermediary system between LBN and the customer's backend system.
- **Option 2** - SAP Cloud Integration/3rd Party Integration system as a middleware.
- **Option 3** - Direct connection (via SOAMANAGER) between SAP Logistics Business Network and your backend SAP S/4HANA or SAP TM system.

In this document, we are discussing the 2nd option where connections to SAP LBN are established using customer's SAP Cloud Integration tenant.

To establish this connectivity, certain integration artifacts need to be made available in your SAP Cloud Integration system. You can choose to develop your own artifacts or utilize the standard integration package – 'SAP Business Network for Logistics Connectivity: Integration Suite Configuration'. This is published in SAP API Hub and can be found in Discover tab of your SAP Cloud Integration tenant. The integration artifacts are configurable and the connectivity details such as communication details and authentication can be configured as mentioned in this document.

Important Note: We've migrated our existing integration platform from the SAP BTP Neo environment to the SAP BTP Multi-Cloud environment. This migration was completed at the end of May 2025. You can read more about the migration [here](#). A detailed [migration guide](#) is available, which outlines the necessary steps. The default value of the previous configuration in the 'Inbound to Network' iflow is now set to the multi-cloud platform. See [section 4.3](#) for more information.

2 Integration Package - SAP Business Network for Logistics Connectivity-Integration Suite Configuration

This package contains following three artifacts:

- **Inbound to Network**
 - As the name suggests this Integration Flow (iflow) is used to send data from your backend SAP system to SAP LBN.
 - The iflow accepts a SOAP message as input and forwards the same to SAP LBN as SOAP message.
 - Necessary headers are captured for monitoring purpose.
 - Logging can be configured by customer. By default, it's set as false.
 - Communication from backend SAP system to this iflow is authenticated based on User-Role. Meaning you can use any preferred authentication mechanism here. We recommend using a client certificate as it's more secure.
 - Communication from this iflow to SAP LBN is authenticated using client certificate.
 - Detailed steps on how to configure these can be found in the section below.
 - It's possible to connect to multiple SAP LBN tenants (test/production or FC/GTT etc.) from your backend systems using this iflow.

- **Outbound to Network**

- This Integration Flow is to connect SAP LBN to your backend SAP systems.
- The iflow accepts a SOAP message as input and forwards the same to your backend SAP system.
- Necessary monitoring headers are determined from the payload.
- Logging can be configured. By default, it's set as false.
- SOAP message from SAP LBN to this iflow is authenticated using a User-Role. LBN supports two modes of authentication when connecting to your SAP Cloud Integration system – Basic and Client Certificate. We recommend using client certificate for better security.
- Connection from this iflow to your backend SAP system is authenticated using Cloud Connector and Basic authentication.
- Cloud Connector location id can be configured.
- Details on how to configure different authentication is mentioned in section below.
- Target URL of SOAP services in your backend SAP system can be configured in a Value Mapping provided in this package.
- As the destination URL and authentication can be configured, it's possible to connect to different backend systems from this single iflow.

- **SystemName_MessageType to Destination**

- This Value Mapping artifact is used to specify the destination URL of a SOAP message based on system name and message type.
- System name and message name is derived from the SOAP message.
- You can configure the destination URL which is maintained in SOAPMANAGER configuration here.

3 How to import SAP BN4L Connectivity: Integration Suite configuration

Copy the integration packages SAP Business Network for Logistics Connectivity: Integration Suite Configuration from the catalogue to your customer workspace in SAP Cloud Platform Integration.

Procedure

1. Log on to the SAP Cloud Platform Integration Web UI as SAP Cloud Platform Integration Administrator.
2. Choose Discover from the top-level menu on the left.
3. Search for the “*SAP Business Network for Logistics Connectivity-Integration Suite Configuration*” package and choose Copy.

If you receive a warning that a package already exists in your workspace, choose either Overwrite or Create copy based on how you want to proceed. You can now start configuring the integration flow contained in this package.

4 Setup Inbound Connection to SAP LBN

As mentioned before, two connections need to be established to achieve inbound connection to SAP LBN.

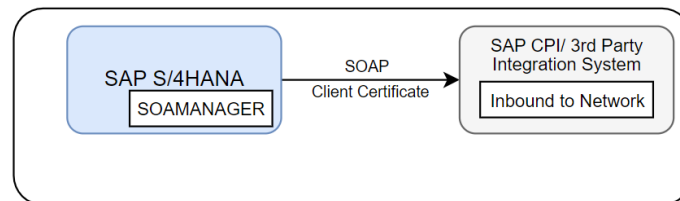
- Connection between your backend SAP system and your SAP Cloud Integration
- Connection between your SAP Cloud Integration and SAP LBN

4.1 Setup connection between backend and your SAP Cloud Integration

Authentication from SAP S/4HANA or SAP TM to SAP Cloud Integration is taken care by User-Role. This User-Role can be assigned to a client certificate or OAuth 2.0 credentials, etc in your SAP Cloud Integration sub-account. We recommend using client certificate as it's more secure. Steps for the same are captured here.

Your backend SAP system needs to store private key which is the key-pair (.p12) and recipient system needs to have the public key (leaf certificate in the certificate chain). The public key (.cer) has to be captured in SAP Cloud Integration tenant as a service key.

At runtime, SAP Cloud Integration checks if a service key is available that contains the client certificate sent by the sender. If a service key is available, the system then checks if the associated service instance has a role specified that grants permissions to call the integration flow endpoint.



4.1.1 Configurations in your backend SAP system

1. Generate a key pair certificate with SAP Identity Authentication (IAS) service.
2. Import the SAP IAS Certificate into your backend SAP system in STRUST transaction.
3. Setup Webservices using SOAMANAGER for inbound services to SAP Logistics Business Network from SAP TM. You can find the list of SAP LBN inbound services (termed as Provider API) here.
4. Deploy the 'Inbound to Network' iflow and configure the endpoint in your webservice.

4.1.2 Configurations in your SAP Cloud Integration

Create Service Instance and Service Key in SAP BTP Cockpit

1. Go to SAP BTP cockpit.
2. Select the subaccount that host your SAP Cloud Integration application.
3. Create an instance with 'Process Integration Runtime' as Service and 'Integration-flow' as service plan.

New Instance or Subscription

1 Basic Info 2 Parameters 3 Review

Enter basic info for your instance or subscription.

Service: * ⓘ Can't find what you're looking for?

Process Integration Runtime

Plan: *

Integration-flow

Instance Name: * ⓘ

instance_demo

Next > Create Cancel

4. Add instance name.
5. Set Roles parameter as 'ESBMessaging.send'
6. Set Grant-types as 'Client Credentials'
7. Create instance.

New Instance or Subscription

1 Basic Info 2 Parameters 3 Review

Configure instance parameters. ⓘ

Form JSON

Roles: ⓘ

ESBMessaging.send x

Grant-types: ⓘ

Client Credentials x

Redirect-uris: ⓘ

Access Token Validity (in seconds): ⓘ

3,600

< Back Next > Create Cancel

8. Then go through Creating Service Key and create a service key with a 'External Certificate' key type.

Service Keys (0)		Create
Name	Status	
No service keys to show. Either none were created, or you don't have space developer authorizations.		

New Service Key

Service Key Name: *

auth_key

Configure Binding Parameters: ⓘ

Form JSON

Key Type: ⓘ

External Certificate

External Certificate (only applicable for Key Type 'External Certificate'): ⓘ

Pin Certificate (only applicable for Key Type 'External Certificate'): ⓘ

Validity in days (only applicable for Key Type 'Certificate'): ⓘ

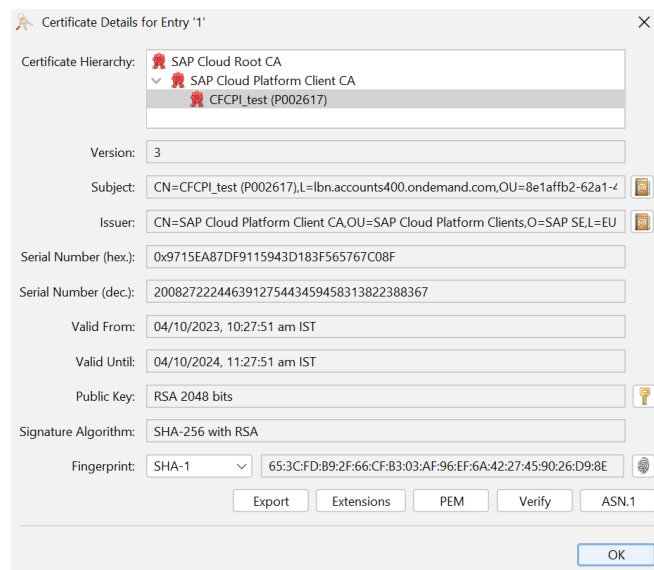
365

Key Size (only applicable for Key Type 'Certificate'): ⓘ

2048

Create Cancel

9. Now, we need to extract the leaf certificate from .p12 file by using KeyStore explorer.



10. Open the leaf certificate with your text editor and copy the content.

```
1 -----BEGIN CERTIFICATE-----
2 MIIIFujCCA6KgAwIBAgIQZNVZzARg0PLF3iPLXQypXDANBgkqhkiG9w0BAQsFADB5
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31 qC7pMbiLHYv6iac7YbF3L40lnyxUYKT3FKktYudgZaHz5jg5hcvKXmj kTwZH27H1
32 /YajRWDVFMuXq3nI3lyTg8cuLL4Mr/pI1Y/GSHzQ
33 -----END CERTIFICATE-----
```

11. Validate that your certificate looks like the one on the screenshot below:

12. Create Service key.

New Service Key

Service Key Name: *

auth_key

Configure Binding Parameters: ⓘ

Form
JSON

Key Type: ⓘ

External Certificate

External Certificate (only applicable for Key Type 'External Certificate'): ⓘ

iPUxlx18Ri64gEW y4W/XwQD2FDExWE21LaWYvNEs0NXhXOJ -----END CERTIFICATE-----

Pin Certificate (only applicable for Key Type 'External Certificate'): ⓘ

Validity in days (only applicable for Key Type 'Certificate'): ⓘ

- 365 +

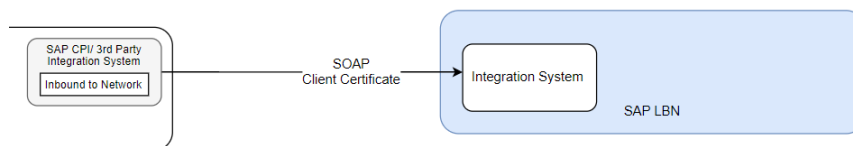
Key Size (only applicable for Key Type 'Certificate'): ⓘ

2048

Create
Cancel

4.2 Setup connection between your SAP Cloud Integration and SAP LBN

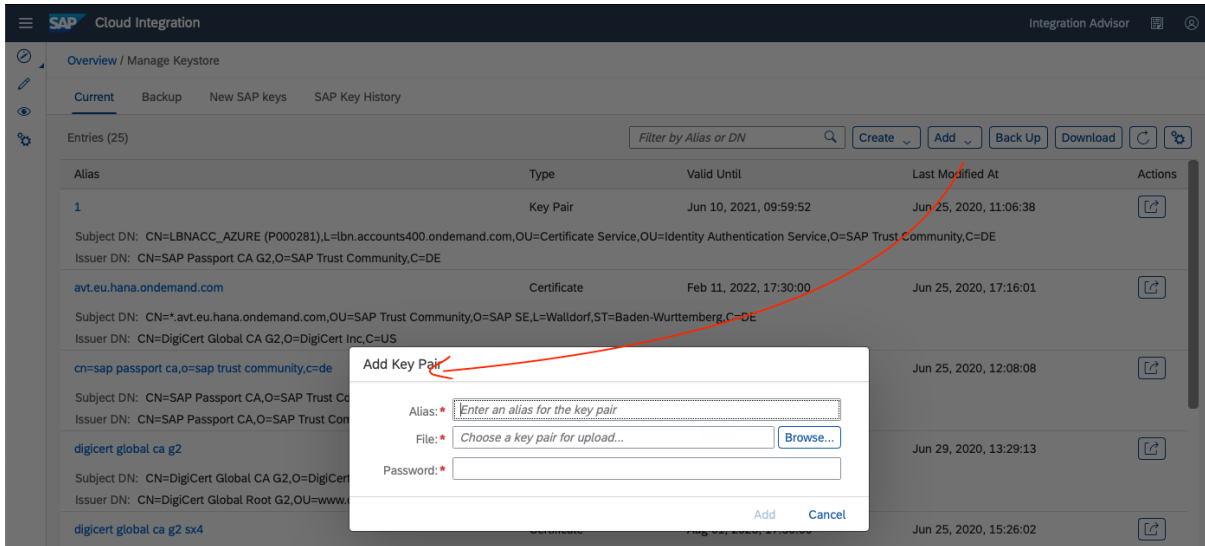
Inbound authentication to SAP LBN is achieved using client credentials only. You can generate another key-pair from your SAP IAS tenant for the same. The private key (.p12) needs to be uploaded in the sender system always, which is your SAP Cloud Integration tenant. The public key needs to be uploaded in your SAP LBN shipper app – System Connections. The private key needs to be uploaded in your SAP Cloud Integration tenant. Steps are captured below.



4.2.1 Configurations in your SAP Cloud Integration

Client certificate needs to be deployed in the SAP Cloud Integration tenant, which is used authenticating the connection from CPI to LBN.

- a) Log in to the SAP Cloud Integration tenant.
- b) From the menu select *Monitor*.
- c) In *Manage Security*, select *Keystore*.
- d) From the *Add* dropdown, select *Key Pair*.



e) Upload the *.p12 file (key pair).

Add Key Pair

Alias: * <LBN_ID>_certificate

File: * Certificate.p12

Password: *

f) Provide an Alias name that should be in the '<LBN_ID>_certificate' format. You must enter the same password as used to generate the key pair.

Alias	Type	Valid Until	Last Modified At	Subject DN	Issuer DN	Actions
...	Key Pair

4.2.2 Configurations in your SAP LBN

1. Logon to SAP Logistics Business Network application. Navigate to 'System Connection' app. Create a new connection of type ABAP-based SAP system.

New Connection

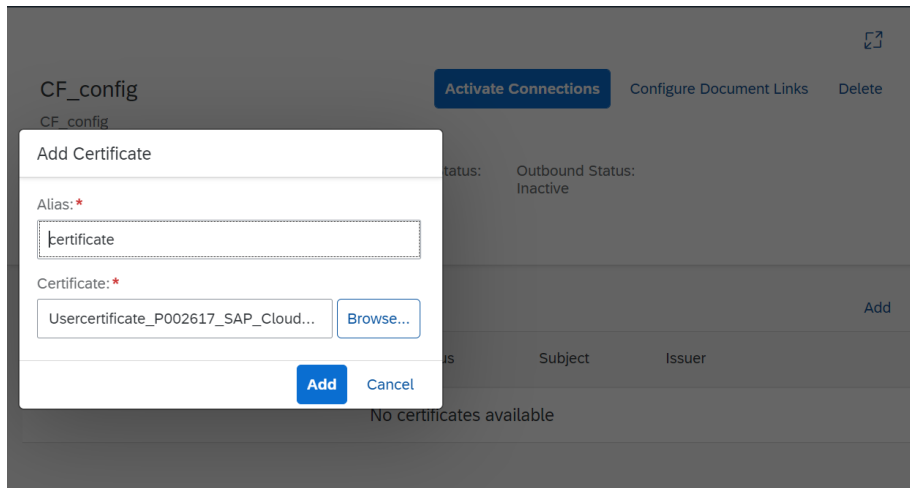
Connection Type: *
 ABAP-based SAP system

Connection ID: *
 CF_config

System ID: *
 CF_config

Add **Cancel**

- In the “Inbound to Network”, click on Add and upload the exported p12 leaf certificate.



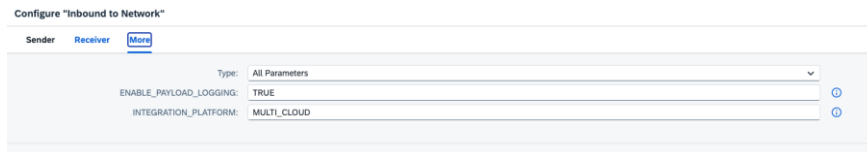
- Activate the Inbound Connection.

4.3 Configure ‘Inbound to Network’ iflow from the Package

- Select the Inbound to Network iflow in the package.
- From the menu, select *Configure*.
- Configure the more for Inbound iflow.
 - Navigate to *more* tab, select the *type* ‘All parameter’ option.
 - Set `ENABLE_PAYLOAD_LOGGING` by default it would be ‘FALSE’. You can enable logging of payload by configuring this as ‘TRUE’
 - The `INTEGRATION_PLATFORM` defaults to MULTI_CLOUD. (Supported values include: NEO and MULTI_CLOUD.) We recommend that you double-check this value. If you're still

working in the Neo environment, set this value to NEO. Refer to the [Important Note](#) at the beginning of the document for more information about the multi-cloud integration platform.

4. Click *Save* and *Deploy*.



5. The integration flows are deployed in the SAP Cloud Integration tenant.
6. To see status of the deployed artifacts, from the menu, select *Monitor* and then select *Manage Integration Content*.

Manage Integration Content section provides an overview of integration content artifacts, such as integration flows, that have been deployed on the tenant.

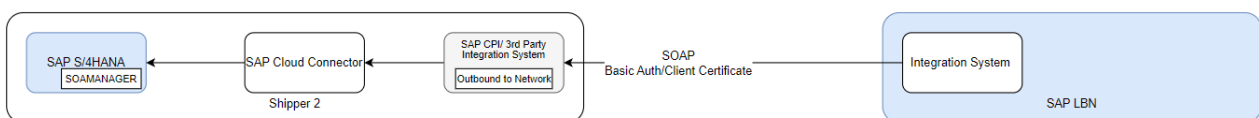
7. In *Artifact Details*, click *View deployed Artifact*.

5 Setup Outbound Connection from LBN to your CPI

Outbound connection from SAP LBN to your backend SAP system via SAP Cloud Integration can be achieved by the next two integration artifacts in the package. In this case, the authentication from SAP LBN to your SAP Cloud Integration tenant can be achieved using client certificate or Basic authentication. We recommend using client certificate as it's more secure.

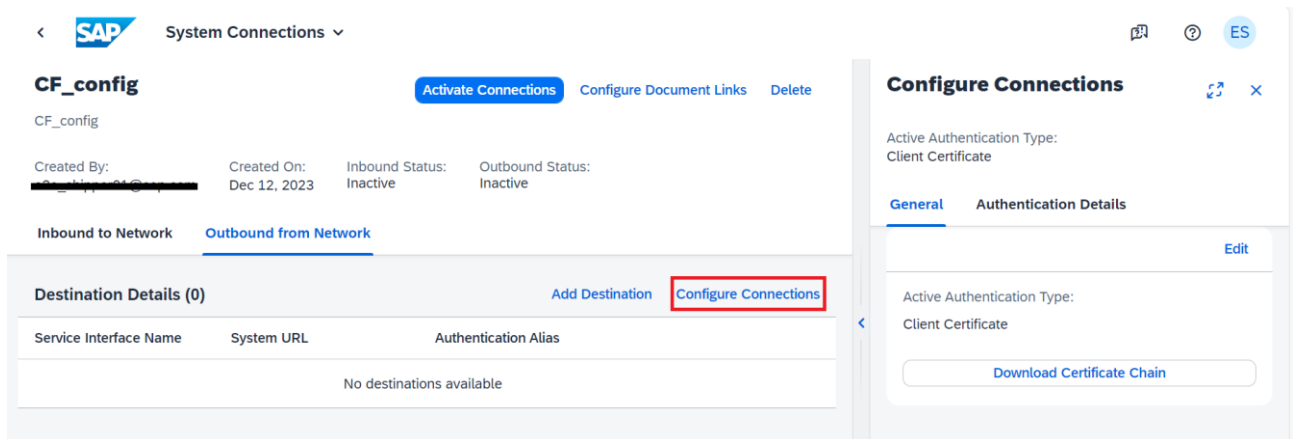
The connection from your SAP Cloud Integration tenant to your backend SAP S/4HANA system needs to be routed via a SAP Cloud Connector. We expect you've taken care of necessary configuration in SAP Cloud Connector to add your SAP Cloud Integration subaccount as a pre-requisite.

5.1 Setup connection between SAP LBN and your SAP Cloud Integration

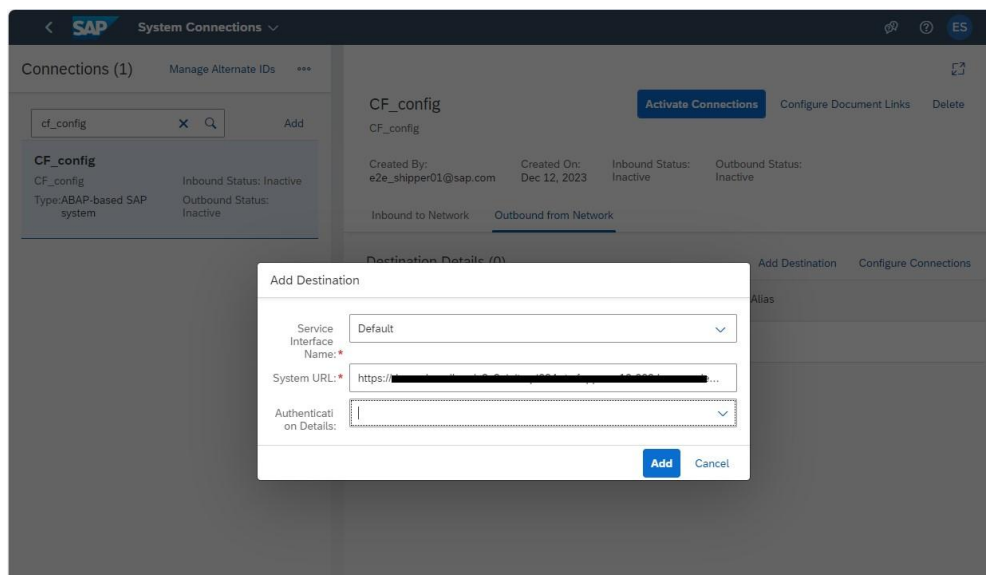


5.1.1 Configurations in LBN

1. In the system connection app, navigate to "Outbound from Network" tab, then click on "Configure Connection". In the right panel, click on "EDIT, select Active Authentication Type as "Client Certificate", then click on "Certificate Chain". This will download a *.P7B file into your web browser's download folder. This certificate will be used to authenticate flow from SAP Logistics Business Network to your SAP Cloud Integration instance.



2. Extract the leaf certificate using key store explorer.
3. Then go through [Create a service key](#) with a 'External Certificate' key type and add the extracted certificate.
4. For communication from SAP Logistics Business Network to your Cloud Integration layer, you must maintain your SAP Cloud Integration iflow endpoint in System connection app.



5. Open System connection app and navigate to connection you have created earlier step.
6. In the Outbound from Network tab, click on "Add Destination" and maintain the endpoint for each "Service Interface Name". Authentication details will be blank.

7. Click on Activate button.
8. Create user credentials in SAP Cloud Integration tenant.
 - a) Log in to the SAP Cloud Integration tenant.
 - b) From the menu select *Monitor*
 - c) In *Manage Security* Select *Security Material*
 - d) Create user credentials with the name as your SAP backend system name. This name is picked from the SOAP message header <RecipientBusinesssystemID>. Example: if you're source system name is captured as ABC_123, credential name should be the same- 'ABC_123_credential'

5.2 Setup connection between your SAP Cloud Integration and your backend SAP system

The Cloud Connector serves as a crucial intermediary, facilitating seamless communication between SAP Business Technology Platform (BTP) applications and on-premise systems. Its design emphasizes simplicity in setup and transparent configuration of on-premise systems that interface with SAP BTP. Operating as an on-premise agent within a secure network environment. Notably, the Cloud Connector provides administrators with fine-grained control, allowing them to specify which on-premise systems and resources can be accessed by cloud applications, as well as configuring the behavior of cloud applications utilizing the Cloud Connector.

Since we're connecting to SAP system, we'd need to connect via Cloud Connector. We should ask the customer to add their CPI sub account in Cloud Connector and maintain the location id from Cloud Connector config in here.

Pre-requisite

1. Your SAP Cloud Integration subaccount should be added in your SAP Cloud Connector. In the Cloud Connector configurations, ensure that you're using subaccount details of your SAP Cloud Integration tenant.

5.2.1 Capturing destination detail in value mapping artifact

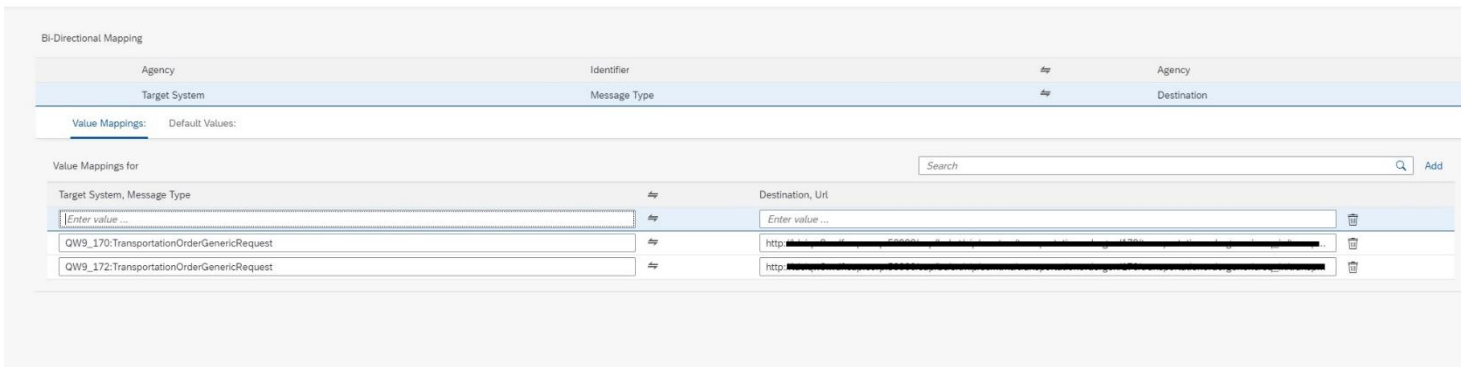
This Value Mapping integration artifact enables customers to maintain a configuration table for the destination URLs for different SOAP services in your backend SAP systems. This offers support to routing to multiple systems from LBN.

1. In the package choose action and configure *Value Mappings*, do the following:
 - a. Add the value mapping.
 - b. Map the Target system name and Message Type to destination URL.
Example:
Target System, Message Type: *QW9_170:TransportationOrderGenericRequest*

Destination, URL:

http://<VirtualHostDefinedinCloudConnector>/<PathDefinedInSOAMANAGER>

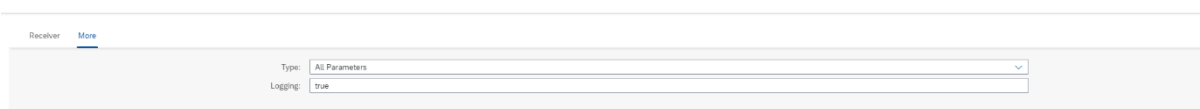
- c. Deploy the value mapping.



- 2. In *Artifact Details*, click *View deployed Artifact*.

5.2.2 Configure 'Outbound from Network' iflow from the package

- 1. Log in to the SAP Cloud Integration tenant.
- 2. To configure the iFlows, from the menu select *Design*.
- 3. Select the integration package.
- 4. Select the required iflow.
- 5. From the *Actions* menu, select *Configure*.
- 6. Configure the more for Outbound iflow.
 - a. In the *more* tab, select the *type* 'All parameter' option.
 - b. Set *ENABLE_PAYLOAD_LOGGING* by default it would be 'FALSE'. You can enable logging of payload by configuring this as 'TRUE'.



- c. In the *Receiver* tab, Enter the 'Location ID'



- d. Click *Save* and *Deploy*.

If you set the parameter to true, the complete message payload containing all data that is to be transferred is stored in the log.

To see status of the deployed artifacts, from the menu, select *Monitor* and then select *Manage Integration Content*

6 Note

Certificates play a crucial role in ensuring secure communication between the S/4 system and the CPI, and any lapse in their validity could disrupt this connection.

1. Certificates within the LBN will receive reminder/notification to monitor the certificate expiry.
2. Certificates used for connecting S/4 and your CPI, customer must keep an explicit reminder for those.