

**SAP e-Way bill for India - Integration with
GSP (GST Suvidha Provider)**

Via SAP Cloud Integration Service

in Neo environment

GSP Integration Set Up Guide

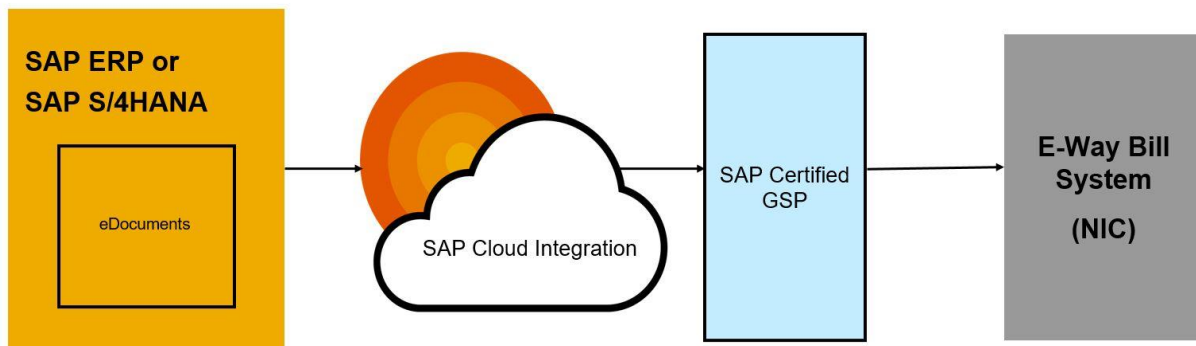
Contents

- 1. Introduction 3
- 2. Pre-requisites (only first-time activity)..... 3
- 3. Establishing the connection between SAP Cloud Integration and GSP 4
 - 1. Registering your Login Credentials for E-way Bill API 10
 - 3. Connectivity Test 12
 - 4. Adding User Credentials to SAP Cloud Integration..... 13
 - 5. Creating content package and Deploying GSP integration flow..... 15
- APPENDIX 18
 - About SAP Cloud Integration tenant..... 18
 - Adding Members to the SAP Cloud Integration Account 18
 - Providing authorizations to SAP Cloud Integration Users 19
 - Creating a Service User in SAP Cloud Integration 20

1. Introduction

Using the SAP Solution for eWay Bill India, you can generate eWay bill number as per the legal requirement in India.

The e-way bill solution requires the integration between SAP Business Application (SAP ERP or SAP S/4HANA) 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 e-Way Bill India integration for Neo environment.

2. Pre-requisites (only first-time activity)

Ensure the following prerequisites are met:

- SAP eWay bill for India solution is available in your landscape. For more information on installation and implementation, see SAP note: [2631687](#)
- 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:
 - I. Login to NIC web portal (<https://ewaybill.nic.in/>).
 - II. Go to Registration > For GSP.

The webpage displays your existing GSP if any login credentials were already created for API access through GSP. If not, continue the steps below.
 - III. Click the radio button Add/New.
 - IV. Choose your GSP name from dropdown list and input your user credentials in expected format.
 - V. Click Add to register your login credentials for E-way Bill API access through your GSP. For more information, see [FAQ 1](#).
- For sandbox access via GSP, request the NIC 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.
 - NIC public key certificate (SAP Cloud Integration expects the certificate in .CER format)
 - NIC 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 e-Way Bill request from SAP business application to specific GSP Integration Flow]

3. Establishing the connection between SAP Cloud Integration and GSP

3.1 Certificate set-up and connection test (only first-time activity or in case of changes in certificate from NIC/GSP)

The following steps details the procedure to establish a connection between SAP Cloud Integration and GSP:

- a. 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 2](#).

- b. 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 3](#).

- c. Deploying NIC public key certificate:
In the SAP Cloud Integration Web UI URL, go to **Monitor > Manage Security > Keystore > Add Certificate** > browse NIC public certificate (certificate should be in .CER format) > Enter alias name as niccert > click **Deploy** > click **Ok**.

For more information, see [FAQ 2](#).

- d. Adding NIC 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](#).

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

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

3.2 Deploy Integration Flow

3.2.1 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.

3.2.2 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, checkmark the integration flow,
 - Then 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.

3.2.3 Deploying Router integration flow

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

Integration flow is successfully added.

- b. Select the Router integration flow. System displays the integration flow screen.

- c. To configure and deploy:

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

The screenshot shows a configuration form for an integration flow. At the top, there is a tab labeled "Sender". Below it, there are three fields:

- Sender:** A dropdown menu with "Sender" selected.
- Adapter Type:** A dropdown menu with "SOAP" selected.
- Address:** A text input field containing the value "/indiaewaybilledoc".

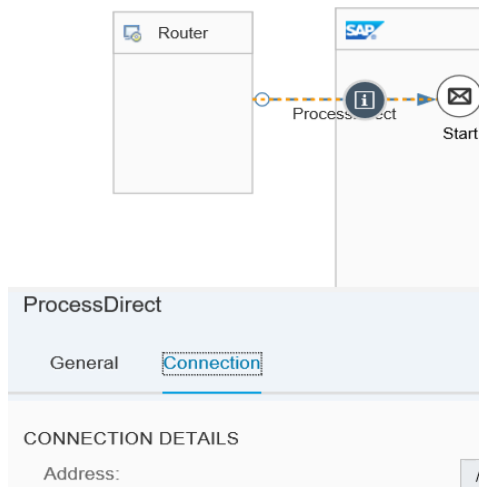
The section is titled "Connection" on the left side.

- d. Click **Save** then **Deploy**.

3.2.4 Deploying GSP integration flow:

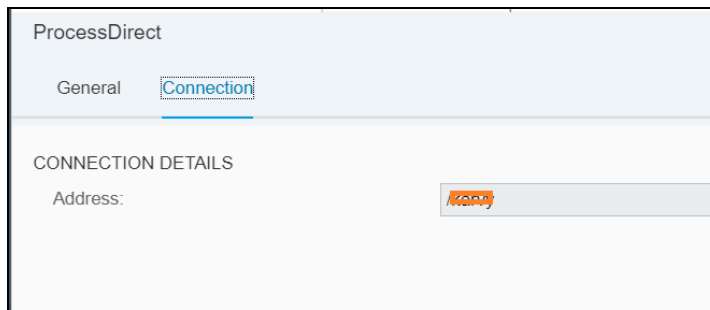
In the content package, in **Artifacts** tab, click **Add > Integration flow** > choose **Upload** > browse to the GSP integration flow (.zip file), give a name, description, sender, receiver → click **Ok**. Now, integration flow is successfully added.

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



For more information, see [FAQ 5](#).

Double click the **processdirect > connection details > address** > make note of this value (sample: /gsp)



Note: You should enter the service provider name as same as the address value (without slash) in the business application > sm30 > in view EDOINEWBGSPV.

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 3.2.2. After updating the parameters, click **Save** then **Deploy**.

Integration Flow	
Name	Value
<gsp>_auth_url	<auth_url_shared_by_gsp>
<gsp>_client-secret	<clientSecret_shared_by_gsp>
<gsp>_clientid	<clientId_shared_by_gsp>
<gsp>_ewaybill_url	<url_shared_by_gsp>
<gsp>pkalias	[REDACTED]
nic_token_expiry	300
nicpkalias	<NIC_public_key_alias>

Note: NIC public key alias value is the same as the alias of the NIC public key certificate you deployed (niccert).

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 :
 - I. Click **Monitor > Manage integration content**
 - II. Choose the Router Integration flow.
 - III. The EndPoint URL can be found on the right side of the page.

Router
Restart Undeploy ...

Deployed On: [REDACTED] ID: com.sap.slh.dcs.ewb.router

Deployed By: [REDACTED] Version: 1.0.0

Endpoints
Status Details
Artifact Details
Log Configuration

https://[REDACTED]
if1map.hcisbp.eu1.hana.ondemand.com/cxf/indiaewaybill11edoc Copy

WSDL ↓

WSDL for ABAP consumer ↓

WSDL without policies ↓

IV. This URL has to be configured in the SOA Manager.

New Manual Configuration of Logical Port for Consumer Proxy 'CO_EDO_IN_EWB_TRANS

1 Logical Port Name 2 Consumer Security **3 HTTPSettings** 4 SOAP Protocol 5 Identifiable Business Context 6 Operation

Back Next Finish Cancel

URL Access Path

Complete URL URL components

* URL: http://[REDACTED]

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

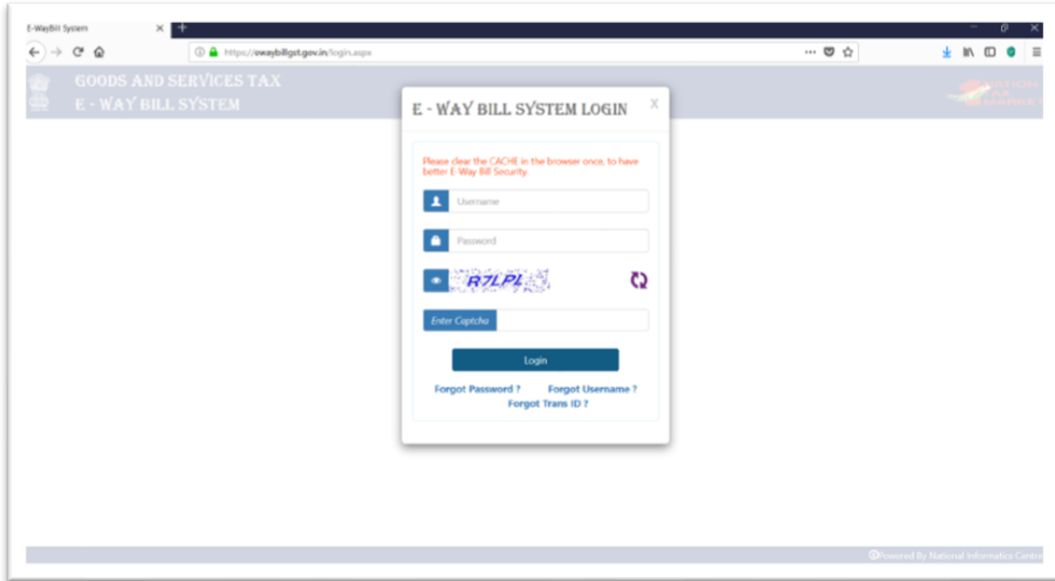
- Any issues with:
 - **SAP Cloud Integration tenant:** Report under SAP component: LOD-HCI-PI-OPS
 - **EWB:** Report under SAP component: XX-CSC-IN-EWB
 - **GSP system access:** Report through GSP defined support mechanism

FAQs:

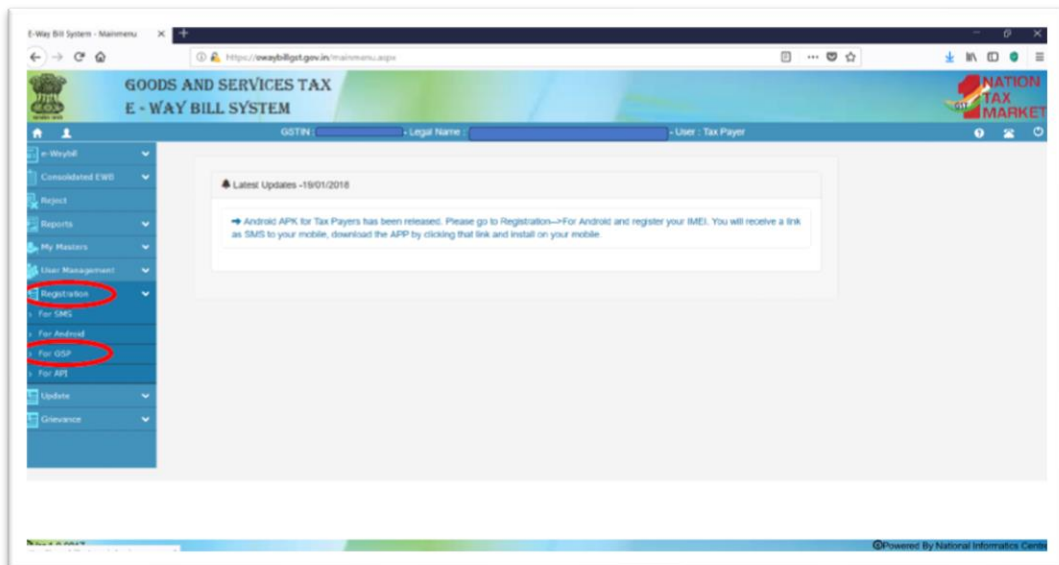
1. Registering your Login Credentials for E-way Bill API

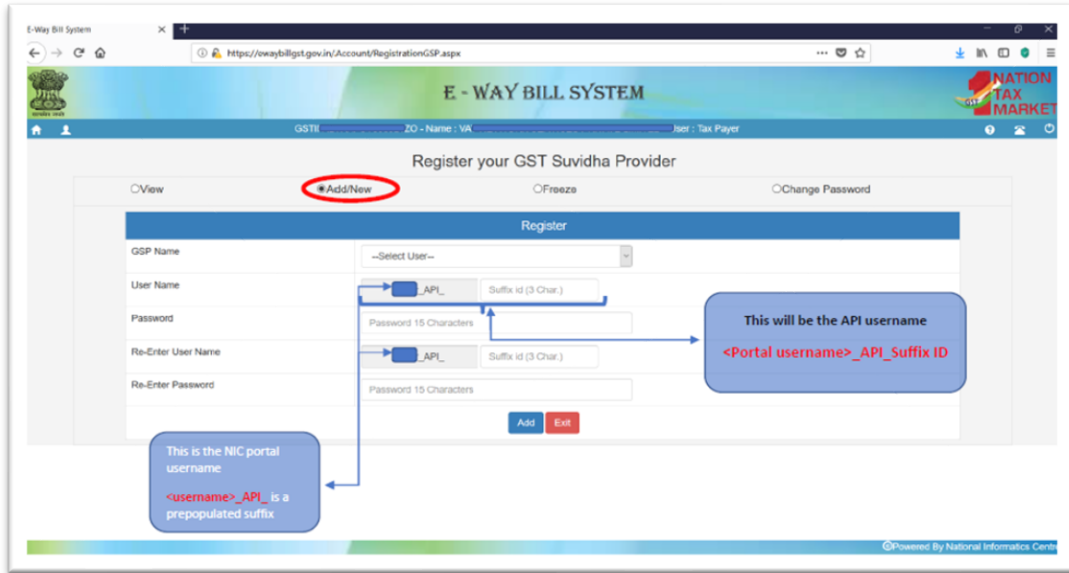
To register your login credentials for E-way Bill API, access through GSP in NIC portal.

- a. Customer must login to NIC web portal (<https://ewaybill.nic.in/>).



- b. Go to Registration > For GSP > The webpage shall now display your existing GSP (if any login credentials were already created for API access through GSP). If not, click Add/New. Choose your GSP name from dropdown list and input your user credentials in the expected format. Click Add to register your login credentials for E-way Bill API access through your GSP.



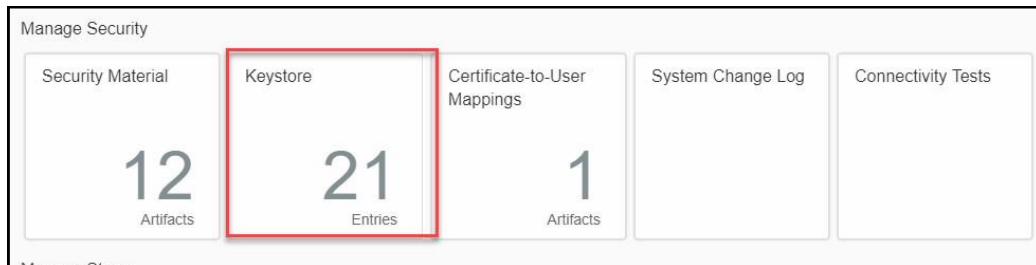
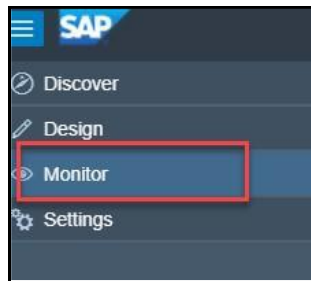


2. Adding New Certificates to the SAP Cloud Integration

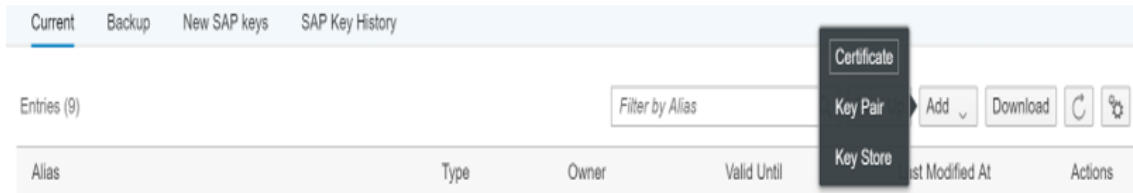
You can add the security artifacts like keystore entries by following the process detailed [here](#).

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

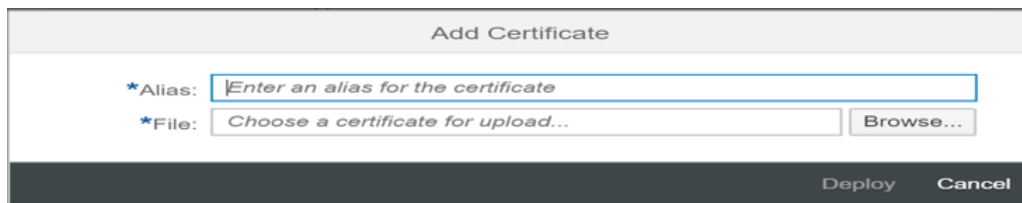
- a. Navigate to **Monitor > Manage Security > Keystore**.



- b. Click **Add > Certificate > Add Certificate**.



- c. Enter an alias to identify the certificate. Browse the certificate from local desktop.

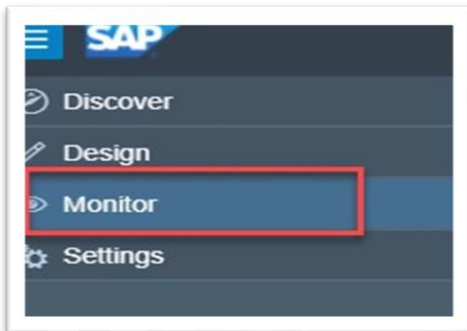


- d. Click **Deploy**.

3. Connectivity Test

To check the connectivity with GSP, follow the steps:

- a. Go to **Monitor**



- b. Choose Manage Security > Connectivity tests

Manage Security

Security Material 11 Artifacts	Keystore 9 Entries	Certificate-to-User Mappings 0 Artifacts	Connectivity Tests
---	---------------------------------	---	--------------------

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

Request

*Host:

*Port:

Authenticate with Client Certificate

Validate Server Certificate

Send

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

Response

Successfully reached host at **www.example.org** in:443

Client Certificate Used:

Certificates:

```

1 dn=CN=www.example.org
 issuerDN=CN=Amazon, OU=Server CA 1B, O=Amazon, C=US
 subjectAlternativeNames=DNSName=www.example.org
 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

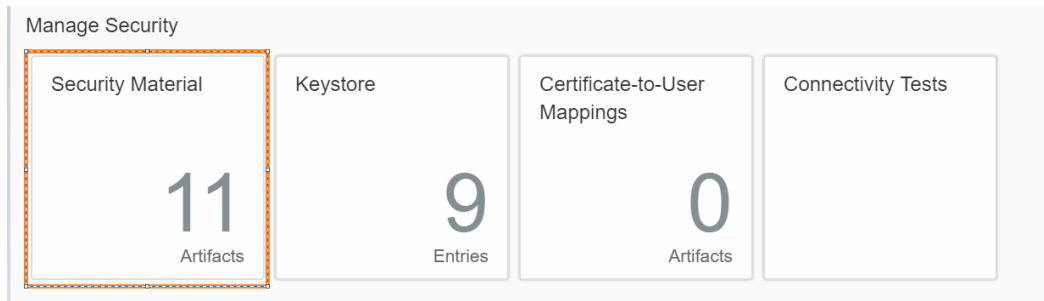
```

4. Adding User Credentials to SAP Cloud Integration

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

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

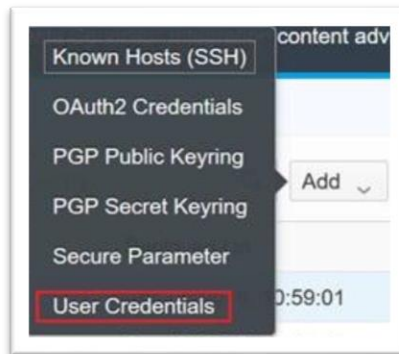
- a. Go to Security material. Navigate to **Monitor > Manage Security > Security Material**.



- b. **Add** a new user credential.



- c. Click **User Credentials**.



- d. **Add** and **Deploy** the user credentials.

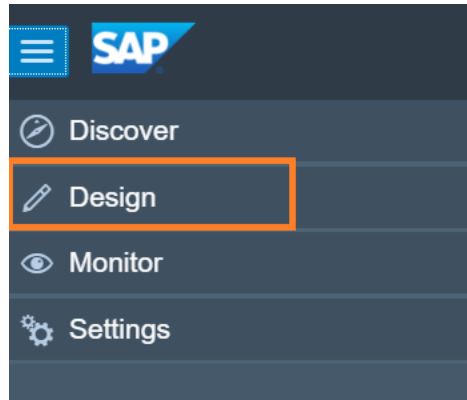
The screenshot shows the 'Add User Credentials' form. It includes fields for Name, Description, User, Password, and Repeat Password. There is a checkbox for SuccessFactors. The 'Deploy' button is highlighted with an orange border.

Note: in the Name field, enter the GSTIN of the business place to which the user belongs.

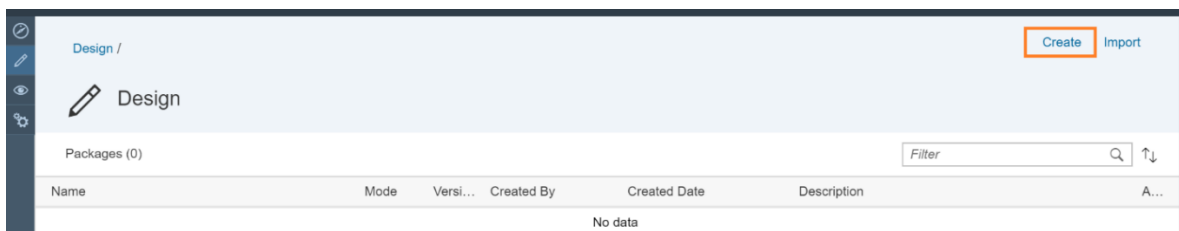
5. Creating content package and Deploying GSP integration flow

To create a content package, follow the steps:

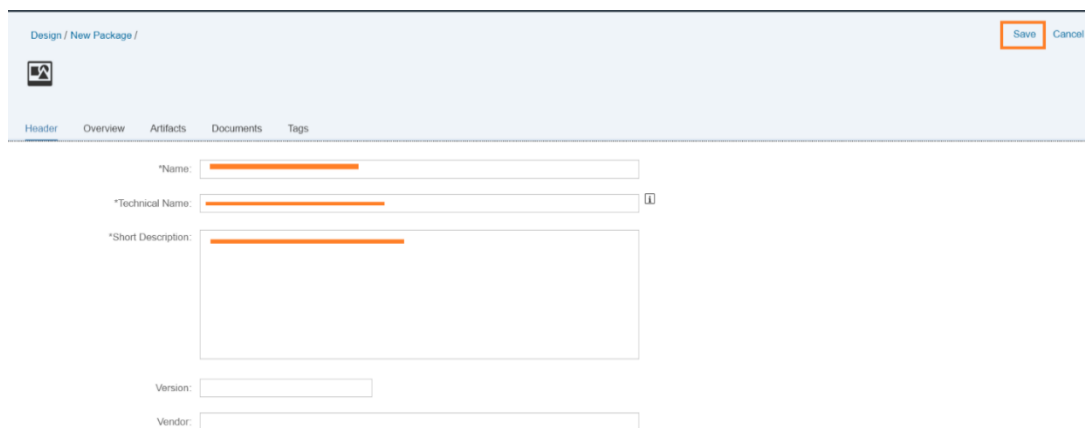
- a. Go to **Design**.



- b. Choose **Create**.

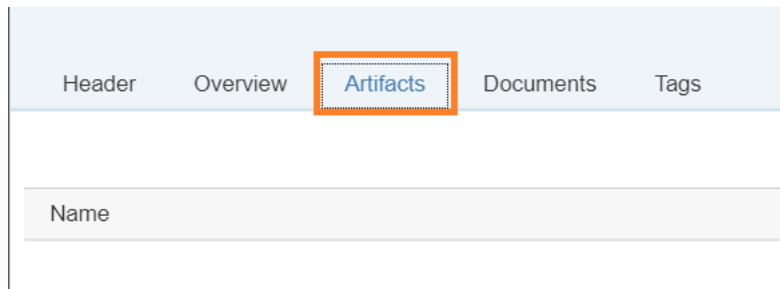


- c. Enter appropriate **Name** and **Description** and click **Save**.

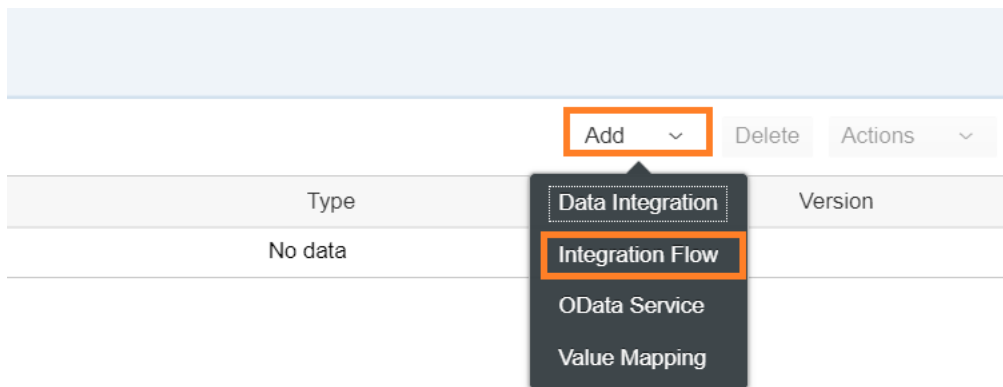
A screenshot of the SAP Design 'New Package' form. The form is titled 'Design / New Package /' and has a 'Save' button highlighted with an orange border. The form has tabs for 'Header', 'Overview', 'Artifacts', 'Documents', and 'Tags'. The 'Header' tab is selected. The form contains several input fields: '*Name:' (with an orange underline), '*Technical Name:' (with an orange underline and a small icon), '*Short Description:' (with an orange underline), 'Version:', and 'Vendor:'. The 'Name' and 'Short Description' fields are currently empty.

To deploy GSP integration flow, follow the steps:

a. Choose **Artifacts**.



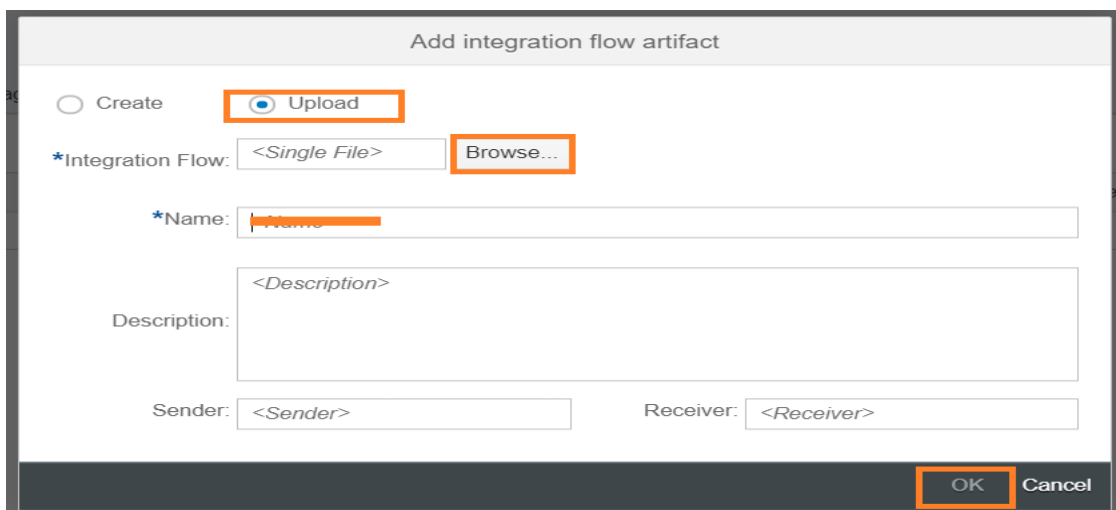
b. Click **Add** and choose **Integration Flow**.



c. Select **Upload**.

d. Browse for the appropriate Integration flow (.zip file)

e. Enter the **Name** and **Description** and click **Ok**.

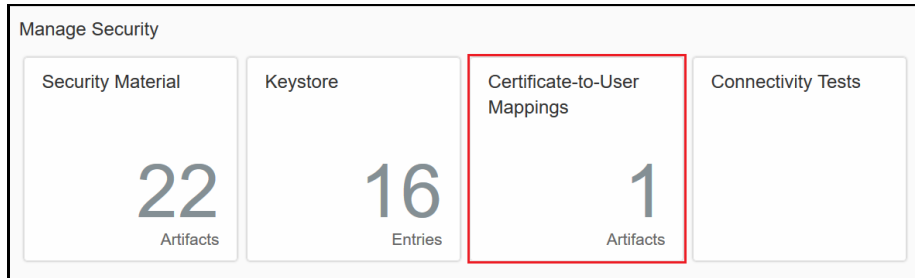


6. Deploying Client Certificate to SAP Cloud Integration

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.

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

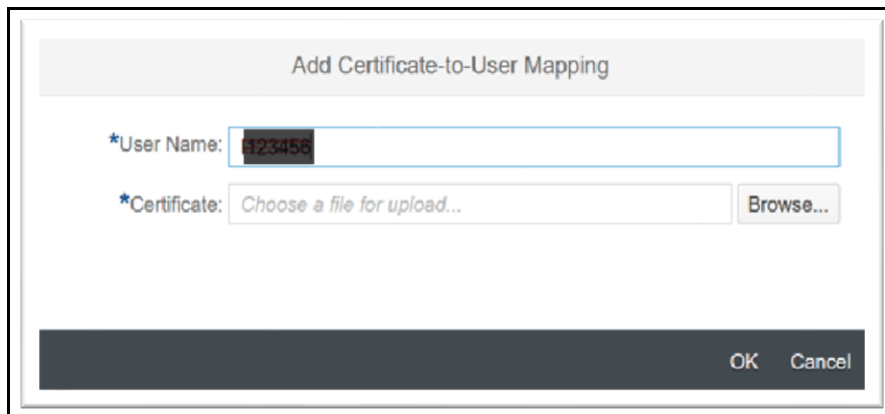


- b. Click **Add**.



- c. 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 'eWay_Bill_Installation_and_Configurations' document attached to SAP note: 2631687

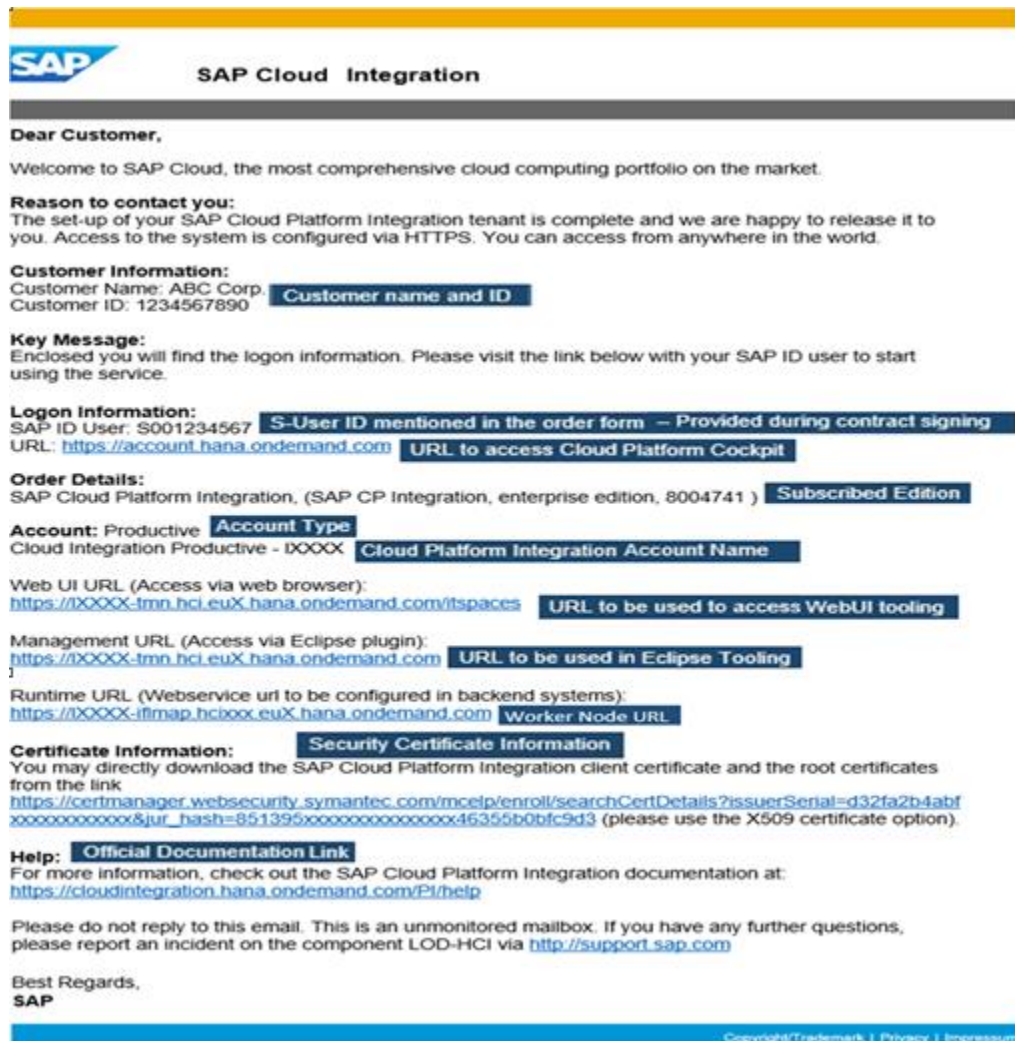


APPENDIX

About SAP Cloud Integration tenant

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

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



Adding Members to the SAP Cloud Integration Account

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

- Logon to the Account URL with the SAP ID user provided in the mail.
- Add members and assign roles to this account by navigating to **Members > Add Members**.



c. Assign the following roles.

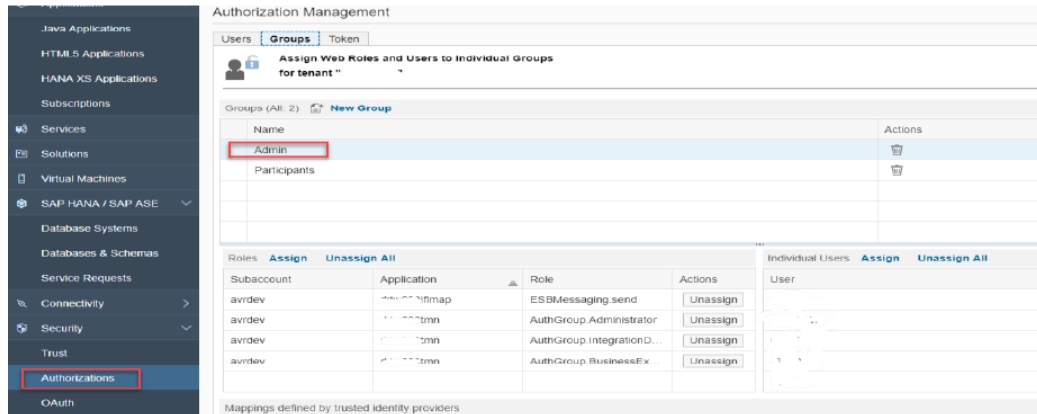
- **Administrator:** Assign the role of *Administrator* to the user who is supposed to have the full permissions of an administrator.
- **Application User Admin:** Assign the role of *Application User Admin* to the user who is supposed to have restricted administrator privileges.

A screenshot of a dialog box titled 'Add Members'. The dialog contains a text input field for 'User IDs' with a placeholder instruction: 'Enter up to 100 SAP user IDs. To separate them, you can use commas, spaces, semicolons, or line breaks.' To the right of the input field is a section titled 'Assign roles:' with a list of roles and checkboxes: 'Administrator (predefined role)' (checked), 'Developer (predefined role)', 'Support User (predefined role)', 'Application User Admin (predefined role)', 'Cloud Connector Admin (predefined role)', and 'CloudConnector'. Below the roles is a text input field for 'Comment (optional, visible to all members)'. At the bottom right of the dialog are two buttons: 'Add Members' and 'Cancel'.

Providing authorizations to SAP Cloud Integration Users

To provide authorizations to the SAP Cloud Integration Users:

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



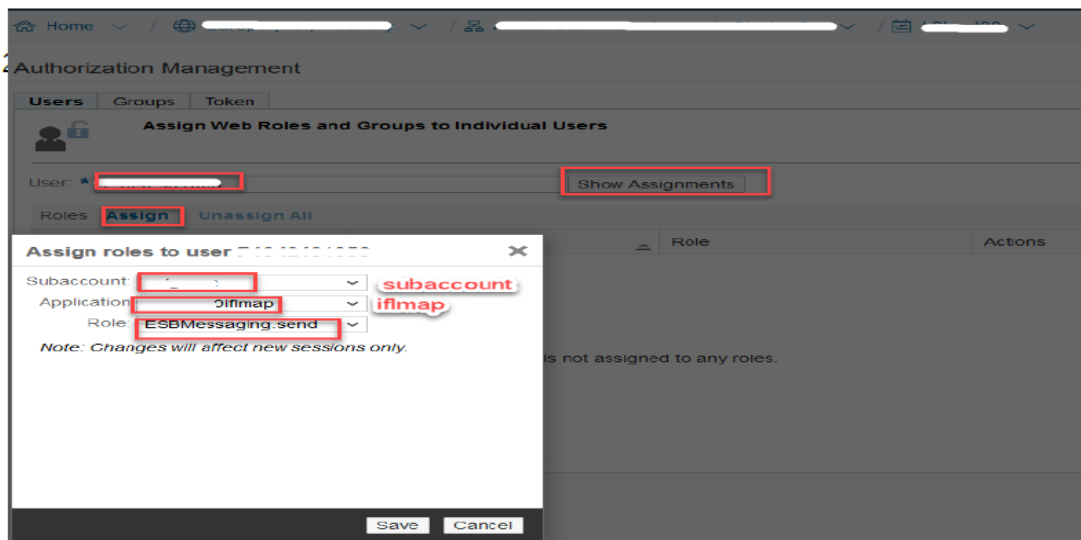
The authorization group AuthGroup.Administrator is designed for the administrator at customer side who administers a (customer-specific) tenant management node.

For more details refer [here](#).

Creating a Service User in SAP Cloud Integration

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

- g. Register a new user at <https://account.hana.ondemand.com/#/home/welcome>.
- h. Assign the ESBMessaging.Send role to the user.



Useful links:

- 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/03cf78a217574e7abd75bfba990c085.html>