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

Via SAP Cloud Integration Service in Neo 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	2020-03-02	Created Section 4.1 'Base 64 encoded X.509(.cer) format conversion' in FAQ
1.2	2020-06-09	Updated Screenshots for section 3.2 'Deploy Integration Flow'
1.3	2020-09-23	• Updated section 3.2 Deploy Integration flow • Updated section 3.1 Certificate set-up and connection test. Added step 4 to Deploy IRP Signed Content Verification Public Key Certificate • Updated Section 4.4 Adding User Credentials to SAP Cloud Integration
1.4	2021-03-24	• Updated the complete document to reflect the latest SAP Branding changes for SAP Business Technology Platform(BTP), SAP Cloud Integration and Integration Flow. • Updated Section 3.2 'Deploy Integration Flow' with details on new field userGSTIN_publicAPI in step 4 'Deploying GSP Integration flow'.

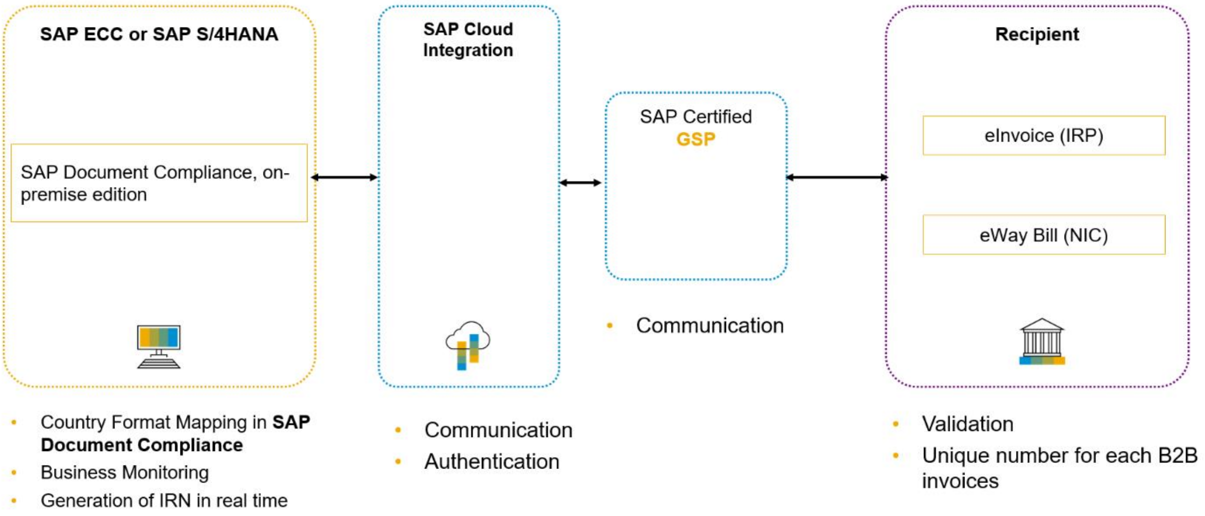
Contents

1 Introduction

Using the SAP Solution for eInvoice India, you can register the invoice with the Invoice Reference Portal (IRP) and subsequently generate Invoice Reference number (IRN) as per the legal requirement in India.

The eInvoice solution requires the integration between SAP Business Application (ERP/S4HANA) and GSPs. This document describes the steps to adapt and deploy the SAP Cloud Integration content flow to establish

the communication between SAP Business Application and GSPs.



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 Neo environment.

2 Prerequisites

Ensure the following prerequisites are met:

- SAP E-Invoice (EINV) for India solution is available in your landscape. For more information on installation and implementation, see SAP Note: 2884058
- Provisioned live SAP Cloud Integration production and/or pre-production tenants.
  - A sample of the URL's you'll need are:
    - Account URL: https://account.hana.ondemand.com
    - Web UI URL: https://xxx-tmn.avt.eu1.hana.ondemand.com/itspaces
    - Runtime URL: https://xxx-iflmap.avtsbhf.eu1.hana.ondemand.com
      Use your P-user or S-user credentials to login. If you get HTTP status 403 error, then send a mail to **service@sap.com**.
  - User role:
    - SAP Cloud Integration service user should have the ESBMessaging.Send role.
    - User should have AuthGroup.Administrator role to perform steps related to KeyStore, client certificate mapping and User credentials.
- For production access via GSP:
  Kindly contact GSP for Production access details.
- For sandbox access via GSP, request the IRP user credentials from GSP directly.
- Completed registration with GST Suvidha Provider (GSP) system and have received the following:
  - GST Suvidha Provider (GSP) integration/set up manual.
  - Trusted certificates from GSP for SSL handshake.
  - IRP public key certificate (SAP Cloud Integration expects the certificate in Base-64 encoded X.509 (.CER) format). See FAQ 4.1.
  - IRP signed content verification public key. (SAP Cloud Integration expects the certificate in Base-64 encoded X.509 (.CER) format). See FAQ 4.1.
  - IRP user credentials per GSTIN.
  - Other required technical details from GSP.
  - 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]

3 Establishing the connection between SAP Cloud Integration and GSP

This section details the procedure to establish a connection between SAP Cloud Integration and GSP (GST Suvidha Provider).

3.1 Certificate set-up and connection test

(only first-time activity or in case of changes in certificate from IRP/GSP)

1. Deploying SSL certificate:
   In the SAP Cloud Integration Web UI URL, go to **Monitor** > **Manage Security** > **Keystore** > **Add Certificate** (fill parameters here) > click **Deploy** > click **Ok**.

   > Note:
   >
   > To perform the above operation, you need to have the role as `AuthGroup.Administrator`. For more information, see FAQ 4.2.

2. Connection test (recommended):
   In the SAP Cloud Integration Web UI URL, go to **Monitor** > **Manage Security** > **Connectivity tests** > enter GSP base URL without https and port > click **Send**. On successful connection, system displays a successful response message. For more information, see FAQ 4.3.
3. Deploying IRP public key certificate:
   In the SAP Cloud Integration Web UI URL, go to **Monitor** > **Manage Security** > **Keystore** > **Add Certificate** > browse IRP public key certificate {the public key certificate must be converted to Base-64 encoded `X.509` (`.CER`) format as detailed in FAQ 4.1} > Enter alias name as **`irpcert`** > click **Deploy** > click **Ok**.
   For more information, see FAQ 4.2.
4. Deploying IRP signed content verification public key certificate:

   This Certificate is used to validate the signed content fields such as SignedQRCode and SignedInvoice received from IRP.
   In the SAP Cloud Integration Web UI URL, go to **Monitor** > **Manage Security** > **Keystore** > **Add Certificate** > browse IRP signed content verification public key certificate {the public key certificate must be converted to Base-64 encoded `X.509` (`.CER`) format as detailed in FAQ 4.1} > Enter alias name as **`jwtcert`** > click **Deploy** > click **Ok**.
   For more information, see FAQ 4.2.
5. Adding IRP user credentials as per GSTIN:

   In SAP Cloud Integration Web UI URL, go to **Monitor** > **Manage Security** > **Security Material** > **Add** > Click **User Credentials** (fill parameters here) > click **Deploy**.
   For more information, see FAQ 4.4.

Field	Description
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	User ID created in IRP portal (production) or received from GSP (pre-production)
Password/ Repeat password	Password

6. Deploying client certificate to SAP Cloud Integration (optional but highly recommended):
7. Download the client certificate from source system.

   Note:

   This option does not work with self-signed certificates. This certificate to user mapping functionality works only if there exists a certificate in the source system's trust store which is signed by one of the root CA's supported by SAP Cloud Integration.

   In the SAP Cloud Integration Web UI URL, go to **Monitor** > **Manage Security** > **Manage Certificate-to-User Mappings** > click **Add** > Add user name as SAP Cloud Integration user name (this user must have `ESBMessaging.Send` role assigned) and certificate as client certificate from the source system. For more information, see FAQ 4.6.

3.2 Deploy Integration Flow

1. Creating content package: (one-time activity)
   In the Web UI URL of the tenant, go to **Design** > **Create** > **In Header**, give a meaningful name (technical name), short 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 **Edit** button (seen in left side)
  - Go to **Artifacts** tab, checkmark the integration flow.
  - 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.
  - checkmark the integration flow, then click on action icon -> **Delete**.

  Note:

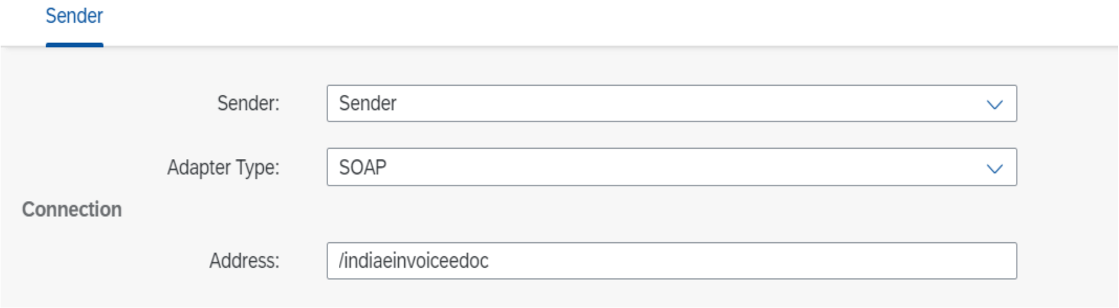
  Repeat this 'Updating content package' step for each of the router and GSP integration flows.

3. Deploying Router Integration flow:

1. Within the same content package, in artifacts tab, click **Add** > **Integration flow** > **Upload** > browse to the router integration flow (`.zip` file), give a name, description, sender, receiver > click **Ok**.

   Integration flow is successfully added.
2. Select the Router integration flow. System displays the integration flow screen.
3. To configure and deploy:

   In Artifacts screen, against the router integration flow, click **Actions** > **Configure** > verify the value as shown in the image below:



Sender

Connection

Sender: Sender

Adapter Type: SOAP

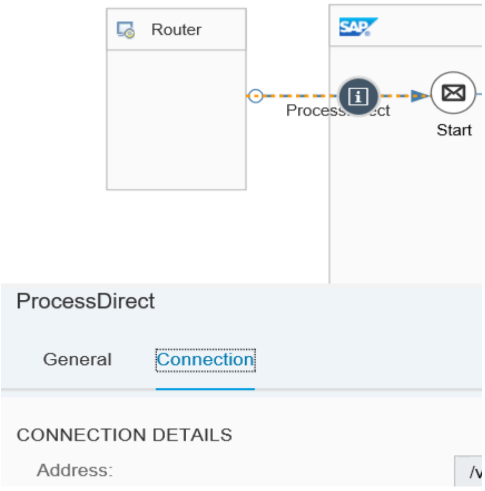
Address: /indiaeinvoiceedoc

4. Click **Save** then **Deploy**.

4. Deploying GSP Integration flow:

   1. In the content package, in **Artifacts** tab, click **Add** > **Integration flow** > **Upload** > browse to the GSP integration flow (.zip file), give a name, description, sender, receiver > click **Ok**. Now, integration flow is successfully added.

      Select the GSP integration flow. System displays the integration flow screen.



ProcessDirect

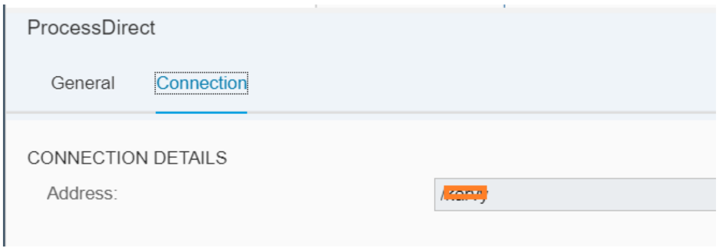
General Connection

CONNECTION DETAILS

Address: /v

For more information, see FAQ 4.5.

   2. Double click the **ProcessDirect** > **Connection Details** > **Address** > make note of this value (sample: /gsp)

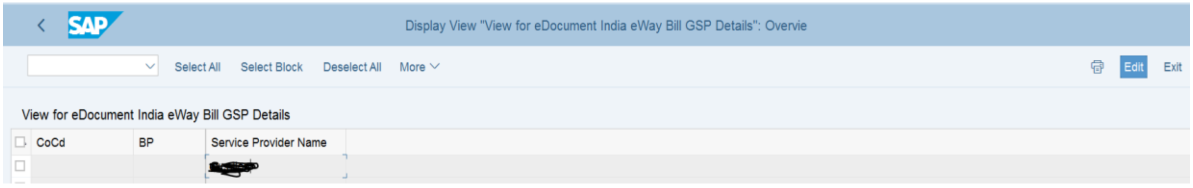


CONNECTION DETAILS

Address: [redacted]

Note:

You should enter the service provider name as same as the address value (without slash) in the business application > `sm30` > in view `EDOINEINVGSPV`



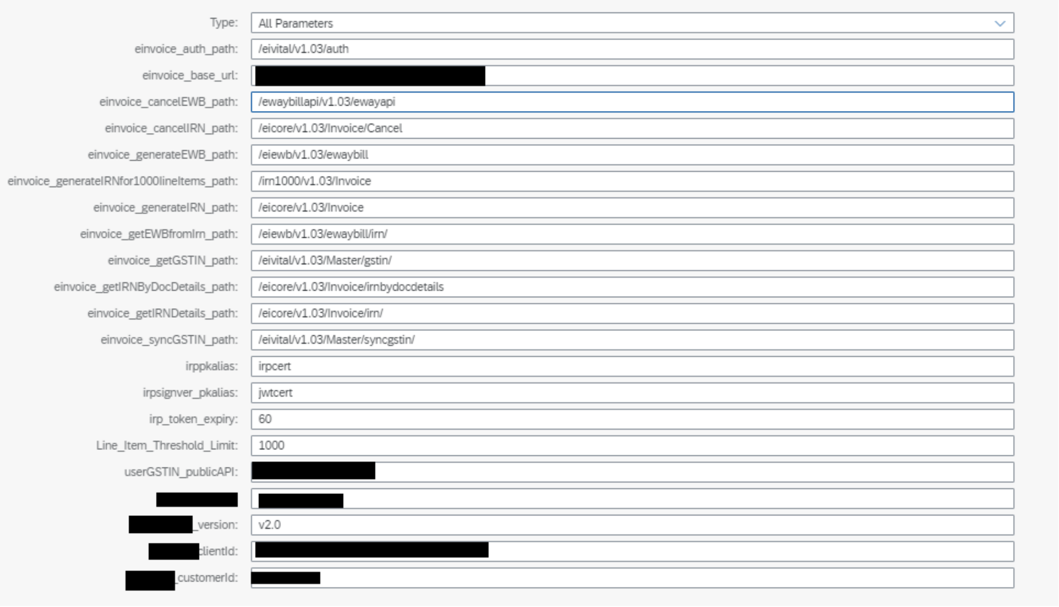
Display View "View for eDocument India eWay Bill GSP Details": Overvie

View for eDocument India eWay Bill GSP Details

CoCd	BP	Service Provider Name
		[redacted]

After that to configure and deploy:

In Artifacts screen, against the GSP integration flow, click **Actions** > **Configure** > Define the externalized parameters as provided by GSP to SAP customer. In case of updating the new integration flow, use the parameters copied as suggested in the step 2. After updating the parameters, click **Save** then **Deploy**.



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]

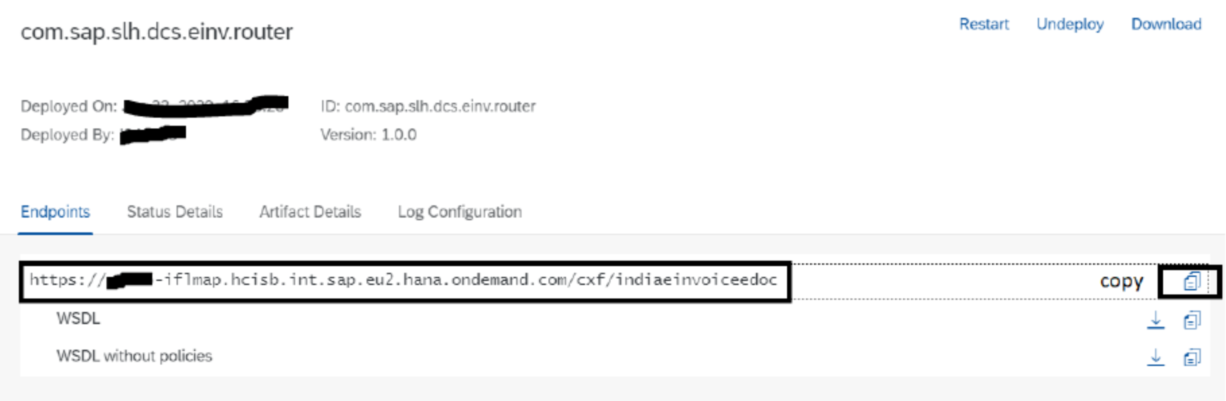
Note:

- `irppkalias` value is the same as the alias of the IRP public key certificate you deployed (irpcert).
- `irpsignver_pkalias` value is the same as the alias of the IRP signed content verification public key certificate you deployed (jwtcert).
- 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

Important:

- 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.

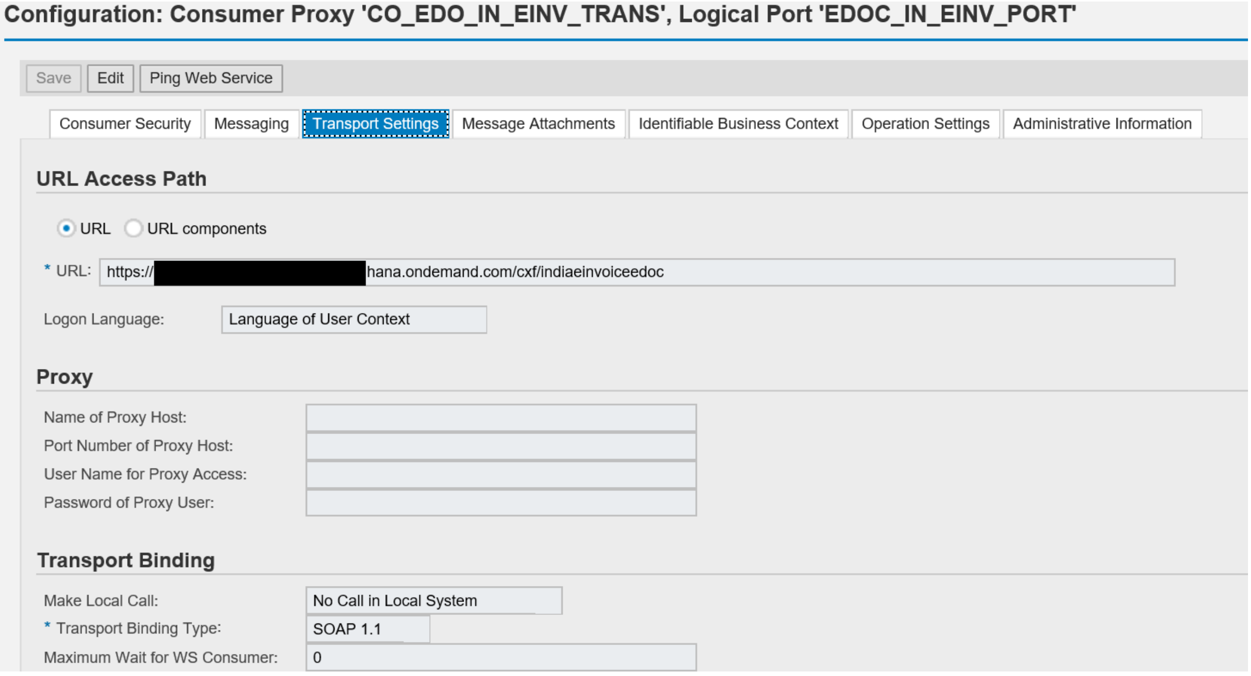


Deployed On: [redacted]
Deployed By: [redacted]

ID: com.sap.slh.dcs.einv.router
Version: 1.0.0

https://[redacted]-iflmap.hcisb.int.sap.eu2.hana.ondemand.com/cxf/indiaeinvoiceedoc

4. This URL has to 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

- Any issues with:
  - SAP Cloud Integration **tenant**: Report under SAP component: `LOD-HCI-PI-OPS`
  - **eInvoice**: Report under SAP component: CA-GTF-CSC-EDO-IN-IV

- **GSP system access**: Report through GSP defined support mechanism

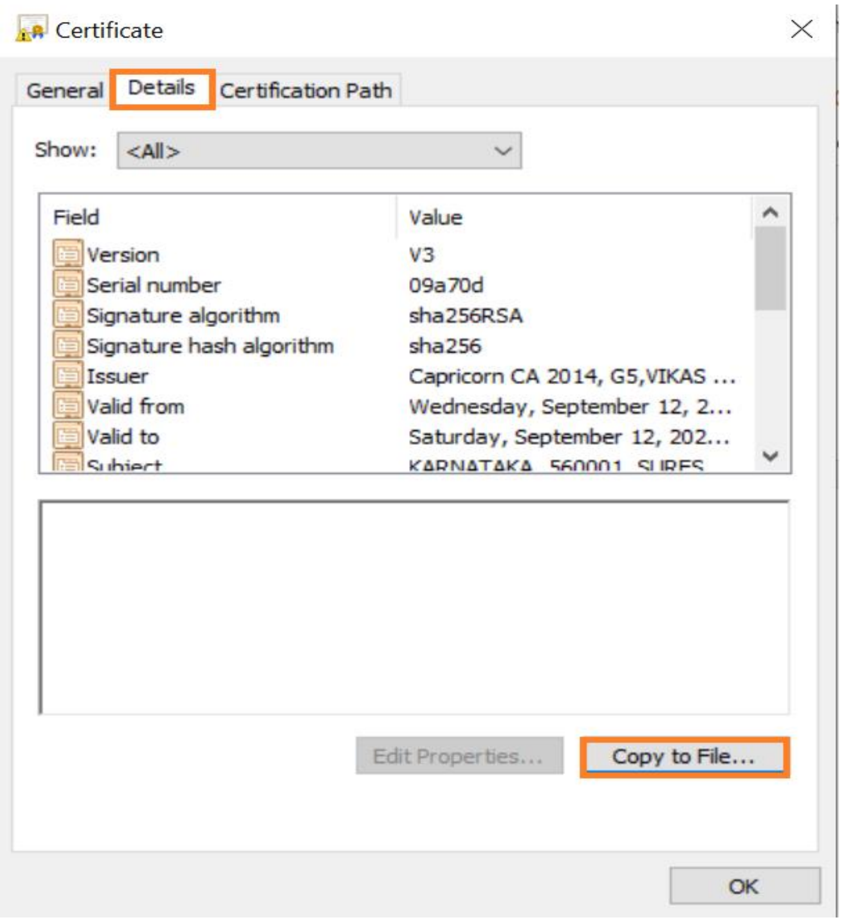
4 FAQs

4.1 Base-64 encoded X.509(.CER) format conversion

This conversion is relevant only for IRP public key certificate received from GSP.

To convert the IRP public key to Base-64 encoded X.509(.CER) format:

1. Double click the certificate saved in the local desktop. Go to **Details** -> **Copy to File...**

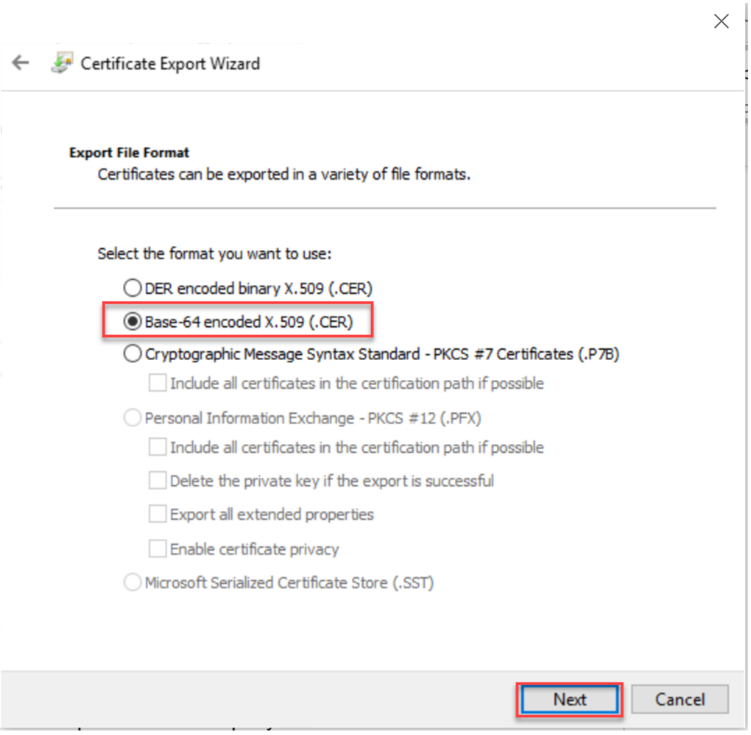


Show: <All>

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

A new window opens. Click **Next**.

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

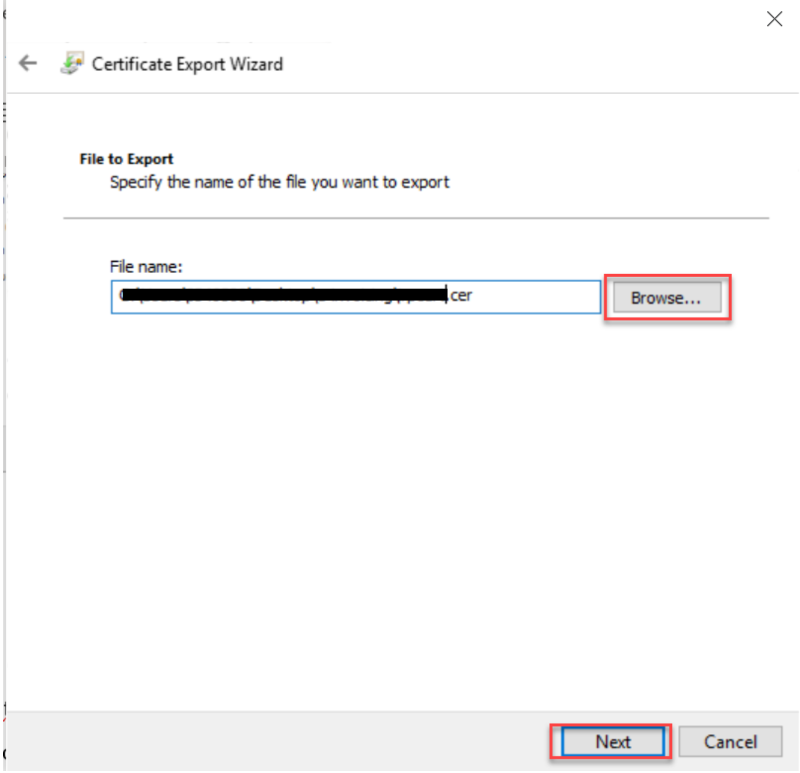
□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

3. Browse the path where the certificate has to be saved and click **Next**.



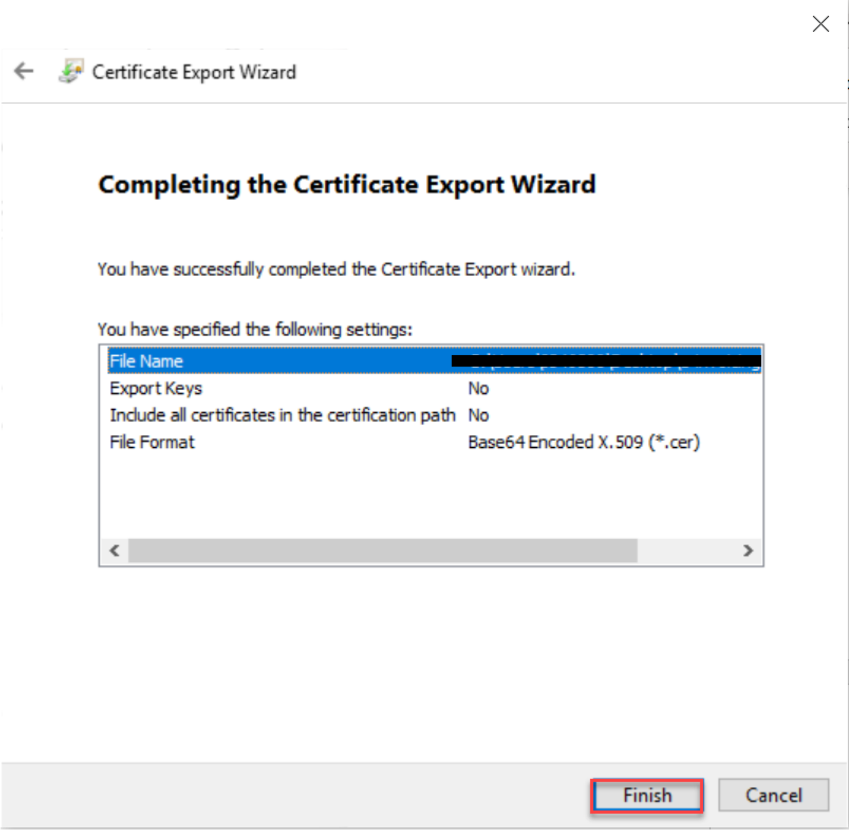
Certificate Export Wizard

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.



Certificate Export Wizard

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)

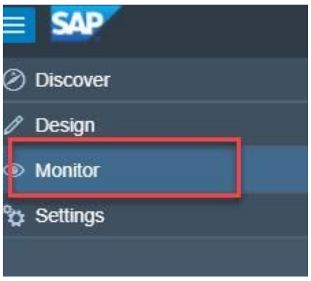
Add the above converted IRP public key certificate to SAP Cloud Integration.

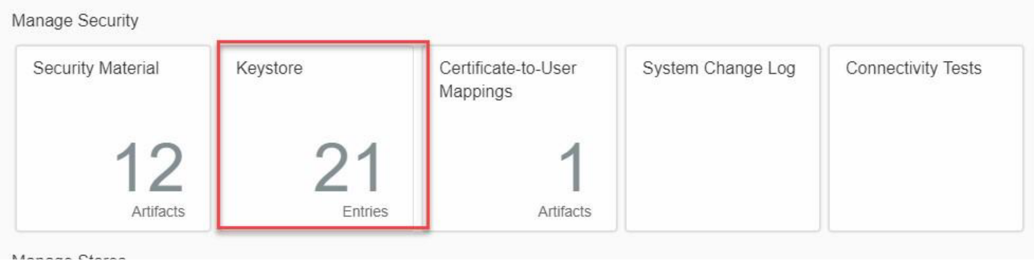
4.2 Adding New Certificates to the SAP Cloud Integration

You can add the security artifacts like keystore entries by following the process detailed here.

You should have Tenant Admin authorizations (AuthGroup.Administrator role) for the tenant to perform this operation.

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



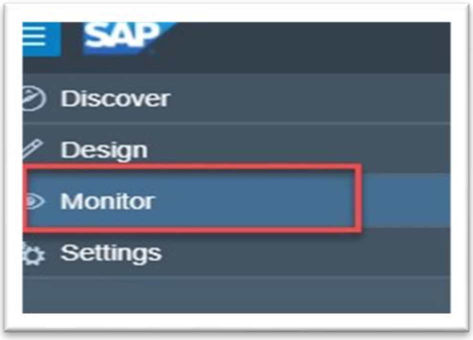


2. Click **Add** > **Certificate** > **Add Certificate**.
3. Enter an alias to identify the certificate. Browse the certificate from local desktop.
4. Click **Deploy**.

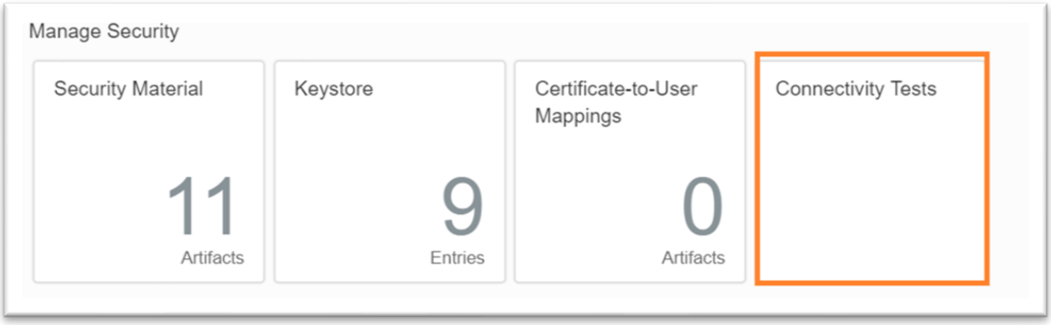
4.3 Connectivity Test

To check the connectivity with GSP, follow the steps:

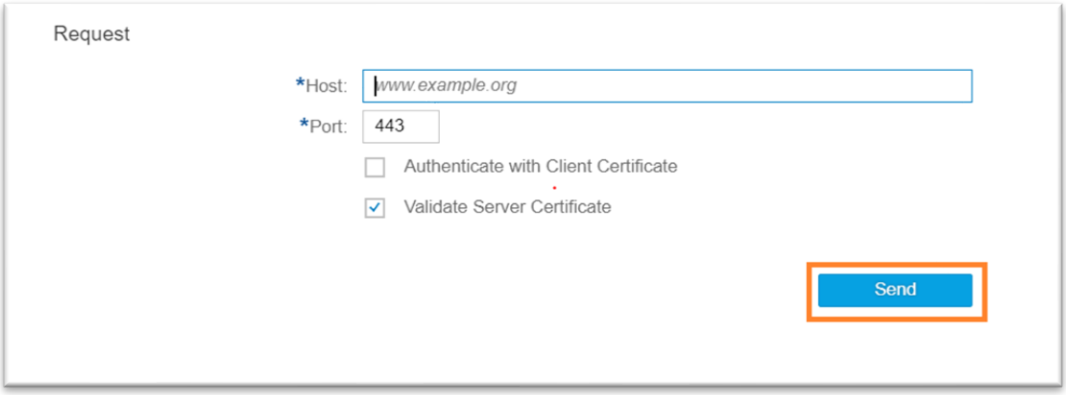
1. Go to **Monitor**



2. Choose **Manage Security** > **Connectivity tests**



3. Enter the host URL without any Protocols and enter the port number. Click **Send**.



Request

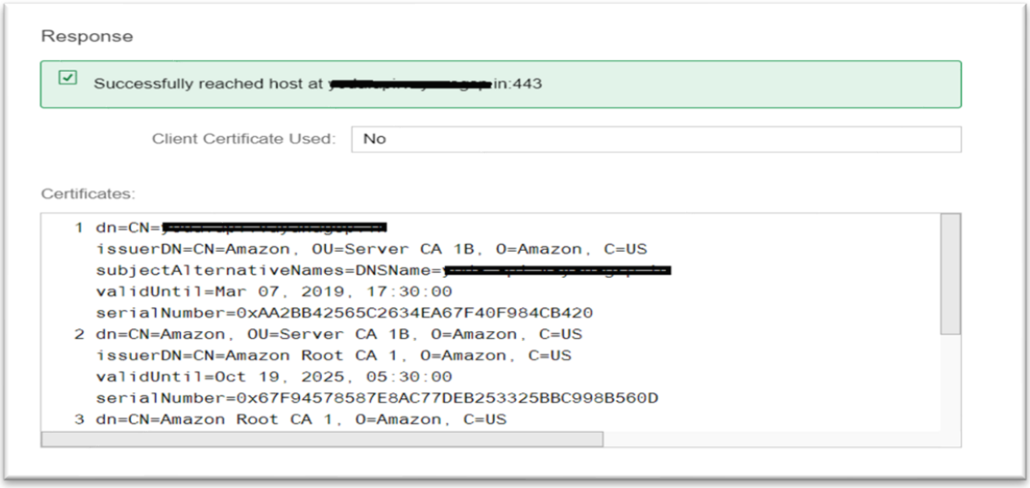
*Host: www.example.org

*Port: 443

☐ Authenticate with Client Certificate

☑ Validate Server Certificate

4. On successful connection, you can see a response as shown below:



Response

☑ Successfully reached host at [redacted]in:443

Client Certificate Used: No

Certificates:

```
1 dn=CN=[redacted]
  issuerDN=CN=Amazon, OU=Server CA 1B, O=Amazon, C=US
  subjectAlternativeNames=DNSName=[redacted]
  validUntil=Mar 07, 2019, 17:30:00
  serialNumber=0xAA2BB42565C2634EA67F40F984CB420
2 dn=CN=Amazon, OU=Server CA 1B, O=Amazon, C=US
  issuerDN=CN=Amazon Root CA 1, O=Amazon, C=US
  validUntil=Oct 19, 2025, 05:30:00
  serialNumber=0x67F94578587E8AC77DEB253325BBC998B560D
3 dn=CN=Amazon Root CA 1, O=Amazon, C=US
```

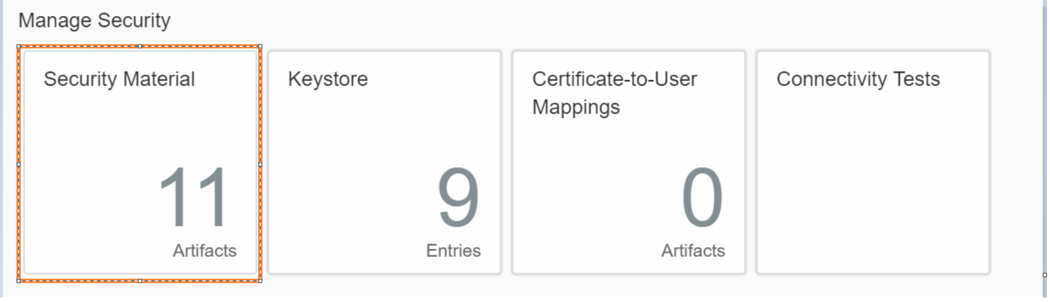
4.4 Adding User Credentials to SAP Cloud Integration

To add User Credentials (per GSTIN credentials provided by GSP/IRP) to SAP Cloud Integration:

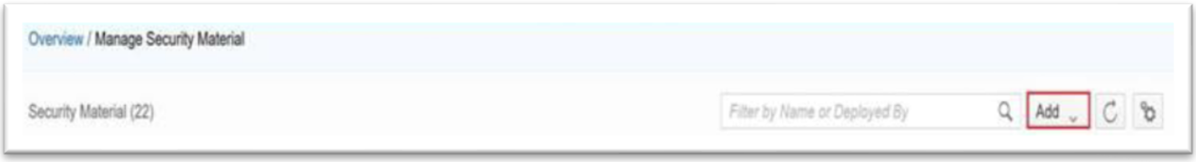
You register the user as per the business place specified in IRP. Use the following steps to add these IRP users in SAP Cloud Integration:

> Note:
>
> For the production system, if you are already using the eWay bill solution, then the user credentials need not be added again since the same credentials are valid for IRN (Invoice Registration Number) generation.

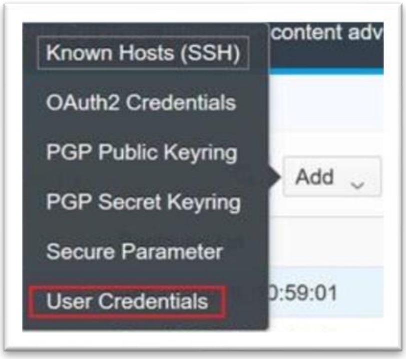
1. Go to Security material. Navigate to **Monitor** > **Manage Security** > **Security Material**.



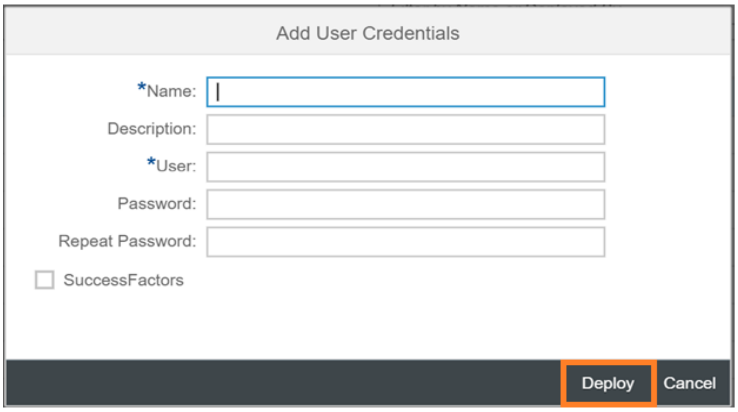
2. Add a new user credential.


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:

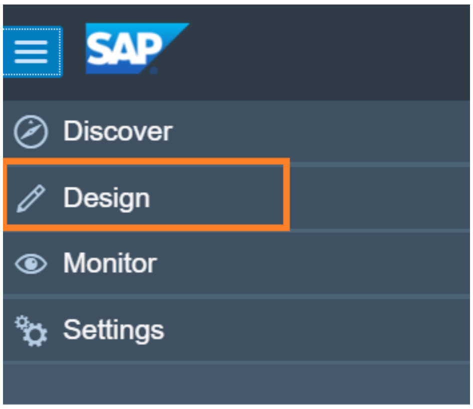
- In the Name field, enter the GSTIN of the business place to which the user belongs.
- In Production, IRP allows the existing eWay Bill API credentials to be used for eInvoice as well.
- However, if the user credentials are created explicitly for eInvoice, then, maintain the name field with the suffix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

Field	Description
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	User ID created in IRP portal (production) or received from GSP (pre-production)
Password/ Repeat password	Password

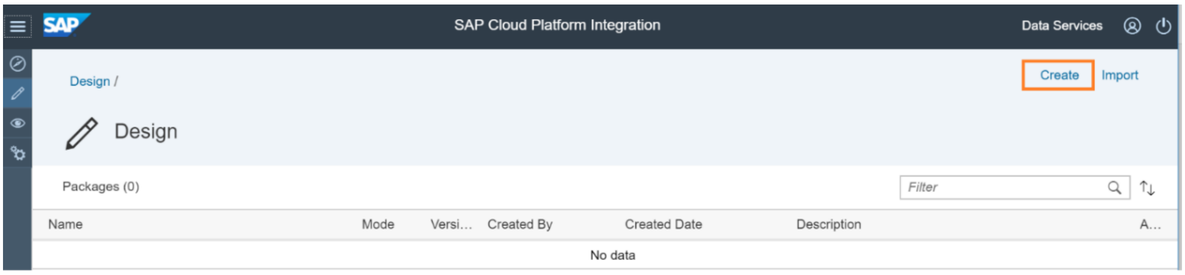
4.5 Creating content package and Deploying GSP Integration flow

4.5.1 To create a content package

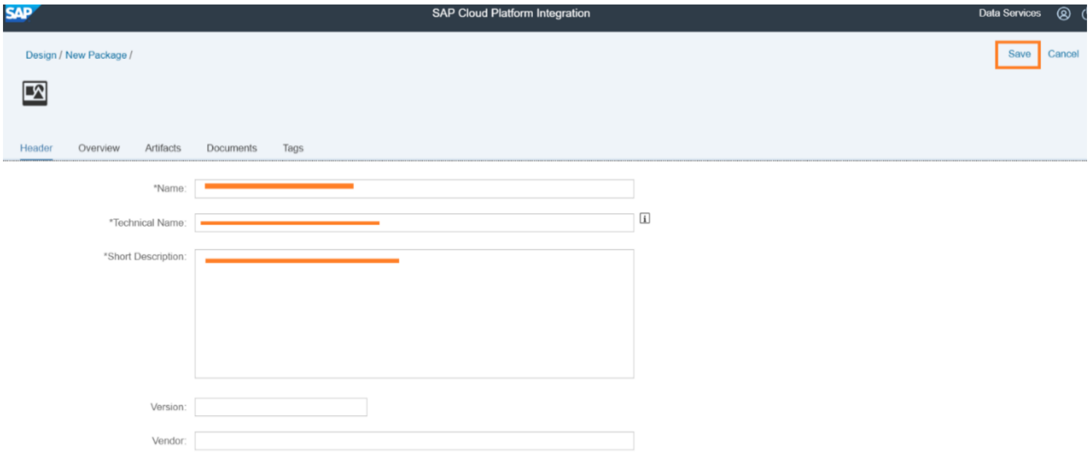
1. Go to **Design**.



2. Choose **Create**.

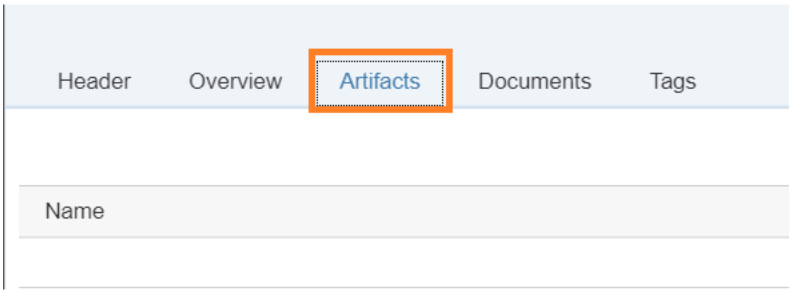


3. Enter appropriate Name and Description and click **Save**.

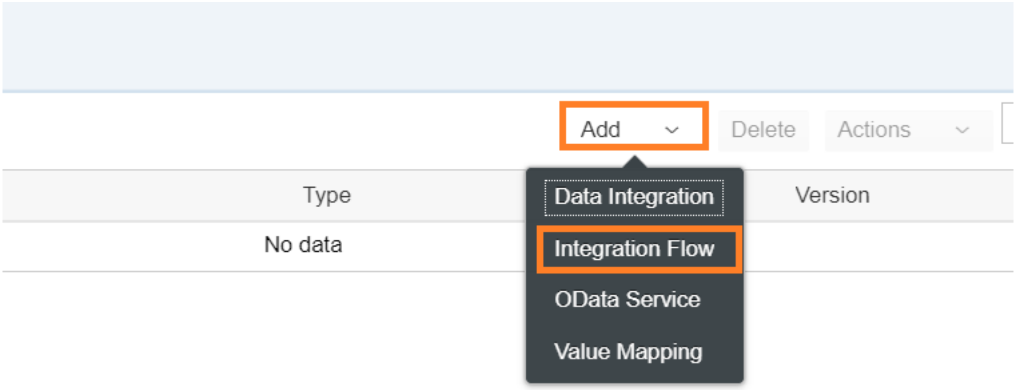


4.5.2 To deploy GSP Integration flow

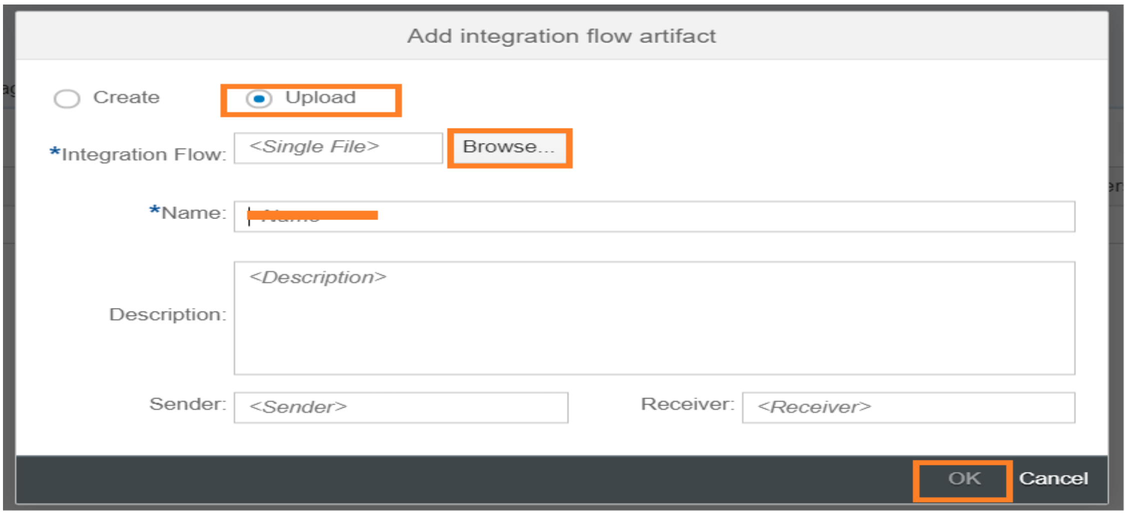
1. Choose **Artifacts**.



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:

Description: <Description>

Sender: <Sender> Receiver: <Receiver>

4.6 Deploying Client Certificate to SAP Cloud Integration

To enable certificate-based authentication between source system to SAP Cloud Integration, the certificate presented by source system should be signed by one of the Certification Authorities (CA) approved by SAP load balancer component.

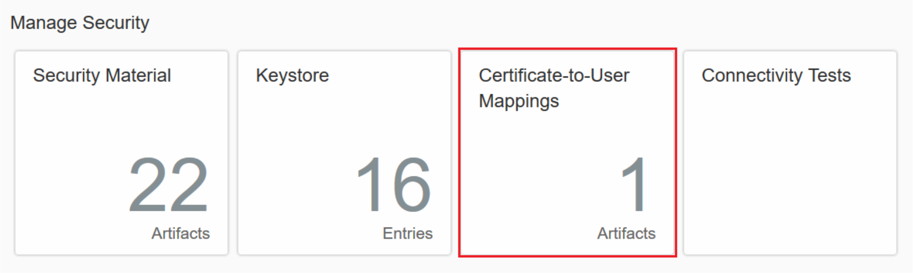
Refer to the below SAP help document on the list of supported CAs.

https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/4509f605e83c4c939a91b81eb3a6cdea.html

To deploy client certificate to SAP Cloud Integration, follow the steps:

For inbound HTTP connections to SAP Cloud Integration, you define Authorization options for the communication user associated with the sender system to define how it accesses the Cloud Integration components. We recommend that you use Client-Certificate with certificate-to-user mapping. Under this option, the authentication of a sender is performed based on a client certificate. With a certificate-to-user mapping, the certificate is mapped to a user, whose authorizations are checked on the tenant.

1. Navigate to **Monitor** > **Manage Security** > **Certificate-to-User Mappings**.



Manage Security

Security Material 22 Artifacts

Keystore 16 Entries

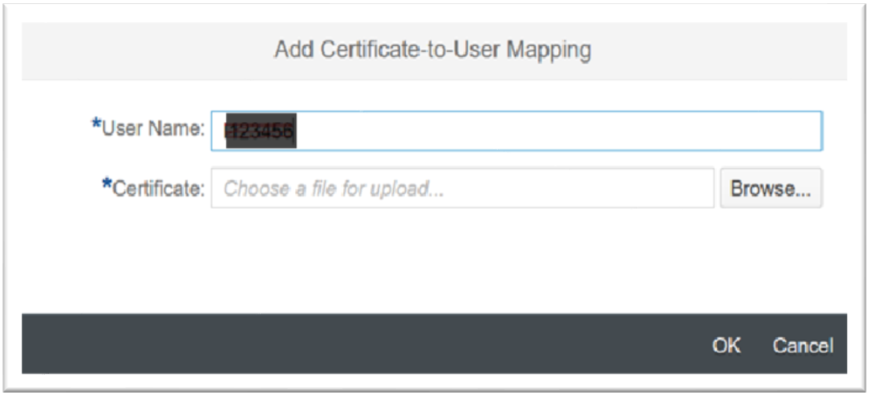
Certificate-to-User Mappings 1 Artifacts

Connectivity Tests

2. Click **Add**.
3. Enter the service user and deploy the client certificate obtained from SAP ERP.

   Note: the service user should have the `ESBMessaging.Send` role assigned to it.

   For more information on how to obtain client certificate from SAP ERP, refer the section ‘Configure Service Providers and Consumer Proxies’ in ‘SAP_Document_Compliance_e-Invoicing_for_India_Implementation_Guide’ document attached to SAP Note 2884058.



Add Certificate-to-User Mapping

*User Name: [redacted]

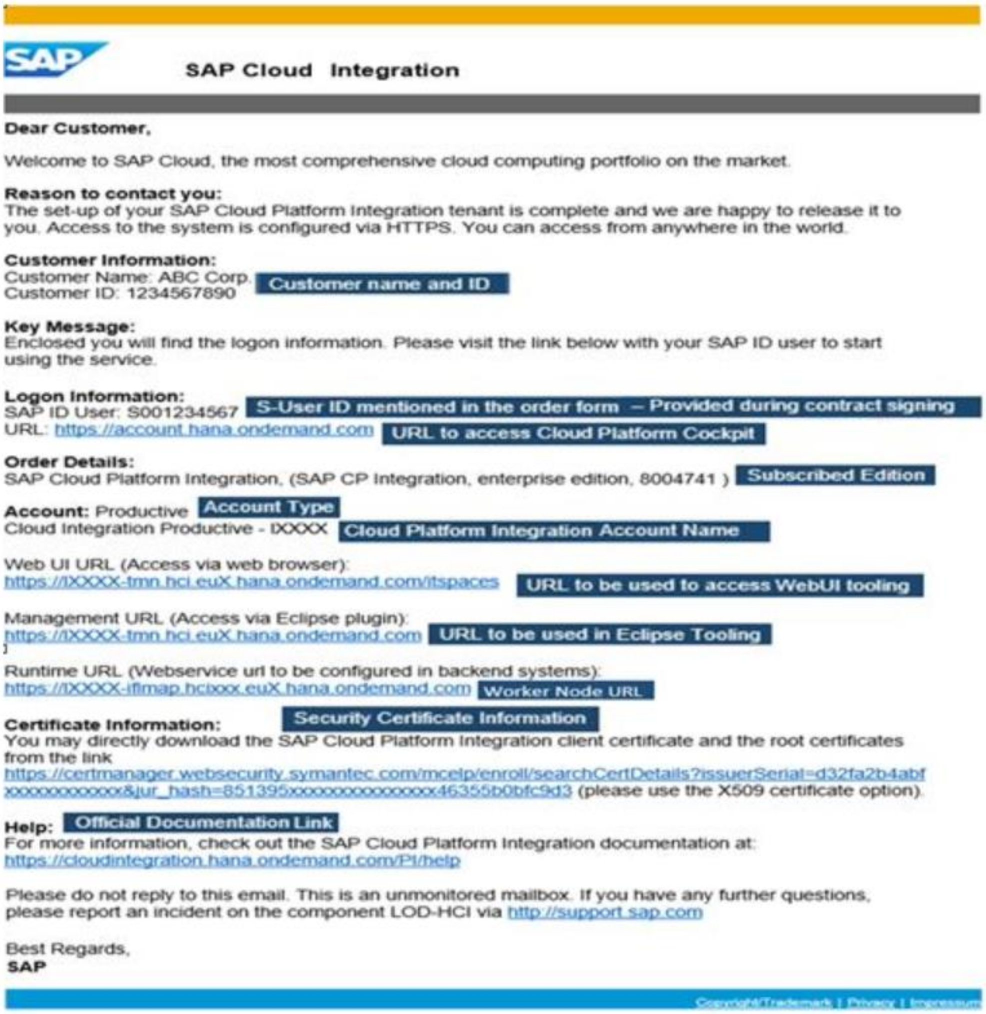
*Certificate: Choose a file for upload...

5 Appendix

5.1 About SAP Cloud Integration tenant

With SAP eInvoice solution, you get two Cloud Integration tenants. For each tenant, you get a welcome email outing the details about the tenant.

We recommend that you use one tenant for development/testing, and another for production.



SAP Cloud Integration

Dear Customer,

Welcome to SAP Cloud, the most comprehensive cloud computing portfolio on the market.

Reason to contact you:
The set-up of your SAP Cloud Platform Integration tenant is complete and we are happy to release it to you. Access to the system is configured via HTTPS. You can access from anywhere in the world.

Customer Information:
Customer Name: ABC Corp.
Customer ID: 1234567890

Key Message:
Enclosed you will find the logon information. Please visit the link below with your SAP ID user to start using the service.

Logon Information:
SAP ID User: S001234567
URL: https://account.hana.ondemand.com

Order Details:
SAP Cloud Platform Integration, (SAP CP Integration, enterprise edition, 8004741)

Account: Productive
Cloud Integration Productive - IXXXX

Web UI URL (Access via web browser):
https://IXXXX-tmn.hci.euX.hana.ondemand.com/itspaces

Management URL (Access via Eclipse plugin):
https://IXXXX-tmn.hci.euX.hana.ondemand.com

Runtime URL (Webservice url to be configured in backend systems):
https://IXXXX-iflmap.hcixxx.euX.hana.ondemand.com

Certificate Information:
You may directly download the SAP Cloud Platform Integration client certificate and the root certificates from the link
https://certmanager.websecurity.symantec.com/mcelp/enroll/searchCertDetails?issuerSerial=d32fa2b4abfxxxxxxxxxxxx&jur_hash=851395xxxxxxxxxxxxxx46355b0bfc9d3 (please use the X509 certificate option).

Help:
For more information, check out the SAP Cloud Platform Integration documentation at:
https://cloudintegration.hana.ondemand.com/PI/help

Please do not reply to this email. This is an unmonitored mailbox. If you have any further questions, please report an incident on the component LOD-HCI via http://support.sap.com

Best Regards,
SAP

Copyright/Trademark | Privacy | Impressum

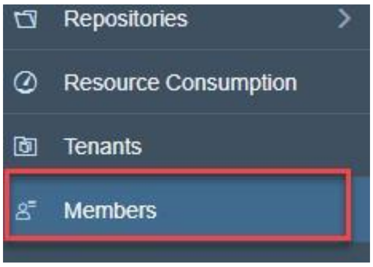
Customer name and ID
S-User ID mentioned in the order form – Provided during contract signing
URL to access Cloud Platform Cockpit
Subscribed Edition
Account Type
Cloud Platform Integration Account Name
URL to be used to access WebUI tooling
URL to be used in Eclipse Tooling
Worker Node URL
Security Certificate Information
Official Documentation Link

5.2 Adding Members to the SAP Cloud Integration Account

To add members to the SAP Cloud Integration account, follow the steps:

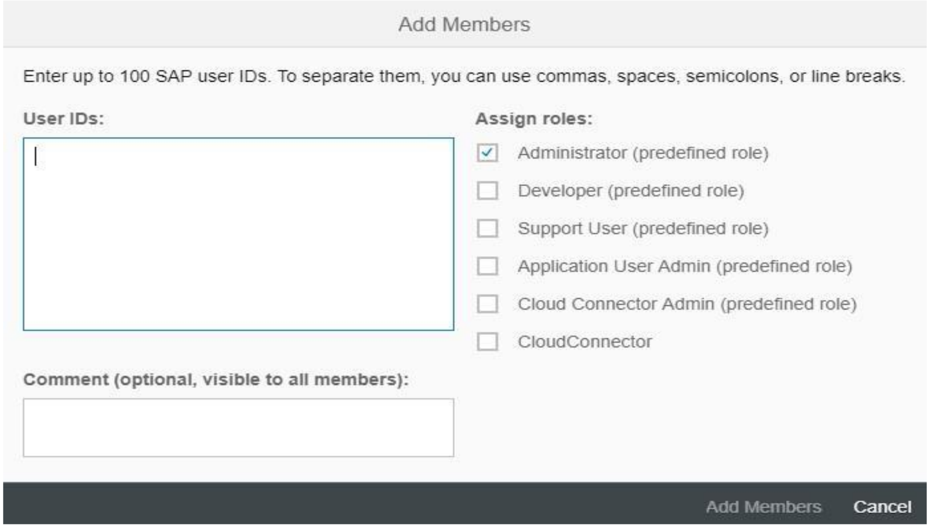
1. Logon to the Account URL with the SAP ID user provided in the mail.

2. Add members and assign roles to this account by navigating to **Members** > **Add Members**.



3. Assign the following roles:

- Administrator: Assign the role of Administrator to the user who is supposed to have the full permissions of an administrator.
- Application User Admin: Assign the role of Application User Admin to the user who is supposed to have restricted administrator privileges.



Add Members

Enter up to 100 SAP user IDs. To separate them, you can use commas, spaces, semicolons, or line breaks.

User IDs:

Assign roles:

☑ Administrator (predefined role)
□ Developer (predefined role)
□ Support User (predefined role)
□ Application User Admin (predefined role)
□ Cloud Connector Admin (predefined role)
□ CloudConnector

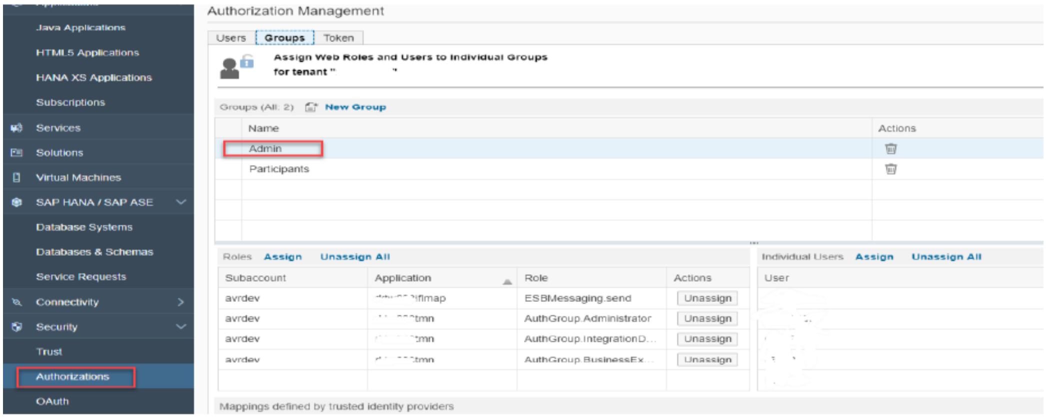
Comment (optional, visible to all members):

Add Members Cancel

5.3 Providing authorizations to SAP Cloud Integration Users

To provide authorizations to the SAP Cloud Integration Users:

1. Logon to the Account URL with the SAP ID user provided in the mail.
2. In the Navigation pane, choose **Security** > **Authorizations**
3. Create a Group and assign Roles and users for this Group.



Name	Actions
Admin	
Participants	

Subaccount	Application	Role	Actions
avrdev	[redacted]iflmap	ESBMessaging.send	Unassign
avrdev	[redacted]tmn	AuthGroup.Administrator	Unassign
avrdev	[redacted]tmn	AuthGroup.IntegrationD...	Unassign
avrdev	[redacted]tmn	AuthGroup.BusinessEx...	Unassign

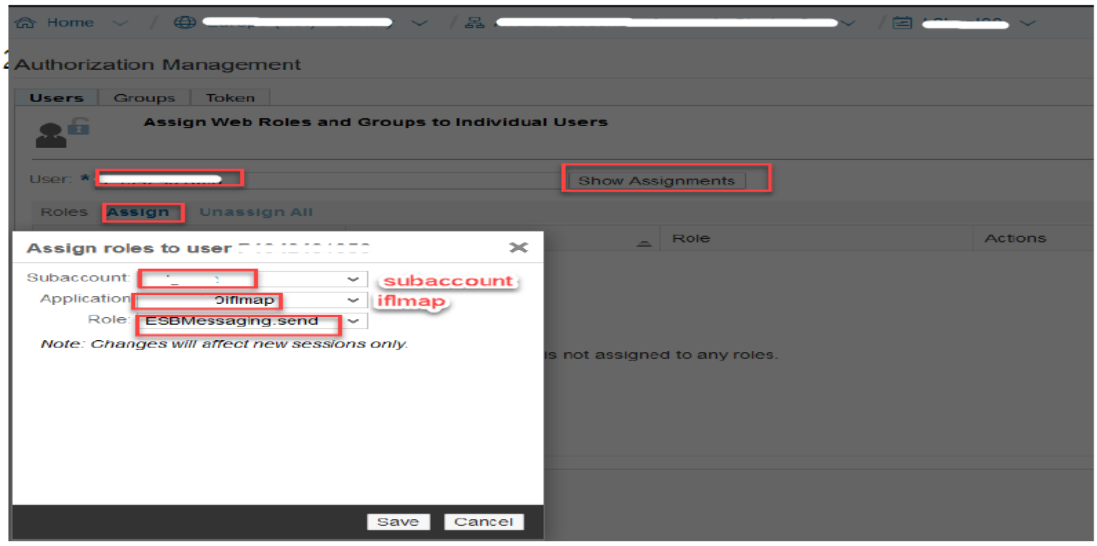
The authorization group `AuthGroup.Administrator` is designed for the administrator at customer side who administers a (customer-specific) tenant management node.

For more details refer here.

5.4 Creating a Service User in SAP Cloud Integration

To create a Service User in Cloud Integration, follow the steps:

1. Register a new user at https://account.hana.ondemand.com/#/home/welcome.
2. Assign the `ESBMessaging.Send` role to the user.



User: * [redacted]

Assign roles to user [redacted]

Subaccount: [redacted]

Application: [redacted]iflmap

Role: ESBMessaging.send

Note: Changes will affect new sessions only.

subaccount

iflmap

6 Useful links:

Area	Link
SAP Cloud Integration	https://help.sap.com/viewer/product/CLOUD_INTEGRATION/Cloud/en-US
SAP Cloud Integration – overview of authorization groups	https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/2937e5ca6ef448cfb21451a2461cc2a6.html
SAP Cloud Integration – user credentials	https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/6912d63bbbc64aee8bbd4ff10314c60c.html
SAP Cloud Integration – Importing a keystore	https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/0db193a325a94675928e717c9310734a.html
SAP Cloud Integration – Importing a certificate	https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/03cf78a217574e7abd75bfbba990c085.html