SAP e-Invoice for India - Integration with GSP (GST Suvidha Provider)

Via SAP Integration Suite Service in Cloud Foundry environment

GSP Integration Set Up Guide

Document History

Version	Date	Change
1.0	2020-02-06	First release of the EInvoice GSP Setup Guide
1.1	2020-09-23	Updated Section 3 ‘Pre-requisites’ with the Initial setup link for Integration Suite option Updated Section 4.2 ‘Deploy IRP User Credentials per GSTIN’ Created new section 4.4 ‘Deploy IRP Signed Content Verification Public Key Certificate’ Updated Section 4.5.2 ‘Deploying GSP Integration flow’ Created section 4.6 ‘Basic Authentication Settings’
1.2	2021-03-24	Updated the complete document to reflect the latest SAP Branding changes for SAP Business Technology Platform(BTP), SAP Integration Suite and Integration Flow. Updated Section 4.5.2 'Deploying GSP Integration Flow' with details on new field userGSTIN_publicAPI in step 10 - Configure.

Contents

1 Glossary

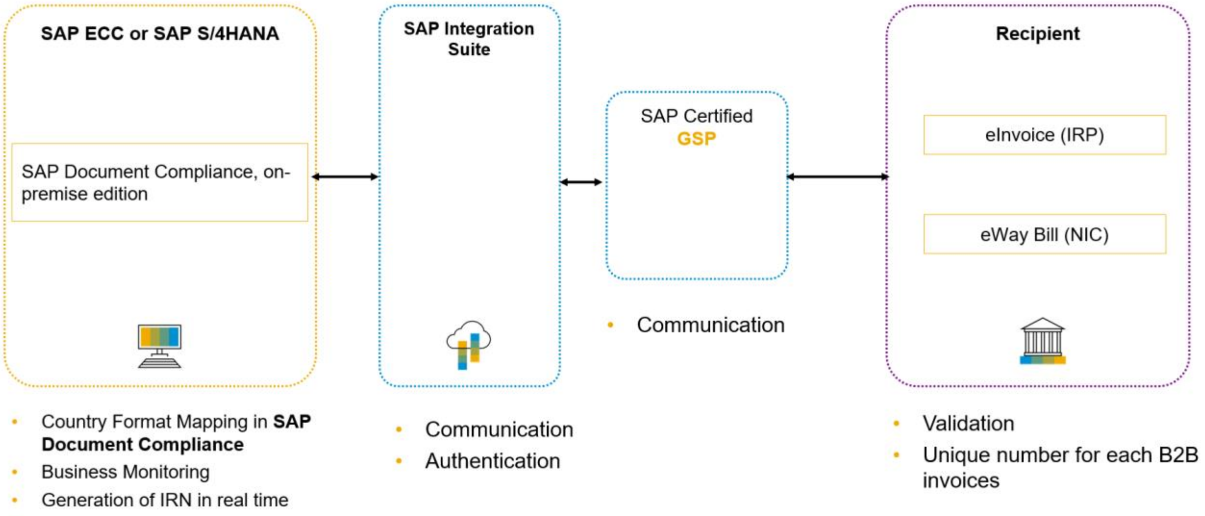
The table below lists the terms and abbreviations used throughout this document:

Term	Description
GST	Goods and Services Tax
GSP	GST Suvidha Provider
GSTIN	Goods and Services Taxpayer Identification Number
IRN	Invoice Reference Number
IRP	Invoice Registration Portal
CF	Cloud Foundry
SAP BTP	SAP Business Technology Platform
NIC	National Informatics Centre

2 Introduction

Using the SAP Solution for eInvoice India, you can generate Invoice Reference Number (IRN) as per the legal requirement in India.

The eInvoice solution requires the integration between SAP Business Application (SAP ERP or SAP S/4HANA) and GSP. This document describes the steps to configure and deploy the SAP Integration Flow to establish communication between SAP Business Application and GSP(s).



Note:

SAP offers two Cloud environments, namely Neo and Cloud Foundry and this document is intended for the setting-up of eInvoice India integration for Cloud Foundry environment.

3 Pre-requisites

Before you start with the activities described in this document, ensure that the following prerequisites are met.

1. You have installed in the test and productive systems all necessary SAP Notes for the eInvoice Solution. Refer note : 2884058
2. If you have subscribed to Process Integration, perform all the initial setup steps described in Initial Setup of SAP Cloud Integration in Cloud Foundry Environment.
3. If you have subscribed to Integration Suite, perform all the initial setup steps described in Initial Setup of SAP Integration Suite.
4. After completing the 'Provisioning the Tenant' step, you have created your own tenant URL. This is the URL (referred as WEB UI URL) needed to complete the steps described in the Configuration Steps section of this guide.
5. You have received the following information from your *GST Suvidha Provider (GSP)*:
    - GST Suvidha Provider (GSP) Integration/Set up Manual.
    - Trusted certificates from GSP for SSL handshake.
    - IRP Public Key Certificate (SAP Integration expects the certificate in Base-64 encoded X.509 (*.CER*) format). For more details, see here.
    - IRP Signed Content Verification Public Key Certificate. (SAP Integration expects the certificate in Base-64 encoded X.509 (.CER) format). For more details, see here.
    - For Sandbox access via GSP, request the IRP test user credentials from GSP directly
    - For Production access via GSP, refer here.
    - Other technical details such as API end point URLs for sandbox/production, GSP specific credentials, etc.
    - Two Integration Flows (.zip files) from GSP and save to any local location in your desktop.
        - GSP Integration Flow (Integration Flow specific to GSP)
        - Router Integration Flow (Routes eInvoice request from SAP Business Application to specific GSP Integration Flow)

4 Configuration Steps in SAP Integration Suite

Perform the following steps:

1. Import SSL Certificates from GSP to SAP Integration Tenant
2. Deploy IRP User Credentials per GSTIN
3. Deploy IRP Public Key Certificate
4. Deploy IRP Signed Content Verification Public Key Certificate
5. Deploying Integration Flow
6. Basic Authentication Settings
7. Client Certificate-based Authentication Settings

Note:

The SSL certificate upload, setting-up of user credentials, IRP Public Key Certificate Upload, IRP Signed Content Verification Public Key Certificate Upload and authentication setup are all required to be done only during the initial set up of the eInvoice Integration scenario. Subsequently, if there is an updated version of integration flow delivered, it is required to repeat only Step 5. However, in case there is a change in certificate from GSP or IRP, then step 1 or step 3 or step 4 needs to be done accordingly.

4.1 Import SSL Certificates from GSP to SAP Integration Suite Tenant

To set up an SSL connection between the SAP Integration Tenant and GST Suvidha Provider (GSP), you must import the required security certificates into SAP Integration Tenant Keystore.

Note:

You receive these certificates from your GSP.

Procedure

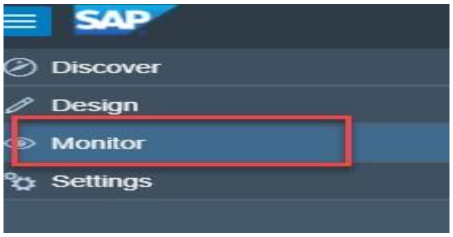
1. Access the SAP Integration Tenant.

   After Provisioning the tenant as described in the Initial Tenant Setup, the URL will be created.

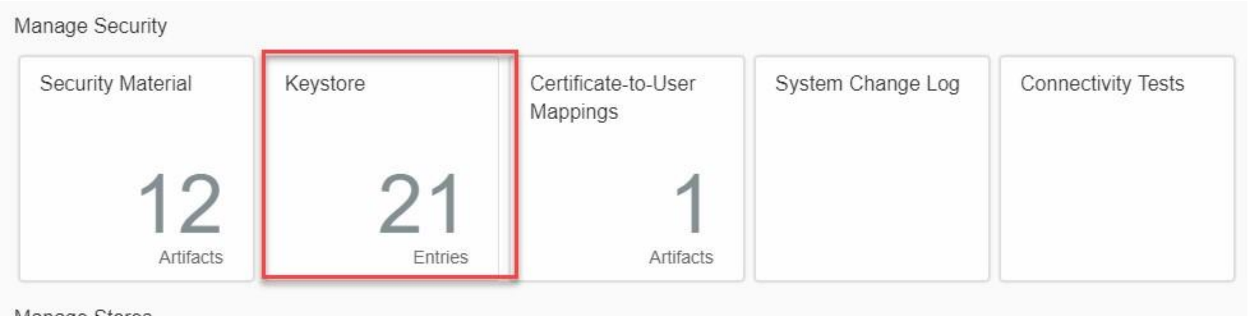
   Use this URL to go to the Web UI of the tenant.
2. To logon, enter your S user.

   If you get *HTTP Status 403* error, then send a mail to service@sap.com.

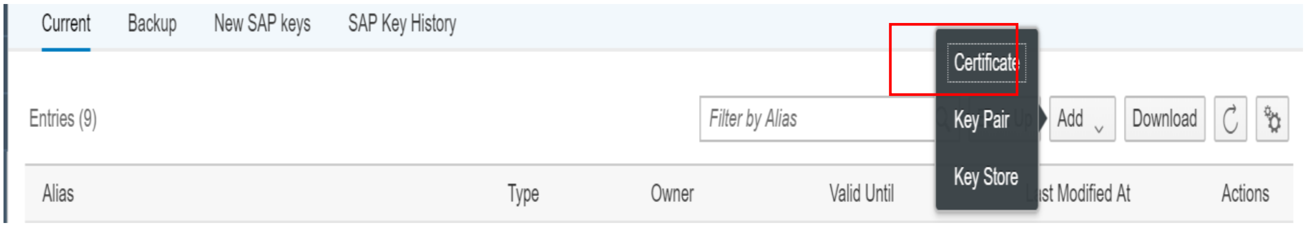
3. After successful login, from the menu in the upper left corner, choose *Monitor*.



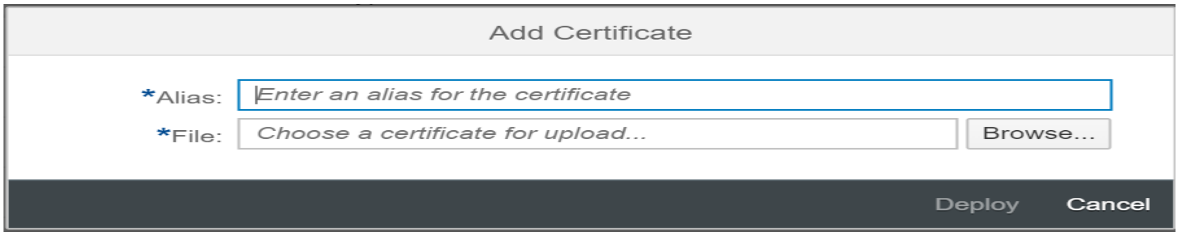
4. Choose **Manage Security** and then **Keystore**.



5. Click Add > **Certificate** > **Add Certificate**



6. Enter an alias to identify the certificate. Browse the certificate from local desktop and then Deploy.


Add Certificate
*Alias:
Enter an alias for the certificate
*File:
Choose a certificate for upload...
Browse...
Deploy
Cancel

Note:

To perform the above operation, you need to be a tenant administrator with role **AuthGroup.Administrator.**

The certificate should be in Base-64 encoded X.509(.CER) format. Refer here.

7. Check the connectivity with GSP.

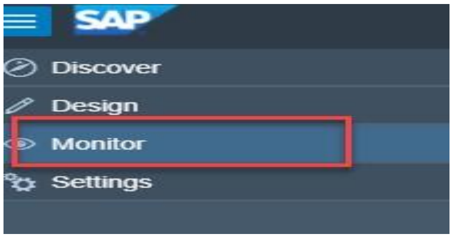
You can perform the Connectivity test with the GSP by using the feature TLS Connectivity Test as mentioned here.

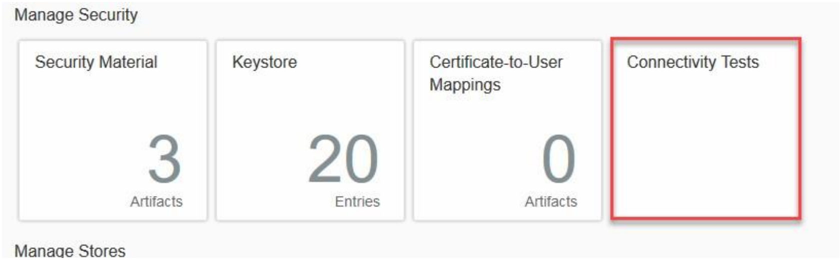
i. Run connectivity test using the Monitor-> Manage Security- >Connectivity Tests.

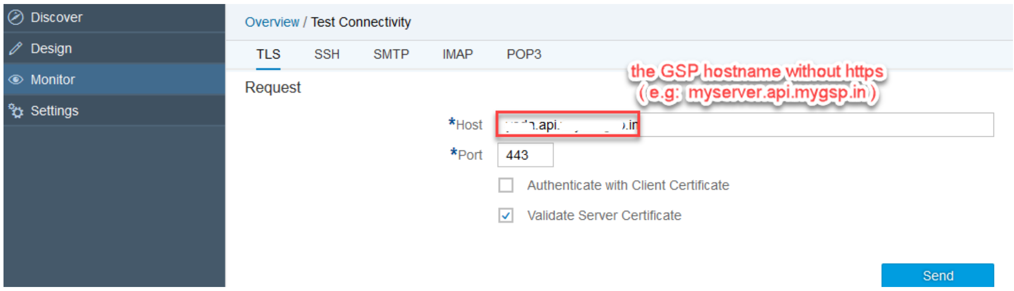
ii. Enter the GSP Base URL without http(s). Enter port.

iii. Click **Send**

On successful connection, system displays successful response message.







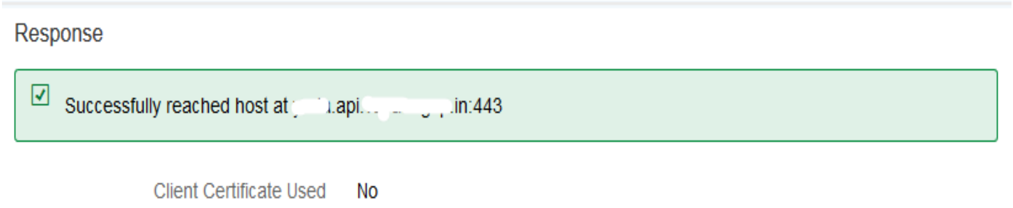
the GSP hostname without https (e.g: myserver.api.mygsp.in)

*Host [redacted]n.api.[redacted].in

*Port 443

□ Authenticate with Client Certificate

☑ Validate Server Certificate



☑ Successfully reached host at [redacted].api.[redacted].in:443

Client Certificate Used No

4.2 Deploy IRP User Credentials per GSTIN

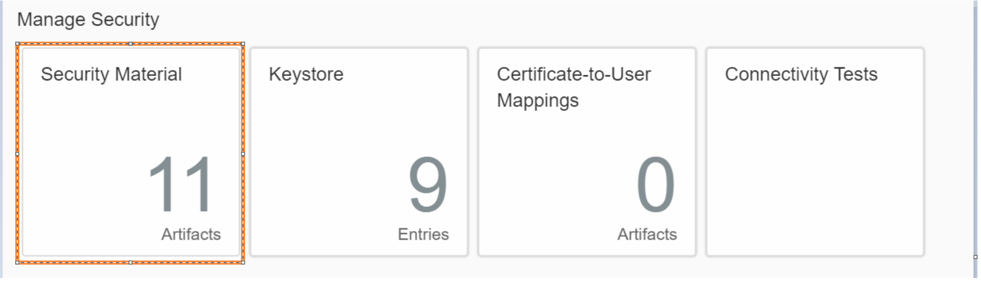
Add IRP User Credentials entries per GSTIN to the User Credentials Service of SAP Integration tenant by following the process mentioned here

Note:

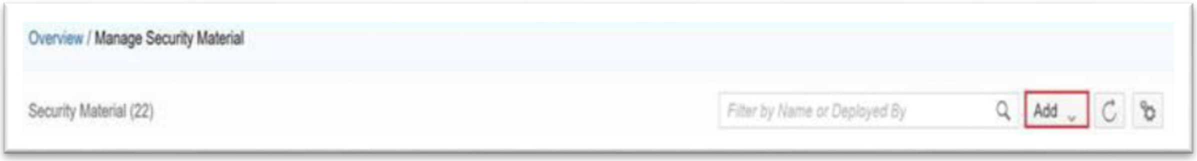
To perform above operation, you need to be a tenant administrator with role **AuthGroup.Administrator.**
Refer GSP Registration on IRP Portal for details.

To add IRP User Credentials per GSTIN to SAP Integration:

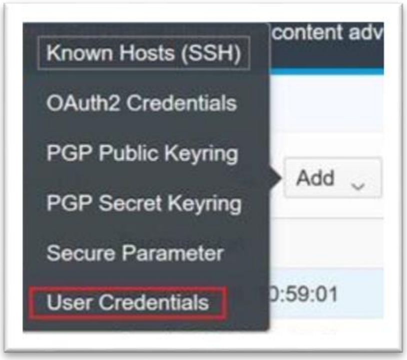
1. Go to Security material. Navigate to Monitor > Manage Security > Security Material.



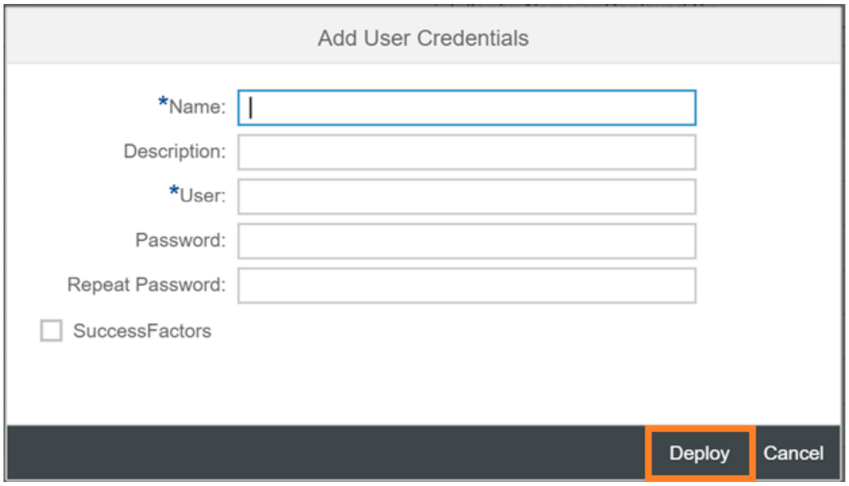
2. Add a new user credential.


Overview / Manage Security Material
Security Material (22)
Filter by Name or Deployed By
Add

3. Click User Credentials



4. Add and Deploy the user credentials



Note:

- In the Name field, enter the GSTIN of the business place to which the user belongs.
- In Production, IRP allows the existing eWay Bill API credentials to be used for eInvoice as well.
- However, if the user credentials are created explicitly for eInvoice, then, maintain the name field with the suffix '_einv' (Ex : 27AAAPI3182M002_einv).
- The suffix (_einv) is case sensitive.

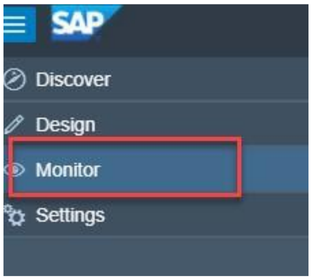
Name	GSTIN of the business place to which the user belongs / GSTIN of the business place with suffix '_einv'
Description	Any relevant text (optional)
User	API User ID created in IRP portal (production) or received from GSP (pre-production)
Password/ Repeat password	Password

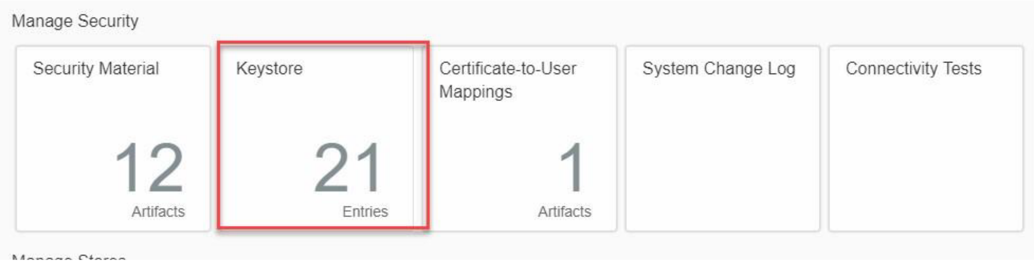
4.3 Deploy IRP Public Key Certificate

You need to add the IRP Public Key Certificate. You get this certificate from your GSP.

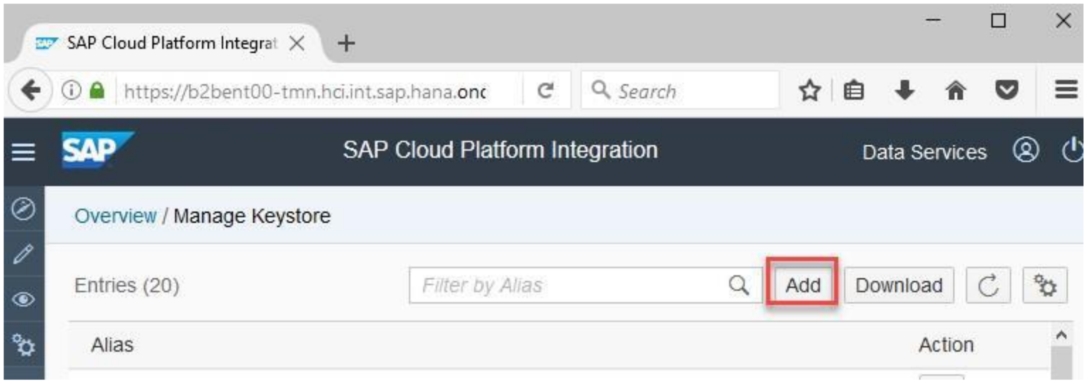
Follow the below steps to add the IRP Public Key Certificate to the SAP Integration KeyStore.

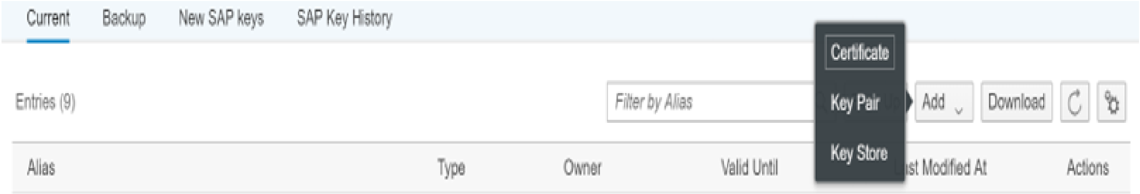
1. Navigate to **Monitor** > **Manage Security** > **Keystore**



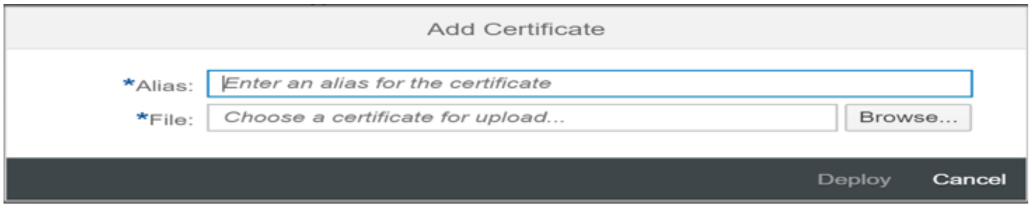


2. Click Add > **Certificate** > **Add Certificate**


SAP Cloud Platform Integrat
https://b2bent00-tmn.hci.int.sap.hana.ond
Search
SAP
SAP Cloud Platform Integration
Data Services
Overview / Manage Keystore
Entries (20)
Filter by Alias
Add
Download
Alias
Action



3. Enter an alias(**irpcert**) to identify the certificate. Browse the IRP Public Key Certificate from local desktop.


Add Certificate
*Alias:
Enter an alias for the certificate
*File:
Choose a certificate for upload...
Browse...
Deploy
Cancel

4. Click **Deploy**

Note:

To perform the above operation, you need to be a tenant administrator with role **AuthGroup.Administrator.**

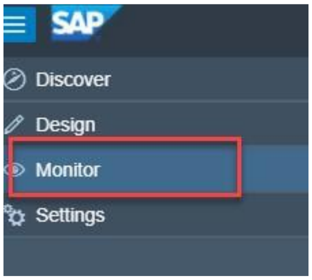
The certificate should be in Base-64 encoded X.509(.CER) format. For more information, see here.

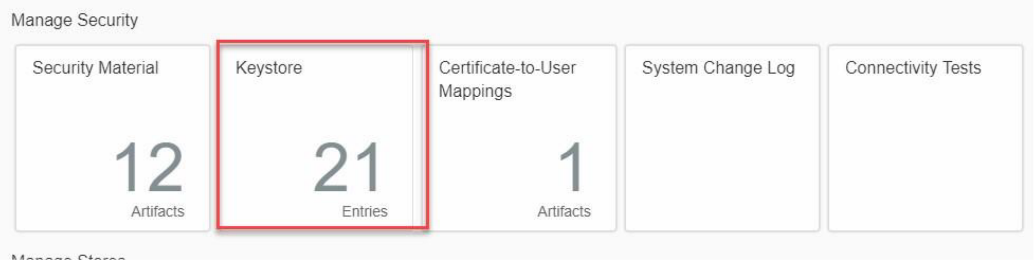
4.4 Deploy IRP Signed Content Verification Public Key Certificate

You need to add the IRP Signed Content Verification Public Key Certificate. You get this certificate from your GSP. This Certificate is used to validate the signed content fields such as SignedQRCode and SignedInvoice received from IRP.

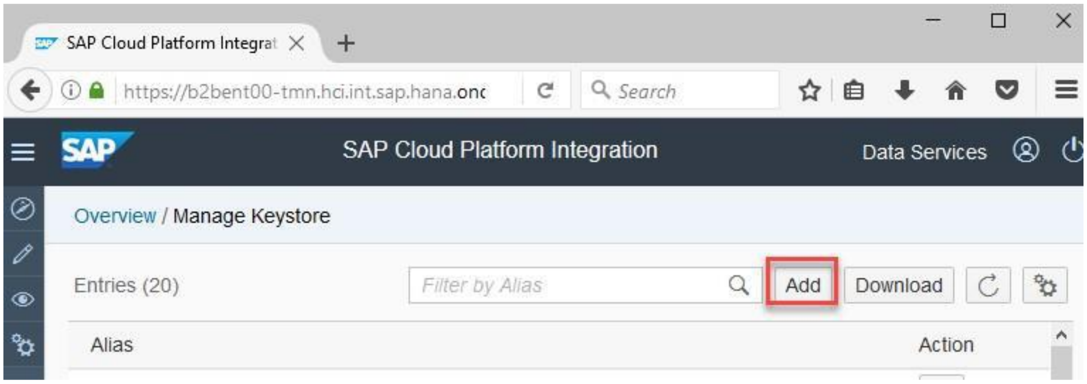
Follow the below steps to add the IRP Signed Content Verification Public Key Certificate to the SAP Integration KeyStore.

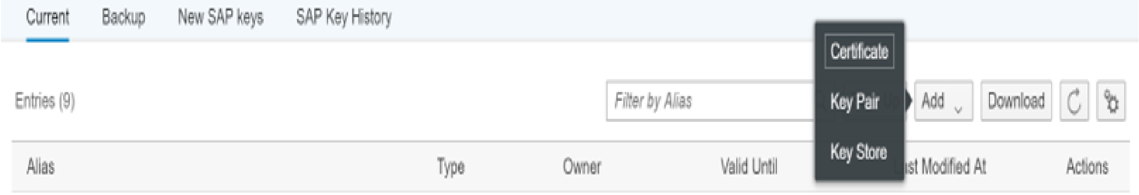
1. Navigate to **Monitor** > **Manage Security** > **Keystore**



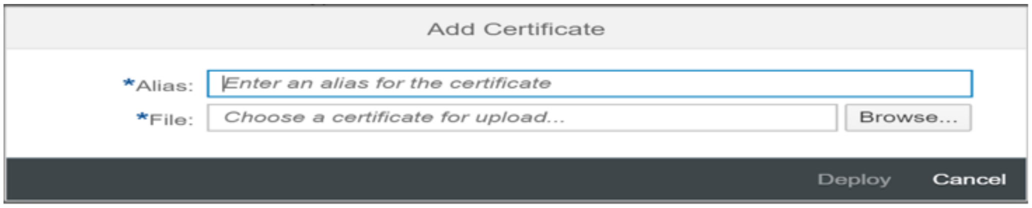


2. Click Add > **Certificate** > **Add Certificate**


SAP Cloud Platform Integrat
https://b2bent00-tmn.hci.int.sap.hana.onc
Search
SAP
SAP Cloud Platform Integration
Data Services
Overview / Manage Keystore
Entries (20)
Filter by Alias
Add
Download
Alias
Action



3. Enter an alias(**jwtcert**) to identify the certificate. Browse the IRP Signed Content Verification Public Key Certificate from local desktop.


Add Certificate
*Alias:
Enter an alias for the certificate
*File:
Choose a certificate for upload...
Browse...
Deploy
Cancel

4. Click **Deploy**

Note:

To perform the above operation, you need to be a tenant administrator with role **AuthGroup.Administrator.**

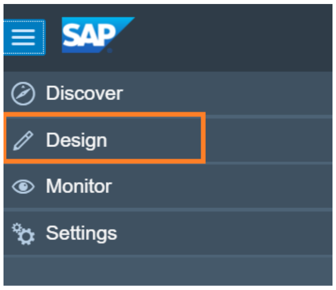
The certificate should be in Base-64 encoded X.509(.CER) format. For more information, see here.

4.5 Deploying Integration Flow

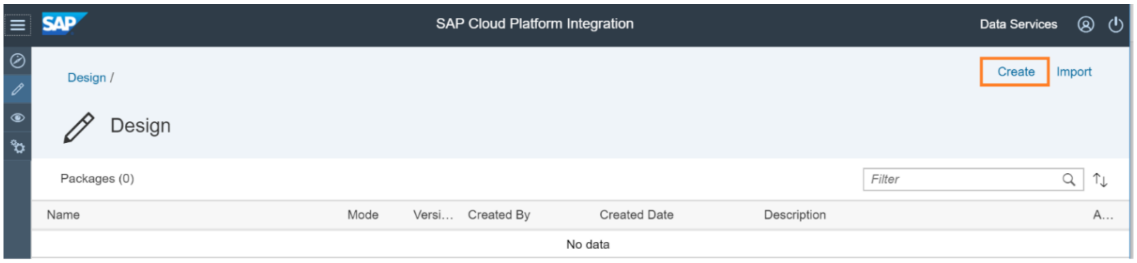
1. Creating content package: (one-time activity)

   To create a content package, follow the steps:

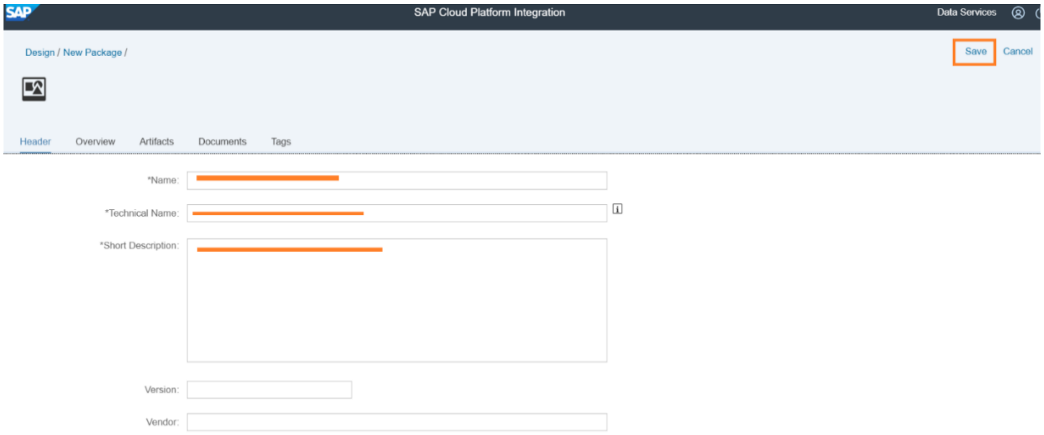
   i. Go to Design.



   ii. Choose Create.



iii. Enter appropriate Name and Description and click Save.



The content package is created.

2. Updating content package

When you already have previous version of integration flow deployed in your tenant and need to replace it with new integration flow, then follow below instructions

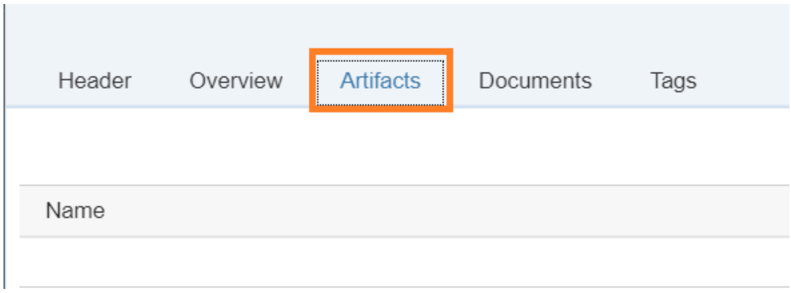
- Choose the content package under which the previous integration flow is deployed.
- Click on "Edit" button (seen in left side)
- Go to artifacts tab, click on action icon □ configure. Copy the values of the fields maintained over there locally, as it can be used later if GSP confirms these parameters are valid or get the exact latest externalized parameters values. Close the configure pop-up screen.
- Select the integration flow, click on action icon □ delete.

Note:

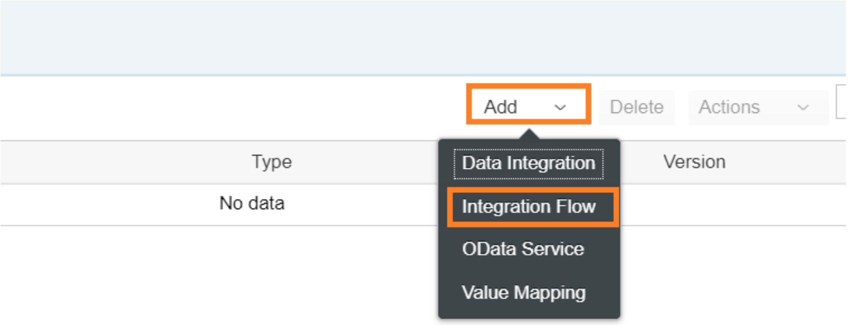
Repeat this 'Updating content package' step for each of the Router and GSP integration flows.

4.5.1 Deploying Router Integration Flow

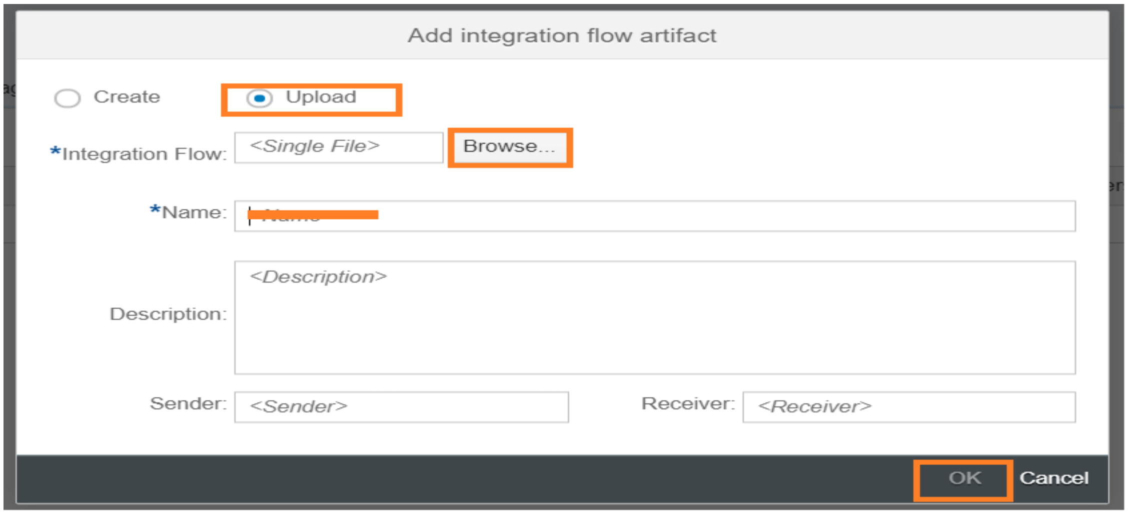
1. Within the same content package, Choose Artifacts.



2. Click Add and choose Integration Flow.



3. Select Upload.
4. Browse for the appropriate integration flow (.zip file)
5. Enter the Name and Description and click Ok.

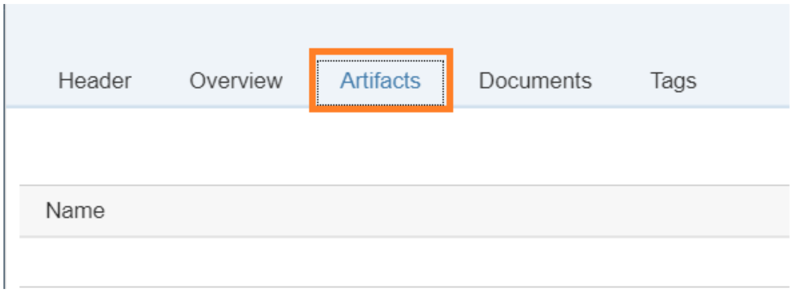


Integration flow is successfully added.

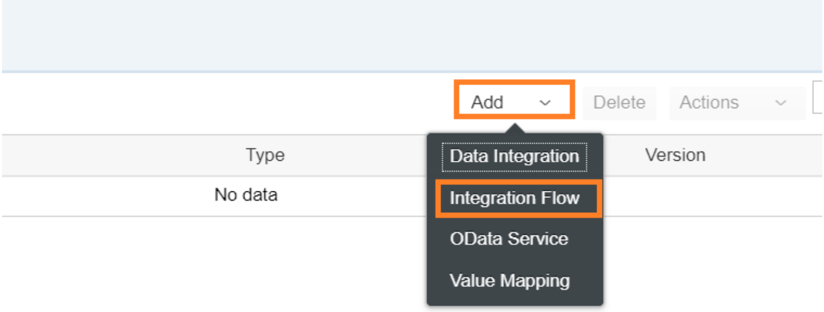
6. Select the Router integration flow.
7. Click **Deploy**.

4.5.2 Deploying GSP Integration Flow

1. In the same content package, Choose Artifacts.



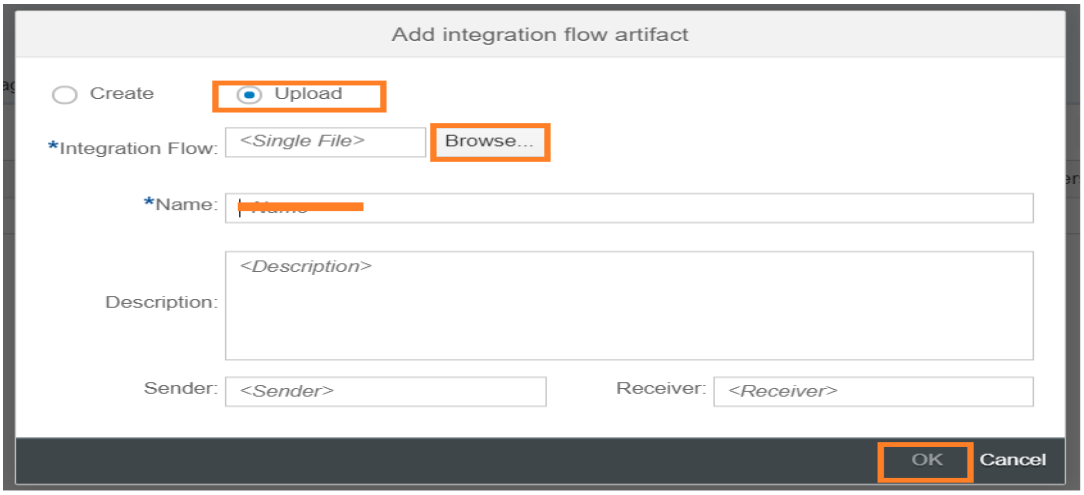
2. Click Add and choose Integration Flow.



3. Select Upload.

4. Browse for the appropriate integration flow (.zip file)

5.Enter the Name and Description and click Ok.



Add integration flow artifact

○ Create ● Upload

*Integration Flow: <Single File> Browse...

*Name: [redacted]

Description: <Description>

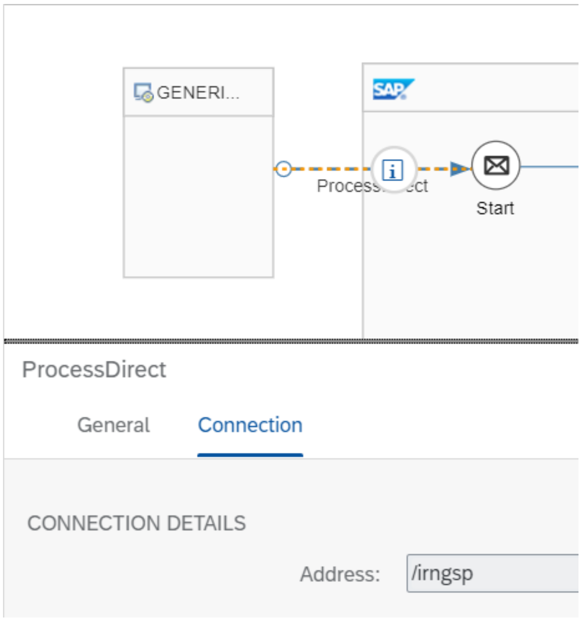
Sender: <Sender> Receiver: <Receiver>

OK Cancel

Integration flow is successfully added. For more information, see here.

8. Select the GSP Integration Flow. The Integration Flow screen is displayed.

9. Click on the Process Direct as shown below.



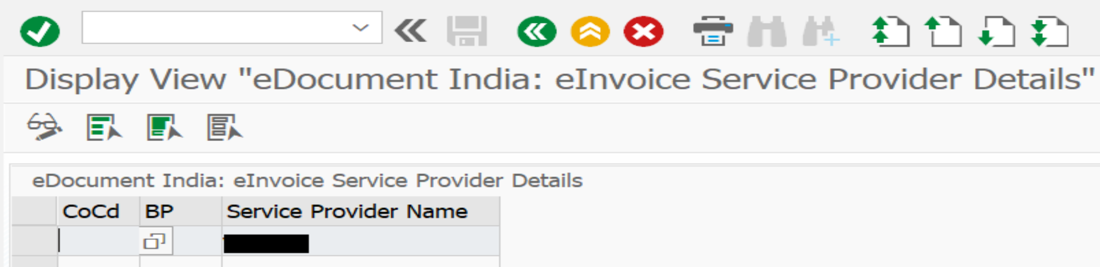
CONNECTION DETAILS

Address: /irngsp

Choose the Connection tab. Copy the value in Address field without slash and irn to the service provider name in the SAP Business Application -> sm30 -> view EDOINEINVGSPV

Note:

The value is case sensitive.



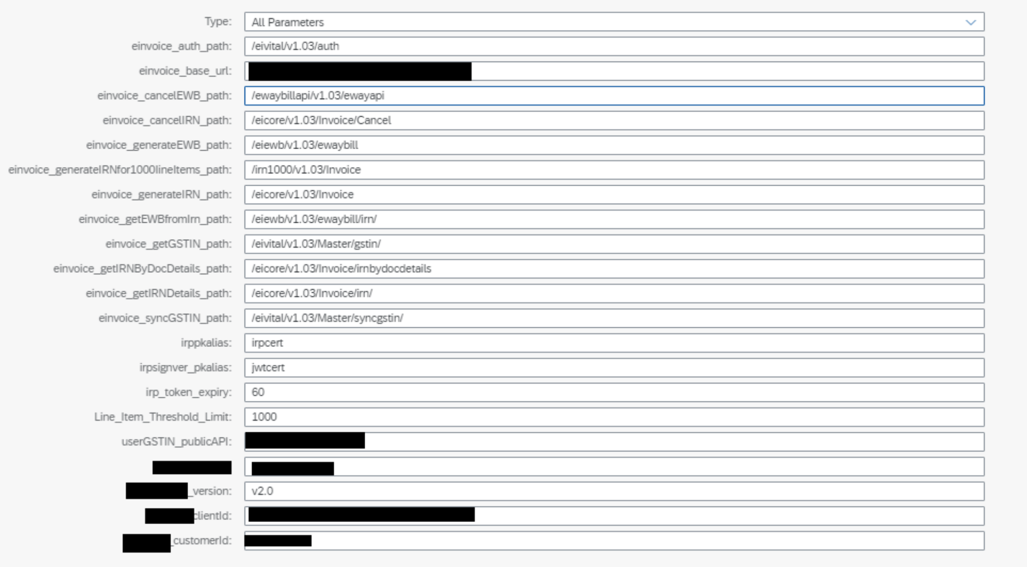
Display View "eDocument India: eInvoice Service Provider Details"

eDocument India: eInvoice Service Provider Details

CoCd	BP	Service Provider Name
		[redacted]

10. Click **Configure**.

    Choose the tab More and modify the parameters as shown below:



Type:	All Parameters
einvoice_auth_path:	/eivital/v1.03/auth
einvoice_base_url:	[redacted]
einvoice_cancelEWB_path:	/ewaybillapi/v1.03/ewayapi
einvoice_cancelIRN_path:	/eicore/v1.03/Invoice/Cancel
einvoice_generateEWB_path:	/eiewb/v1.03/ewaybill
einvoice_generateIRNfor1000lineItems_path:	/irn1000/v1.03/Invoice
einvoice_generateIRN_path:	/eicore/v1.03/Invoice
einvoice_getEWBfromIrn_path:	/eiewb/v1.03/ewaybill/irn/
einvoice_getGSTIN_path:	/eivital/v1.03/Master/gstin/
einvoice_getIRNByDocDetails_path:	/eicore/v1.03/Invoice/irnbydocdetails
einvoice_getIRNDetails_path:	/eicore/v1.03/Invoice/irn/
einvoice_syncGSTIN_path:	/eivital/v1.03/Master/syncgstin/
irppkalias:	irpcert
irpsignver_pkalias:	jwtcert
irp_token_expiry:	60
Line_Item_Threshold_Limit:	1000
userGSTIN_publicAPI:	[redacted]
[redacted]	[redacted]
[redacted]_version:	v2.0
[redacted]lientId:	[redacted]
[redacted]_customerId:	[redacted]

Note:

- In field irppkalias, you enter the alias(**irpcert**) of IRP Public Key Certificate.

  You have already deployed IRP Public Key Certificate in KeyStore as described in section Deploy IRP Public Key Certificate

- In field irpsignver_pkalias, you enter the alias(jwt**cert**) of IRP Signed Content Verification Public Key Certificate.

  You have already deployed IRP Signed Content Verification Public Key Certificate in KeyStore as described in section Deploy IRP Signed Content Verification Public Key Certificate

- In field userGSTIN_publicAPI, you enter one of the GSTIN which needs to be used for making public API calls such as getGSTIN and syncGSTIN and this field is mandatory only for public API calls.

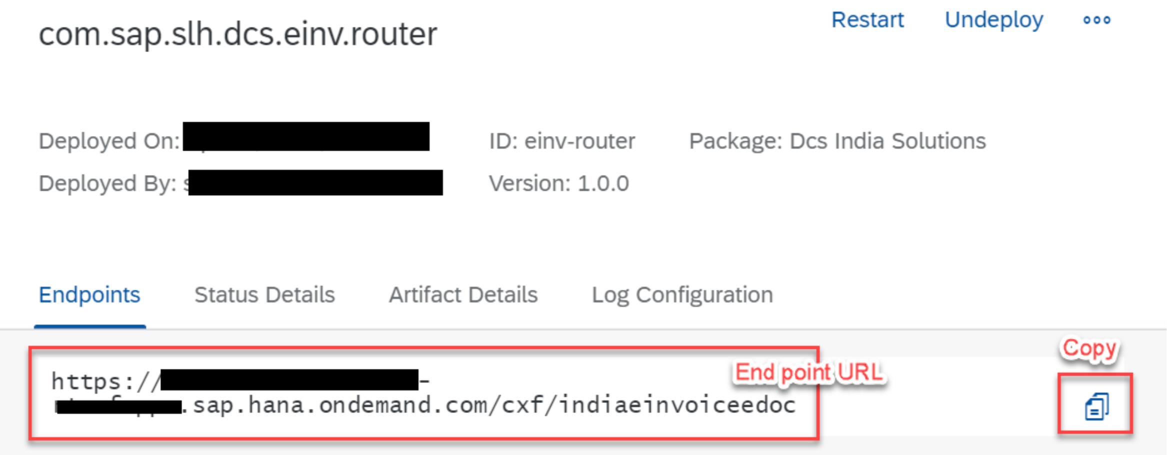
- You receive details about other fields from your GSP

11. Save your changes.

12. Click **Deploy** to deploy the modified integration flow.

Note:

- After the successful deployment, verify that the integration flows are in the Started state by clicking Monitor -> Manage Integration Content.
- To obtain the Endpoint URL:
  1. Click Monitor > Manage integration Content
  2. Choose the Router integration flow.
  3. The Endpoint URL can be found on the right side of the page.



com.sap.slh.dcs.einv.router

Deployed On: [redacted]

Deployed By: [redacted]

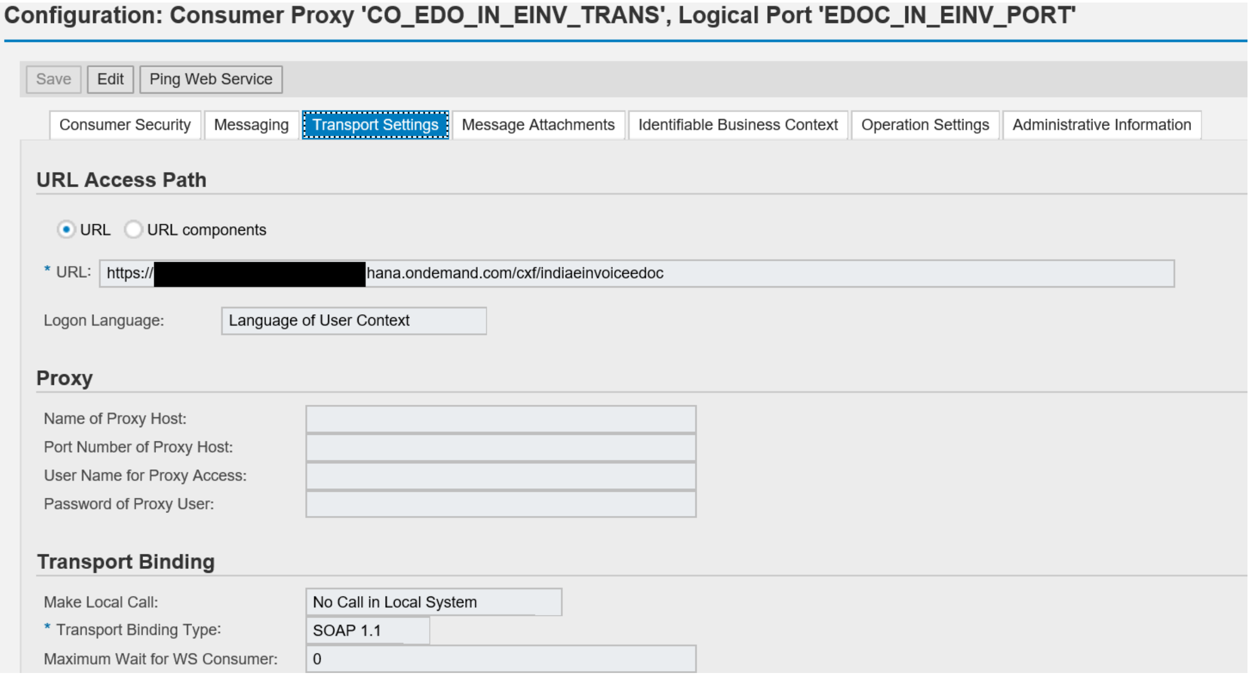
ID: einv-router

Version: 1.0.0

Package: Dcs India Solutions

https://[redacted]-
[redacted].sap.hana.ondemand.com/cxf/indiaeinvoiceedoc

  4. This URL must be configured in the SOA Manager.



Configuration: Consumer Proxy 'CO_EDO_IN_EINV_TRANS', Logical Port 'EDOC_IN_EINV_PORT'

URL Access Path

● URL ○ URL components

* URL: https://[redacted]hana.ondemand.com/cxf/indiaeinvoiceedoc

Logon Language: Language of User Context

Proxy

Name of Proxy Host:

Port Number of Proxy Host:

User Name for Proxy Access:

Password of Proxy User:

Transport Binding

Make Local Call: No Call in Local System

* Transport Binding Type: SOAP 1.1

Maximum Wait for WS Consumer: 0

- For issues with:
  - SAP Integration tenant Provisioning: Report under SAP component: LOD-HCI-PI-PRV
  - eInvoice: Report under SAP component: CA-GTF-CSC-EDO-IN-IV

- GSP system access: Report through GSP defined support mechanism

4.6 Basic Authentication Settings

To setup basic authentication, create service instance and service key as described in the link below.
https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/647eeb3eca5d4c299009cacd1332247e.html

Note:

If the service instance and service key is already created as a part of initial setup, this step is not required.

4.7 Client Certificate-based Authentication Settings

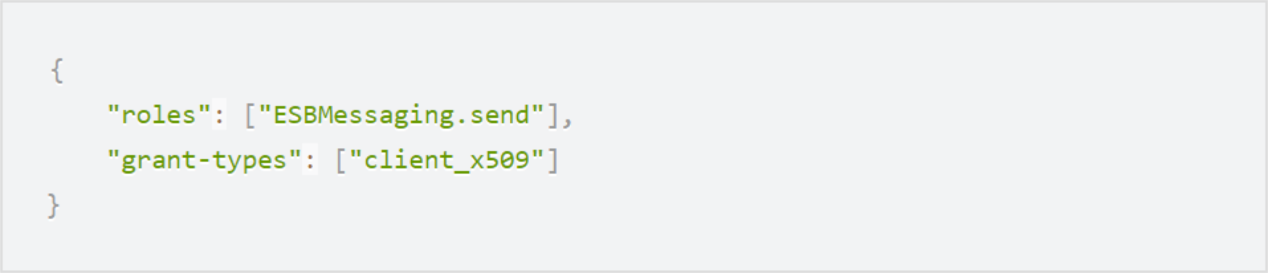
For client certificate-based authentication and authorization in SAP Integration Suite Tenant in Cloud Foundry (CF), the private key pair provisioned with the tenant (alias `sap_cloudintegrationcertificate`) needs to be available in the Keystore (this certificate exists in the tenant by default) and the client certificate used for the inbound call to SAP Integration needs to be maintained in the service key.

To enable certificate-based authentication between source system to SAP Integration Suite, the certificate presented by source system should be signed by one of the Certification Authorities (CA) approved by SAP BTP. Self-signed certificates cannot be used.

Refer to the below SAP help document on the list of supported CAs.
https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/4509f605e83c4c939a91b81eb3a6cdea.html

Details on setting up client certificate-based authentication in Cloud Foundry is as follows:

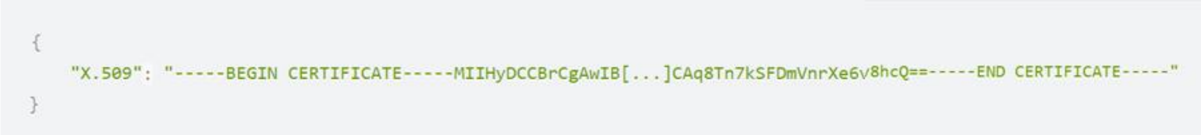
1. Download the client certificate corresponding to SSL client SSL standard PSE from strust.
2. When creating the service instance in CF, to enable client-certificate based authentication, specify “`client x509`” as the grant type.



```
{
    "roles": ["ESBMessaging.send"],
    "grant-types": ["client_x509"]
}
```

More details on creating service instances in Cloud Foundry can be found in the SAP online documentation at Creating a Service Instance in the Cloud Foundry Environment.

3. When creating the service key, provide a Name and in the Configuration Parameters, add the encoded client certificate (from step 1) in the following JSON format:



```
{
    "X.509": "-----BEGIN CERTIFICATE-----MIIHyDCCBrCgAwIB[...]CAq8Tn7kSFDmVnrXe6v8hcQ==-----END CERTIFICATE-----"
}
```

Note that the client certificate is a PEM-encoded X.509 certificate. Remove all line breaks, otherwise the user interface will not accept the entry.

More details on defining service keys in the Cloud Foundry environment can be found at Defining a Service Key for the Instance in the Cloud Foundry Environment.

5 Appendix

5.1 GSP Registration on IRP Portal

To access eInvoice APIs through GSPs, IRP expects taxpayers to register API Credentials per GSTIN for the specific GSP in the IRP portal.

1. For taxpayers already accessing E-way Bill production system via API.

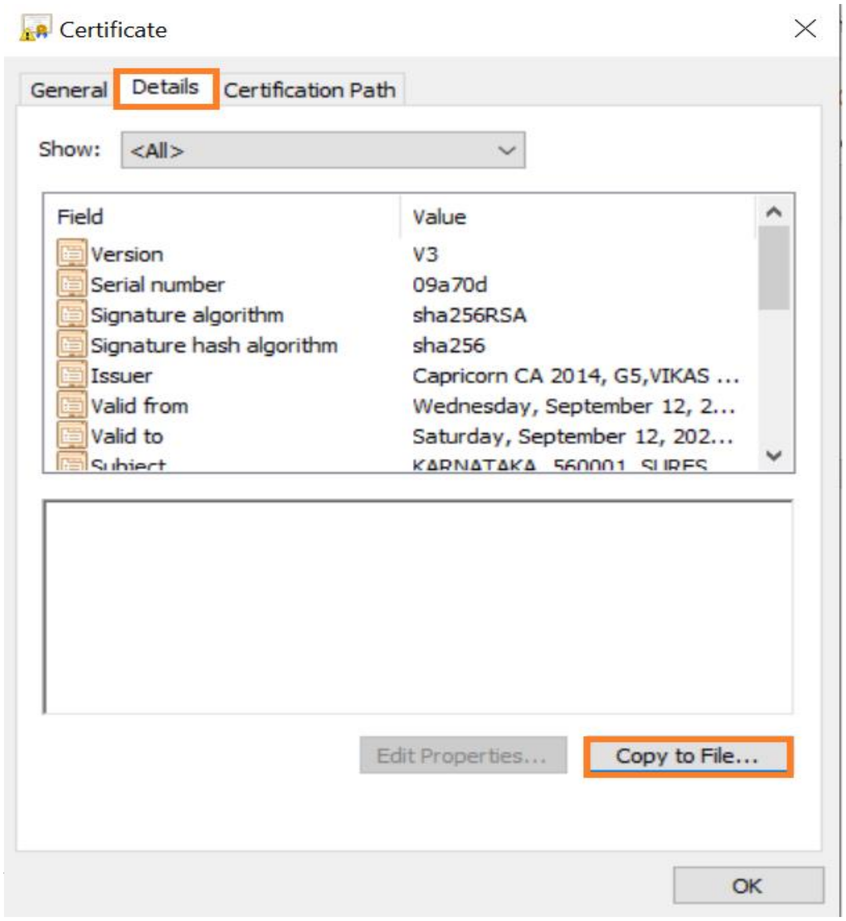
   The same Client Id and Client Secret, and Username and Password used for E-way Bill can be used for e-invoice APIs.

2. For taxpayers not accessing E-way Bill System via API:
   - Pre-requisite is to register GSTIN in eInvoice system
   - Login using registered credentials to get the API username and password

     Note: If pre-requisite is already done, then you can proceed with the login.

5.2 Exporting Certificate as Base-64 encoded X.509(.CER) format

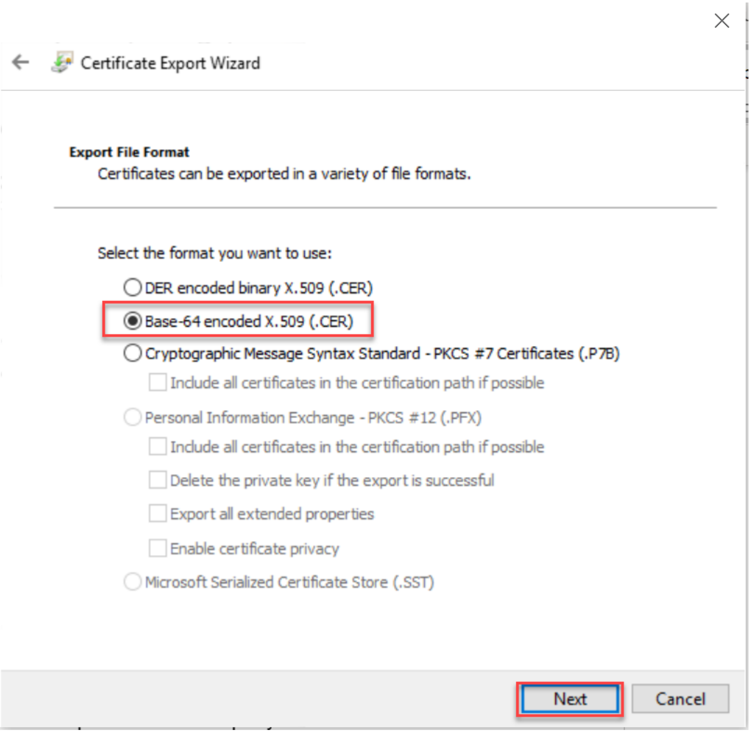
1. Double click the certificate saved in the local desktop. Go to Details -> Copy to File...
   A new window opens. Click **Next**.



Show: <All>

Field	Value
Version	V3
Serial number	09a70d
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Capricorn CA 2014, G5,VIKAS ...
Valid from	Wednesday, September 12, 2...
Valid to	Saturday, September 12, 202...
Subject	KARNATAKA, 560001, SURES

2. Select Base-64 encoded X.509(.CER) and click Next.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

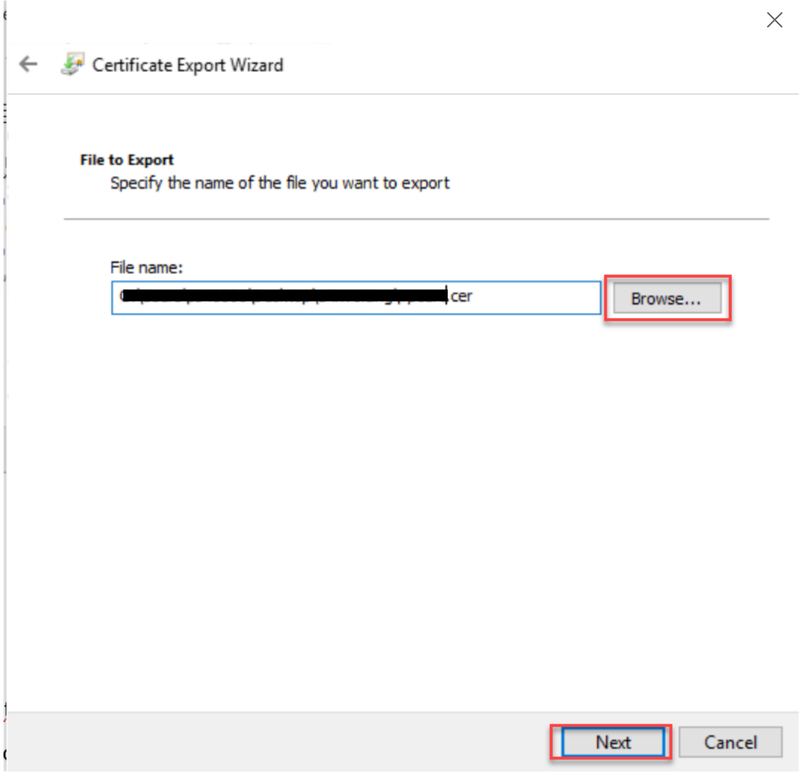
□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

3. Browse the path where the certificate must be saved and click next.



Certificate Export Wizard

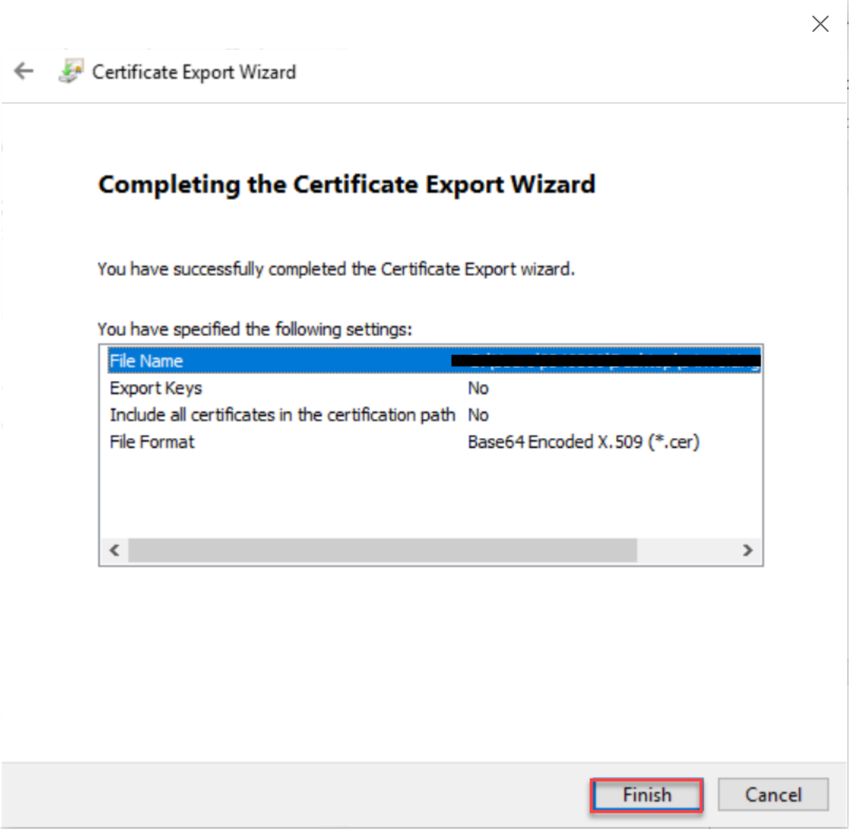
File to Export

Specify the name of the file you want to export

File name:

[redacted]cer

4. Click Finish. Certificate will be saved in the selected location.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	[redacted]
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

5.3 Useful links:

- SAP Integration Suite: https://help.sap.com/viewer/product/CLOUD_INTEGRATION/Cloud/en-US
- SAP Integration Suite – Overview of Authorization Groups:
  https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/4b4ba1c553474259b5be661f4ef0702c.html
- SAP Integration Suite – User Credentials: https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/6912d63bbbc64aee8bbd4ff10314c60c.html
- SAP Integration Suite – Importing a Keystore: https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/0db193a325a94675928e717c9310734a.html
- SAP Integration Suite – Importing a Certificate:
  https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/03cf78a217574e7abd75bfbba990c085.html