PUBLIC

2020-04-10

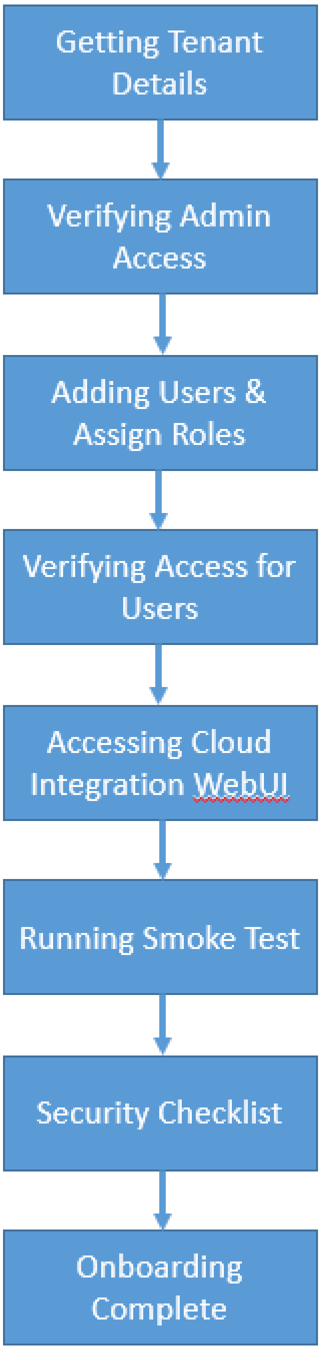
SAP Cloud Platform Integration Onboarding Guide

THE BEST RUN

Content

1 Introduction

This quick start guide provides all the information you need to quickly onboard after subscribing to SAP Cloud Platform Integration. Here are the steps in which you can complete the onboarding:



2 Getting Access to SAP Cloud Platform Integration

Context

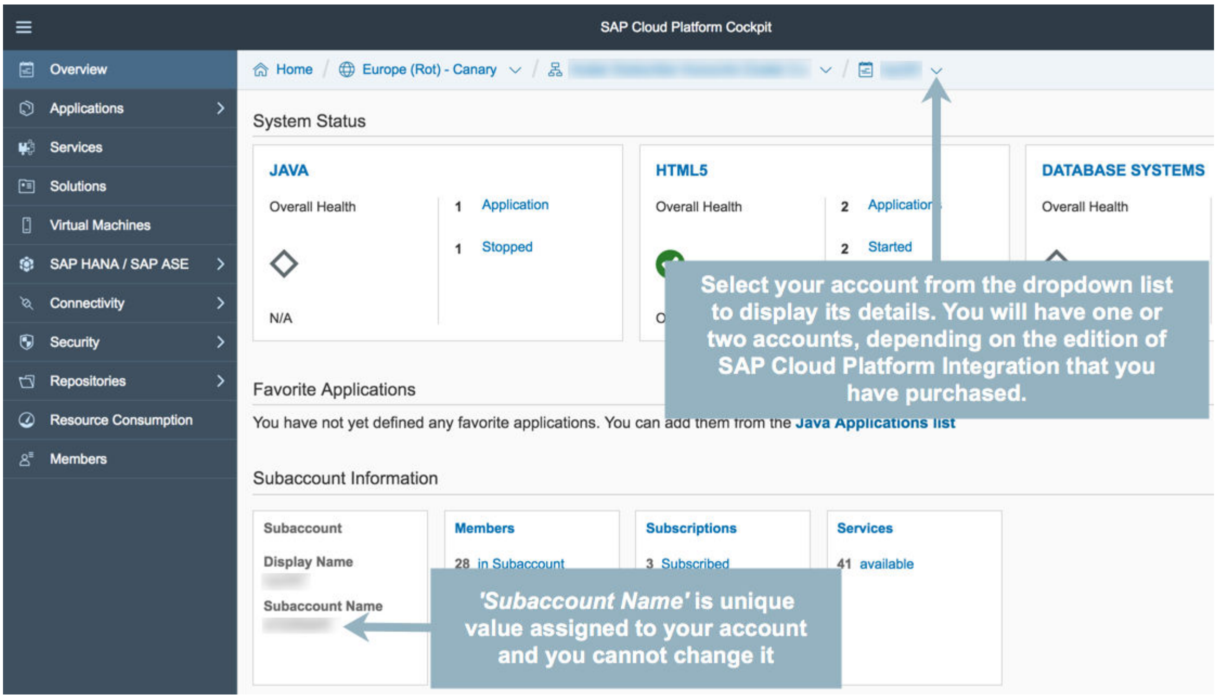
After you subscribe to any of the SAP Cloud Platform Integration editions, you will receive one or two e-mails from SAP based on the edition of SAP Cloud Platform Integration that you have purchased.

- If you have not received this e-mail, the most likely reason is that your user ID was not specified in the order form. Check with your internal team who was responsible for signing the contract and check which e-mail ID or S-user ID was provided to SAP Account Manager in the order form.
- Check with SAP Account Manager which S-user ID was provided in the order form.
- Contact the SAP Customer Success Team at *saphcphelp@sap.com*.
- If you are still facing issues, create a ticket using the component LOD-HCI. The SAP Cloud Operations team will provide a solution.

3 SAP Cloud Platform Integration in SAP Cloud Platform Cockpit

SAP provides Cloud Integration tenants with Admin access to the S-user ID specified in the order form. This user is the administrator of the tenant.

To check whether the administrator can access the Cloud Integration tenants, you need to log on to the SAP Cloud Platform cockpit. There are different URLs for different data centers. You need to use the URL provided in the e-mail from SAP (refer to example e-mail in Getting Access to SAP Cloud Platform Integration [page 4]) and log on with your S-user ID and password. The following screen appears:



You have not yet defined any favorite applications. You can add them from the Java Applications list

Select your account from the dropdown list to display its details. You will have one or two accounts, depending on the edition of SAP Cloud Platform Integration that you have purchased.

'Subaccount Name' is unique value assigned to your account and you cannot change it

You can view the Global Accounts ID by clicking on the i *(information)*

Selecting *Services*, you get an overview of all services enabled for your subaccount. Under *Integration* select the tile *Cloud Integration*. When you choose *Configure Cloud Integration*, you have the following options (when you have purchased Enterprise Edition):

- Provisioning a message broker if you like to use Java Message Service (JMS) queues
- Activating Integration Content Advisor for the subaccount

4 Adding New Administrators (Optional)

Prerequisites

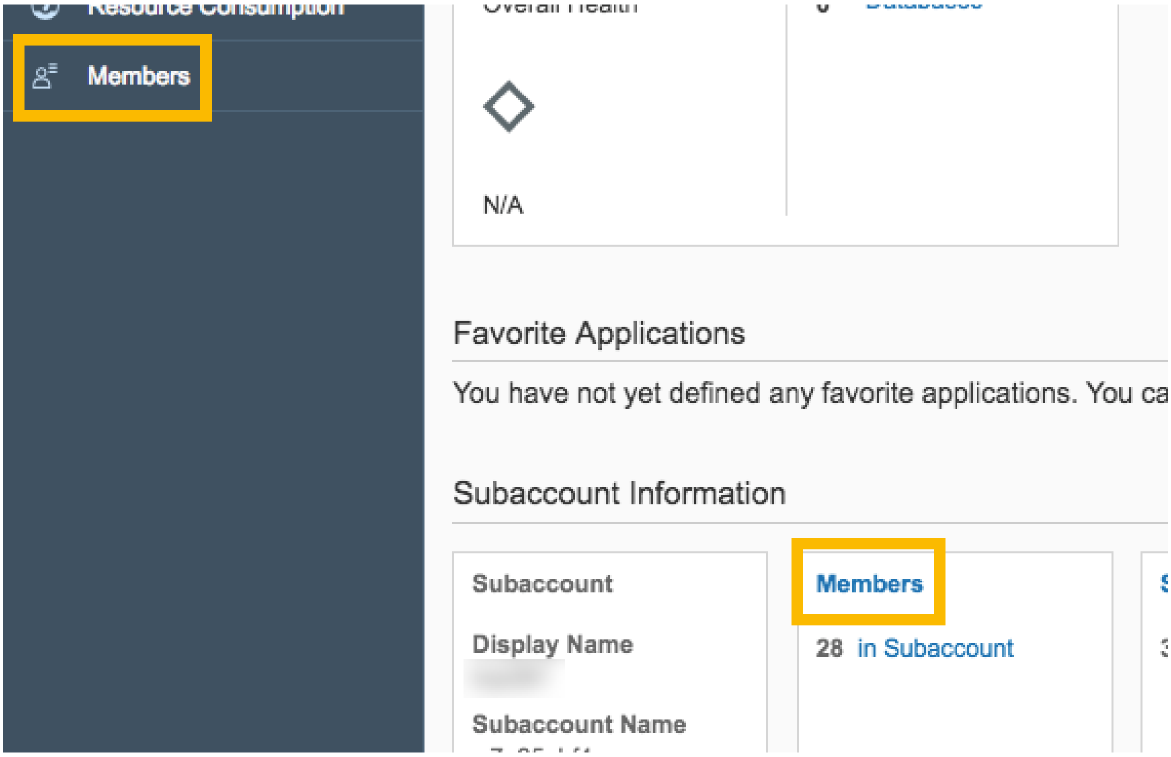
- Only users with a valid S-user or P-user ID can be added as members of the tenant.
- If you don't have an S-user ID but are eligible for one (you are a customer or a partner), please follow the steps in this link to generate a new S-user ID and password.
- If you don't have a P-user ID, please follow the steps in this link to generate a new P-user ID and password.
- You have logged into the SAP Cloud Platform

Context

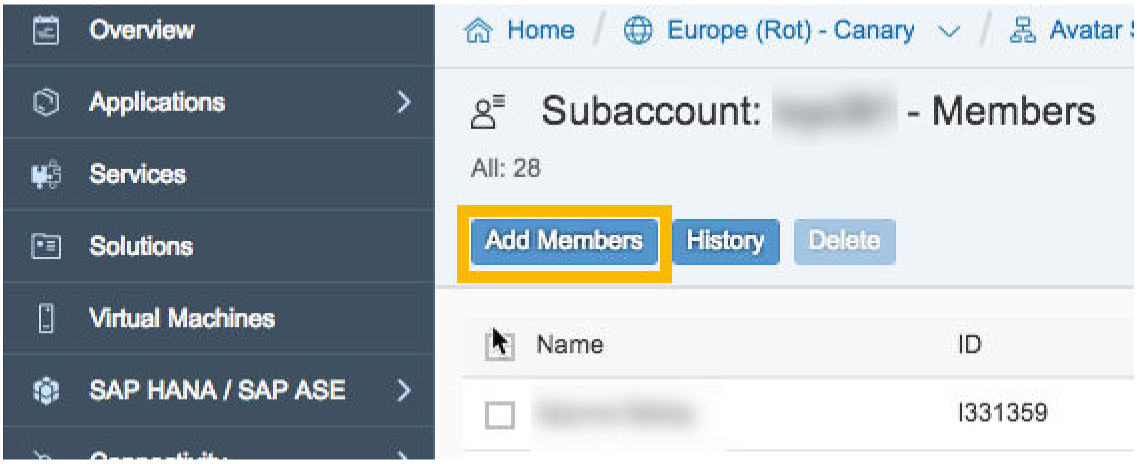
SAP grants administrator rights to the S-user ID specified in the order form. This user can grant administrator rights to other users in this account.

Procedure

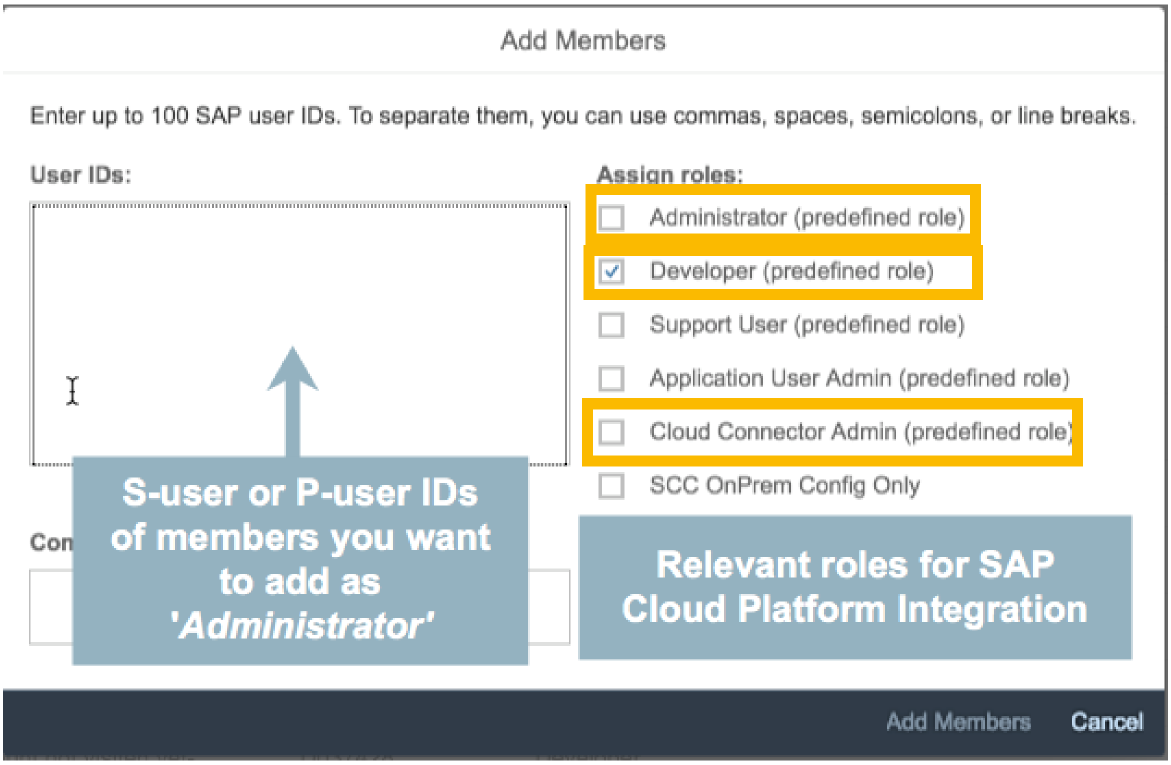
1. In the cockpit, choose *Members*.



2. Choose *Add Members*.



3. In *User IDs* field, enter the S-user or P-user IDs of all the users you want to add as administrators. Select the roles *Administrator (predefined role)*, *Developer (predefined role)* and *Cloud Connector Admin (predefined role)*.


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)

□ SCC OnPrem Config Only

S-user or P-user IDs of members you want to add as *'Administrator'*

Relevant roles for SAP Cloud Platform Integration

Next Steps

- The *Cloud Connector Admin* role is not mandatory for all users and depends on your requirements. Check question 16 in Security FAQs [page 29]. Also, you may not need the *Cloud Connector Admin* role during onboarding.
- If you have more than one tenant, you must add members to each tenant separately.

- For the latest documentation and detailed instructions on how to add members to an account,see Adding Members to an Account.

5 Assigning Users and Roles

Prerequisites

- Only users with a valid S-user or P-user ID can be added as members of the tenant.
- If you don't have an S-user ID but are eligible for one (you are a customer or a partner), please follow the steps in this link to generate a new S-user ID and password.
- If you don't have a P-user ID, please follow the steps in this link to generate a new P-user ID and password.

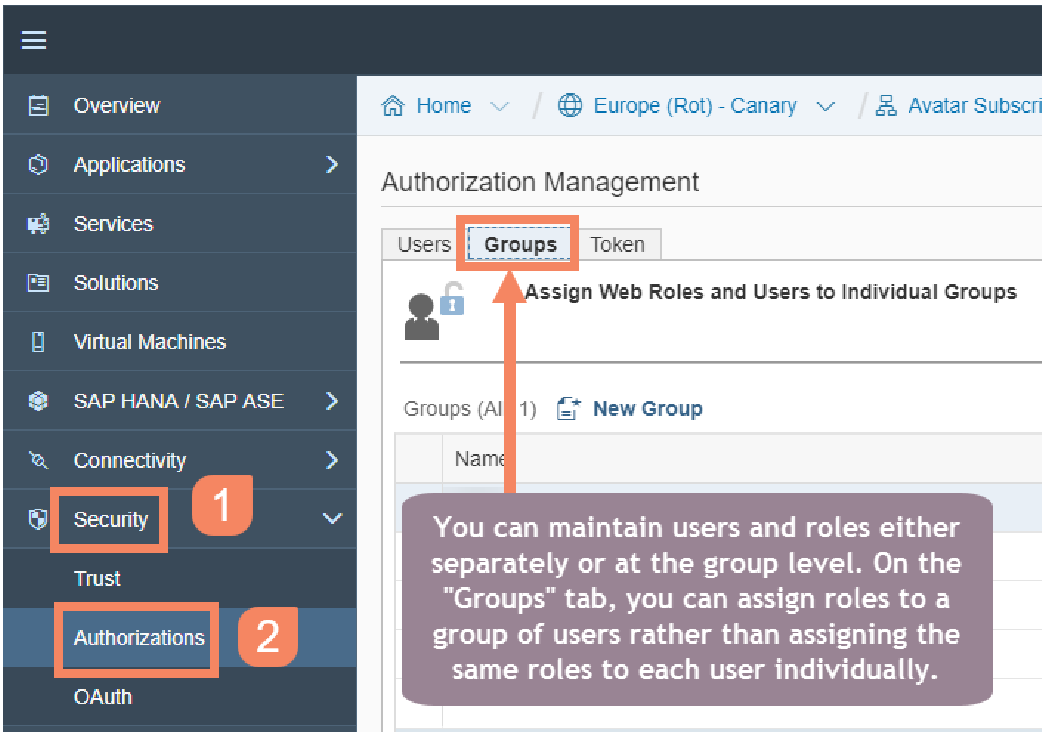
Context

Once you have verified that you have administrator access and have added any additional administrators required, you can assign users who will work on SAP Cloud Platform Integration scenarios and grant them the necessary user roles.

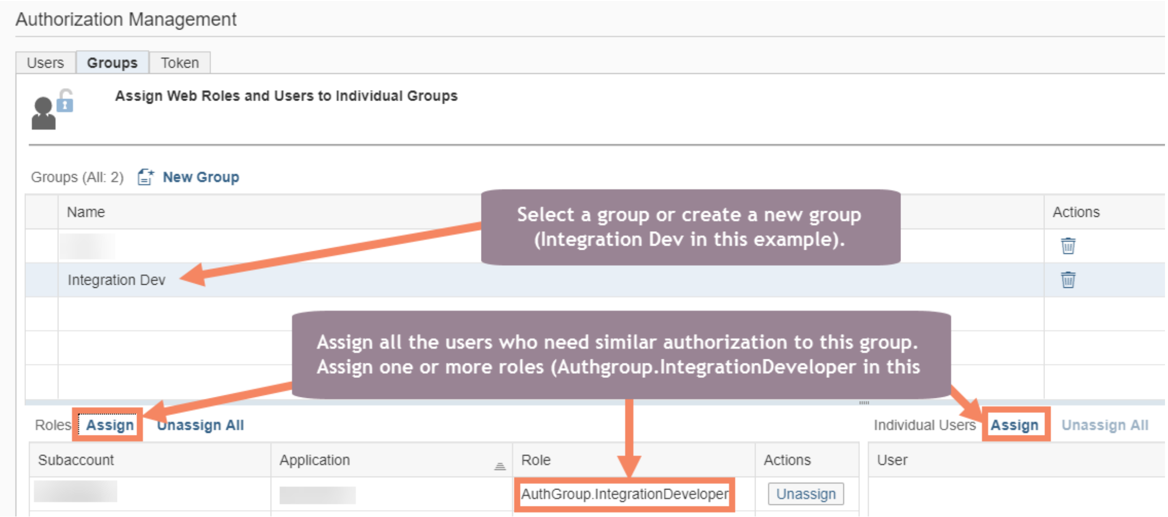
Procedure

1. To assign users to your tenant account, choose *Security* › *Authorizations* › *Groups*.

   We recommend that you assign *Users* and *Roles* on the *Groups* tab as this is the most efficient way of managing user role assignments.



You can maintain users and roles either separately or at the group level. On the "Groups" tab, you can assign roles to a group of users rather than assigning the same roles to each user individually.

2. 

Select a group or create a new group (Integration Dev in this example).

Assign all the users who need similar authorization to this group. Assign one or more roles (Authgroup.IntegrationDeveloper in this

IMPORTANT

We have used *Authgroup.IntegrationDeveloper* as an example here. You can use other authorization groups as well, depending on your requirements.

6 Available Roles and Authorization Groups

We recommend that you use authorization groups to assign user roles. , you need to assign the role *esb.messaging.send* to the user with whom you want to perform basic authentication for the HTTPS inbound scenario for SAP Cloud Platform Integration.

For detailed information on tasks and the roles that you need to perform them, see Tasks and Required Roles.

For the latest documentation and detailed instructions on how to assign roles, see Defining Authorizations.

The following table provides an overview of some of the frequently used authorization groups.

Authorization Groups Overview

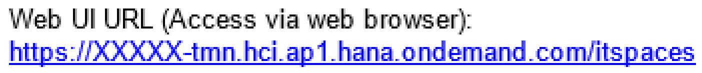
Authorization Group	Description
AuthGroup.BusinessExpert	Enables a business expert to perform business tasks. This includes tasks such as: • Monitoring integration flows • Reading the message payload
AuthGroup.Administrator	Enables the administrator of the tenant cluster (also referred to as the tenant administrator) to connect to a cluster and perform administrative tasks on the cluster. This includes tasks such as: • Deploying security content (for example, keystores or SSH known hosts artifacts) • Deploying integration flows • Canceling messages • Monitoring integration flows • Deleting messages from the transient data store
AuthGroup.IntegrationDeveloper	Enables an integration developer to connect to a cluster using Integration Designer and to display, download, and deploy artifacts (for example, integration flows). This includestasks such as: • Monitoring integration flows • Deploying integration flows • Deploying security content included in integration flows (for example, keystores or SSH known hosts artifacts) • Canceling messages

Authorization Group	Description
AuthGroup.ReadOnly	Enables you to connect to a tenant cluster (from the customer side), display nodes and node properties, and monitor messages.
AuthGroup.SystemDeveloper	Enables a system developer to perform the tasks required for system support. This includes tasks such as: ● Monitoring integration flows ● Restarting subsystems of the tenant cluster ● Software development tasks on VMs of the tenant cluster i Note System developer tasks are typically required in the support case by SAP experts who need to perform tasks debugging on the tenant cluster.

7 Verifying Access for Users

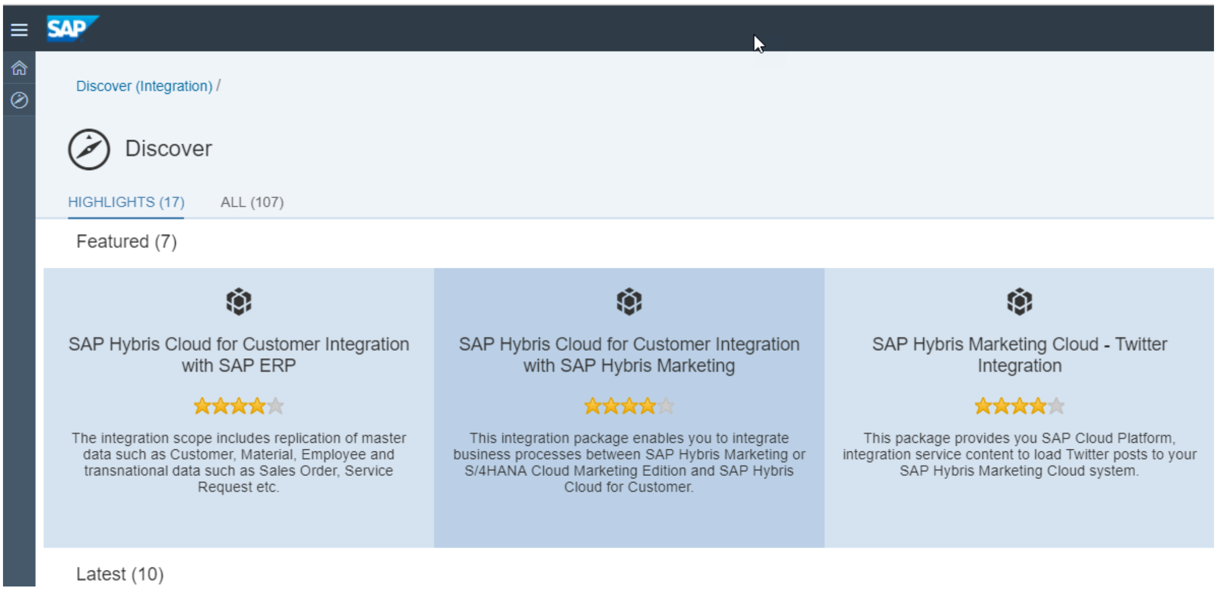
The next step is to verify whether all the users that you have added have access to the SAP Cloud Platform Integration application.

In the welcome e-mail that you received from SAP, you will find the URL for the WebUI, (the Web application.) Here's an example:



Web UI URL (Access via web browser):
https://XXXXX-tmn.hci.ap1.hana.ondemand.com/itspaces

Launch this URL in a browser (Internet Explorer or Google Chrome). Enter your S-user or P-user ID and password to log on to the application. The following screen appears, showing prepackaged integration content from SAP.



SAP Hybris Cloud for Customer Integration with SAP ERP

The integration scope includes replication of master data such as Customer, Material, Employee and transnational data such as Sales Order, Service Request etc.

SAP Hybris Cloud for Customer Integration with SAP Hybris Marketing

This integration package enables you to integrate business processes between SAP Hybris Marketing or S/4HANA Cloud Marketing Edition and SAP Hybris Cloud for Customer.

SAP Hybris Marketing Cloud - Twitter Integration

This package provides you SAP Cloud Platform, integration service content to load Twitter posts to your SAP Hybris Marketing Cloud system.

If you are unable to verify access, perform the following steps:

1. If you get an authentication error or any other issues, please check that you have assigned the right role to the S/P-user that you are verifying access for. For more information, see Assigning Users and Roles [page 9].
2. You can also contact the SAP Customer Success Team at saphcphelp@sap.com.
3. If you get an *Access Denied* error even though you have correctly assigned the required user roles, please check the SSO certificates in your browser. The browser might be using another user for the SSO logon instead of the S-user that you defined in the roles and authorizations.

4. If you are still facing issues, create a ticket using the component LOD-HCI. The SAP Cloud Operations team will look into the issue and provide a solution.

8 Performing a Smoke Test

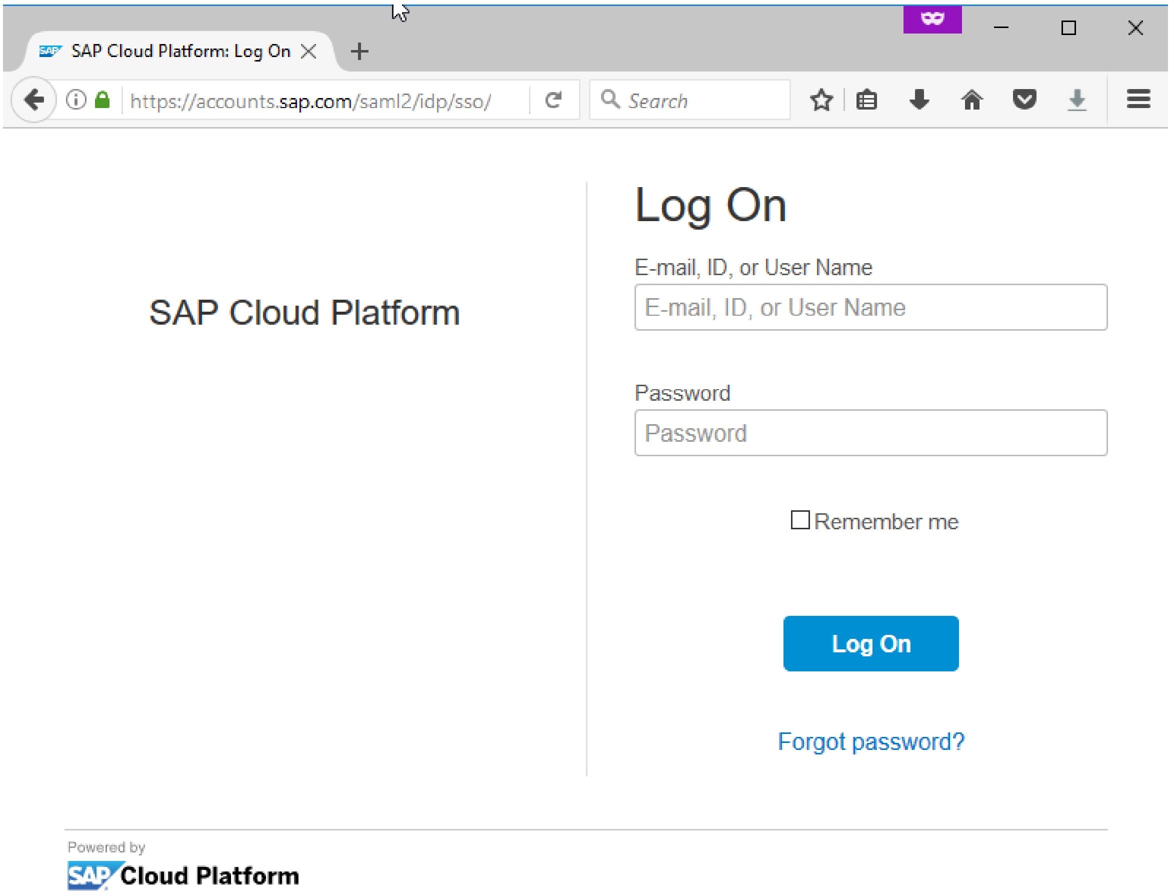
Context

Procedure

1. Launch the application URL provided by SAP.

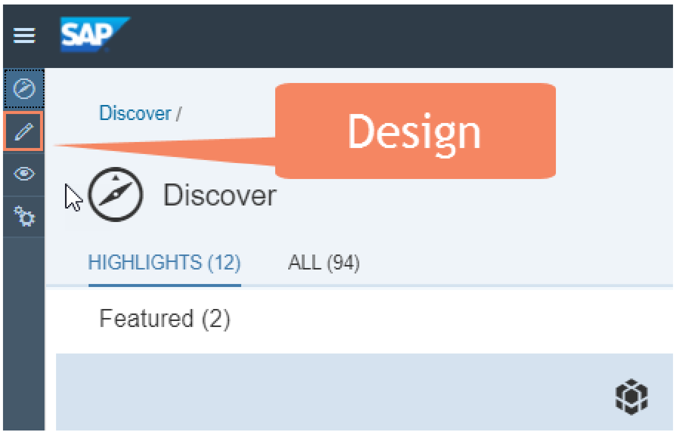
   For information about how to obtain this URL, see Verifying Access for Users [page 13].

   You see the logon screen.

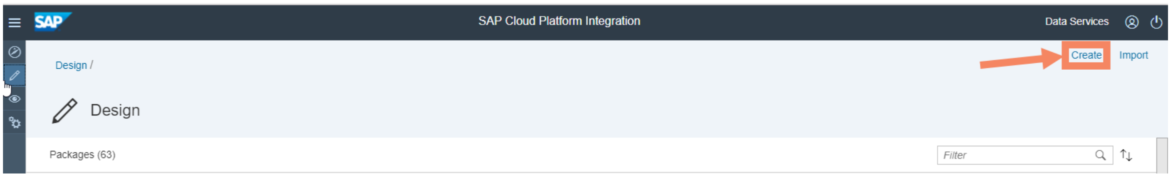


2. Enter your S/P-user ID and password. Choose *Log On*.

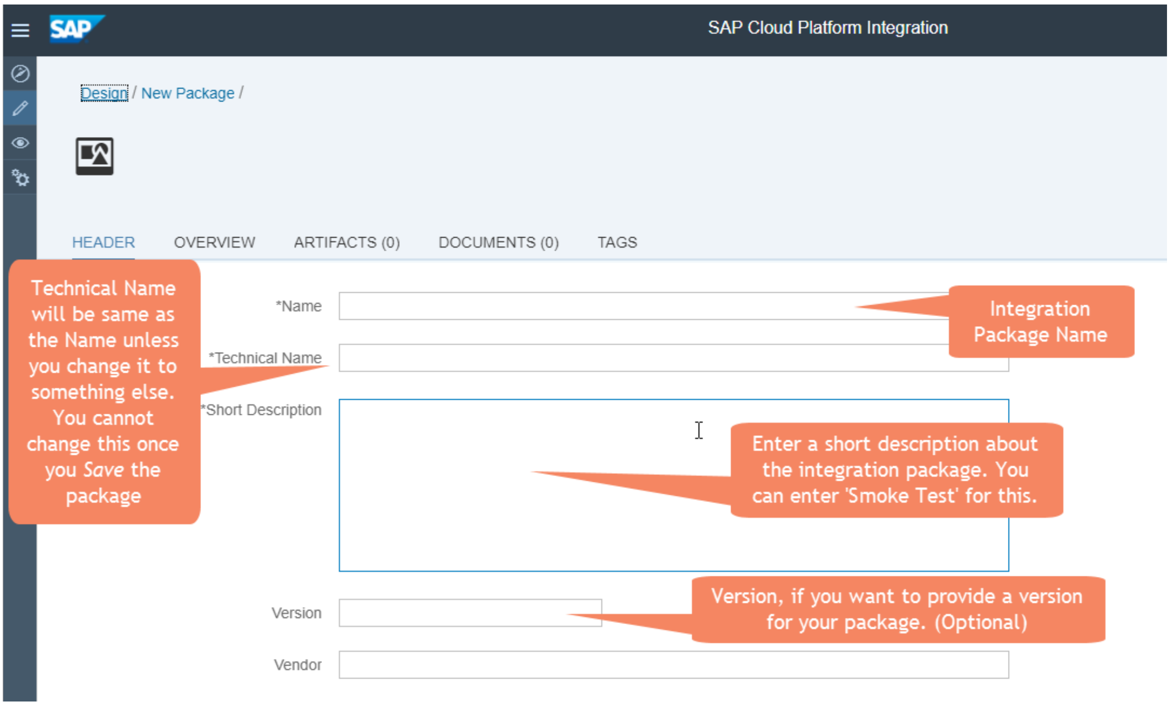
3. Choose ✎ to access your workspace. This is where you will create integration packages and develop and deploy integration flows.



4. Choose *Create* to create a new integration package.



5. Enter `<Name>` and `<Short Description>`. If you leave the `<Technical Name>` field empty, the value you have entered in the `<Name>` field is used. You cannot change this after you have saved the integration package.



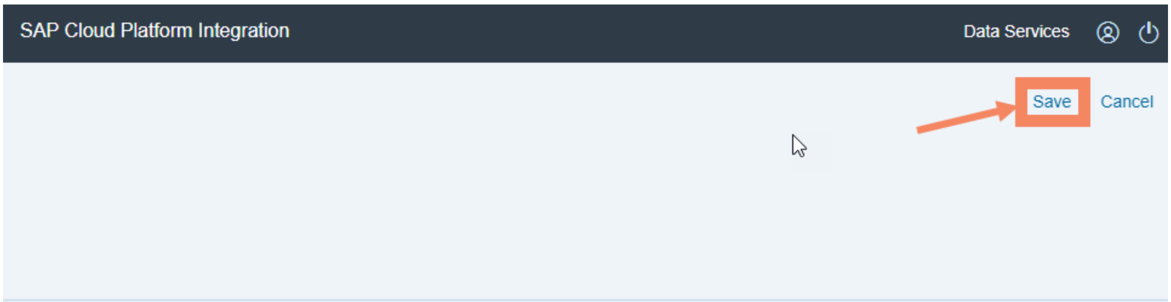
Technical Name will be same as the Name unless you change it to something else. You cannot change this once you *Save* the package

Integration Package Name

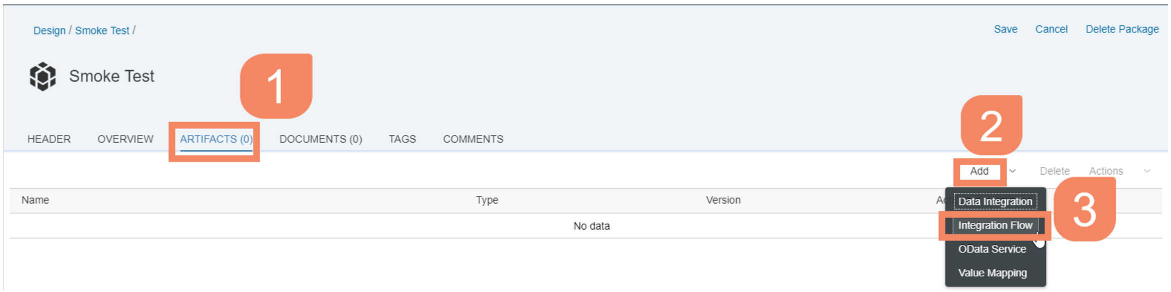
Enter a short description about the integration package. You can enter 'Smoke Test' for this.

Version, if you want to provide a version for your package. (Optional)

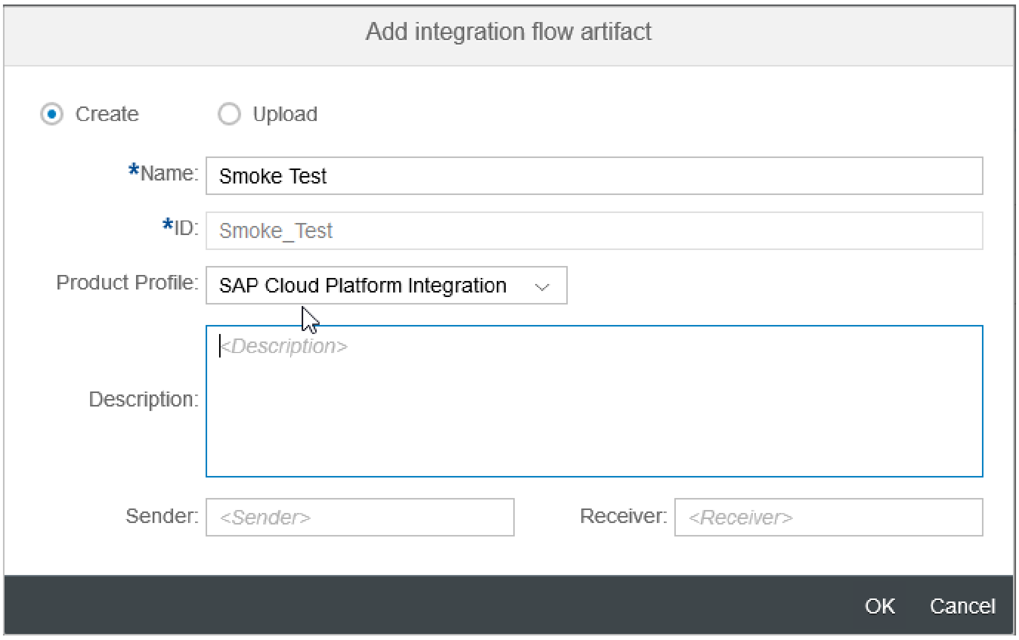
6. Choose *Save*.



7. Choose ▶ *Artifacts* ▶ *Add* ▶ *Integration Flow* ▶.



8. Enter *Name* (mandatory) and *Description* (optional). The `<ID>` is automatically provided by the system. Choose *OK*.


Add integration flow artifact

● Create ○ Upload

*Name: Smoke Test

*ID: Smoke_Test

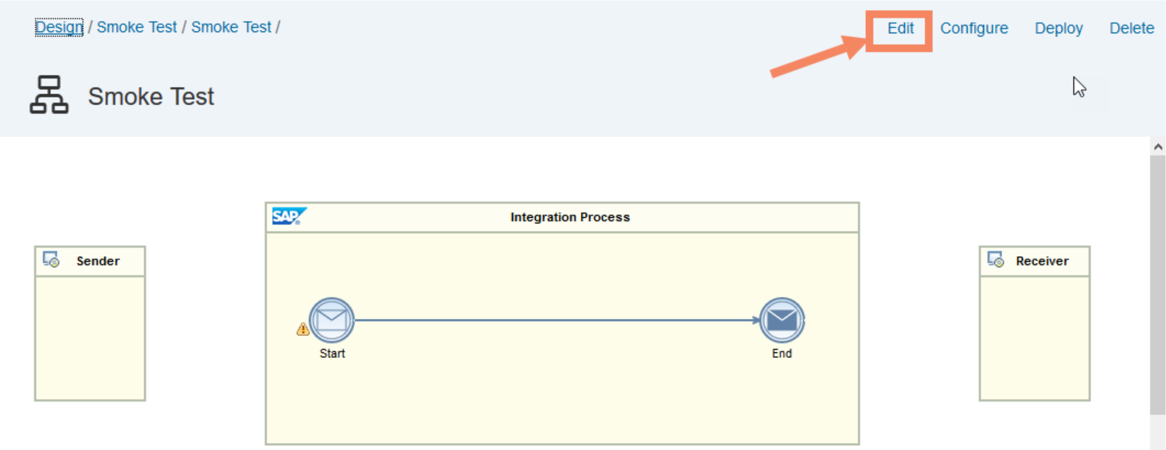
Product Profile: SAP Cloud Platform Integration

Description: <Description>

Sender: <Sender> Receiver: <Receiver>

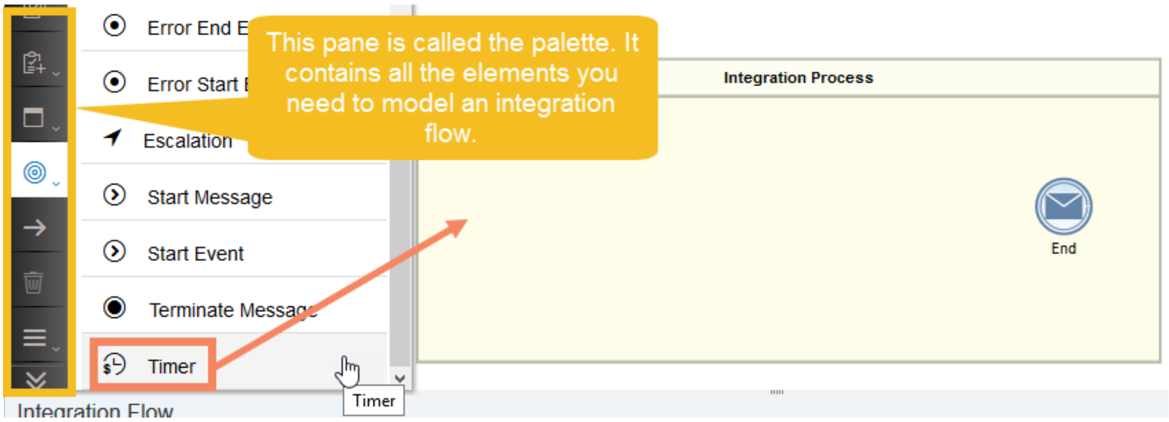
OK Cancel

9. You can now see the artifact with the *Name* you provided. Select it.
10. The integration flow that you have created opens in the integration flow editor. Choose *Edit* to edit the integration flow.

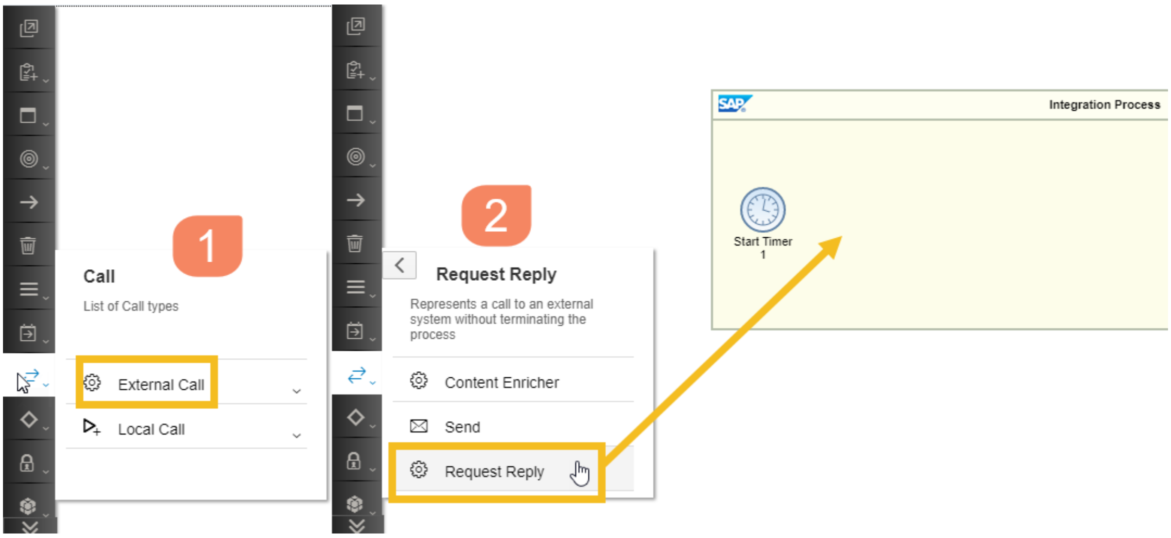


11. Mouse over the *Sender*, *Receiver*, and *Start* steps, and choose *Delete* to remove them from the integration flow. We will not be using these steps in this smoke test. The final integration flow should look like this:

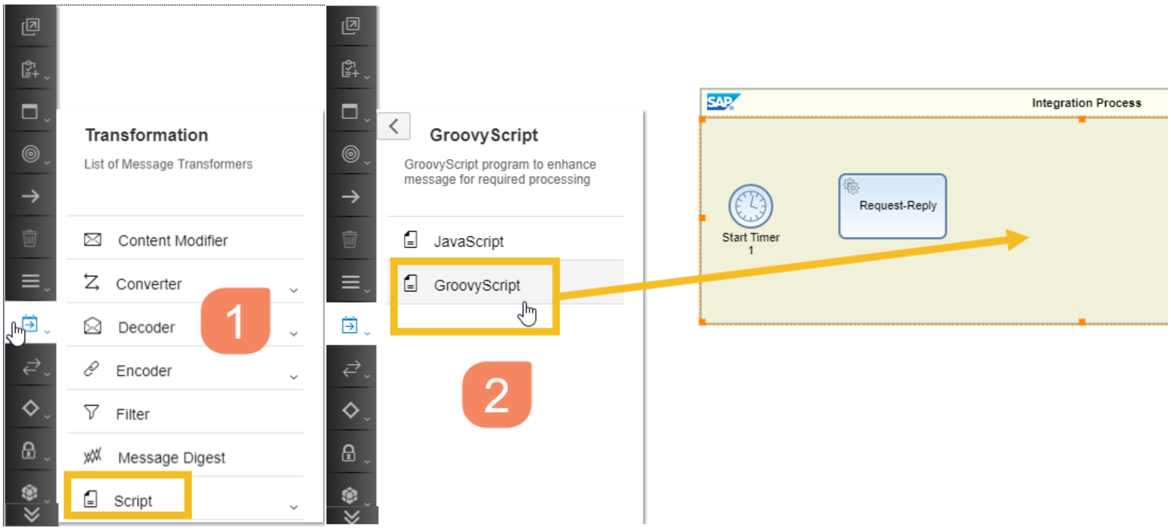
12. Now, let's model the integration flow to create the smoke test. The first step is to add the *Timer* step from the palette. Select ◎> Timer, then click inside the *Integration Process* where you want to place the *Timer*.


This pane is called the palette. It contains all the elements you need to model an integration flow.

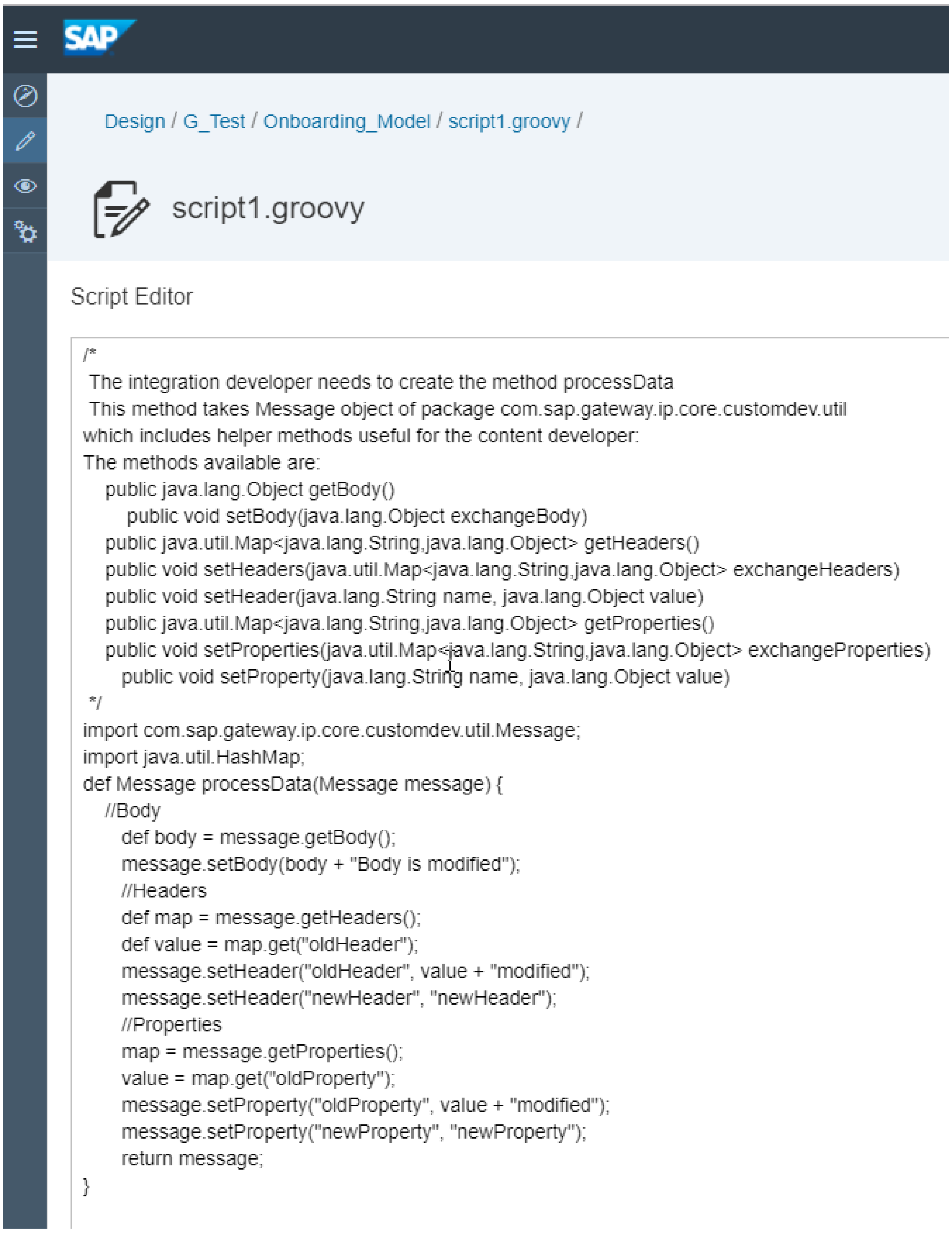
13. Select > > *External Call* > *Request Reply* > and add it to the integration process.



14. Select ▶ ▶ *Script* ▶ *Groovy Script* ▶ and add it to the integration process.



You see the *Script Editor*.

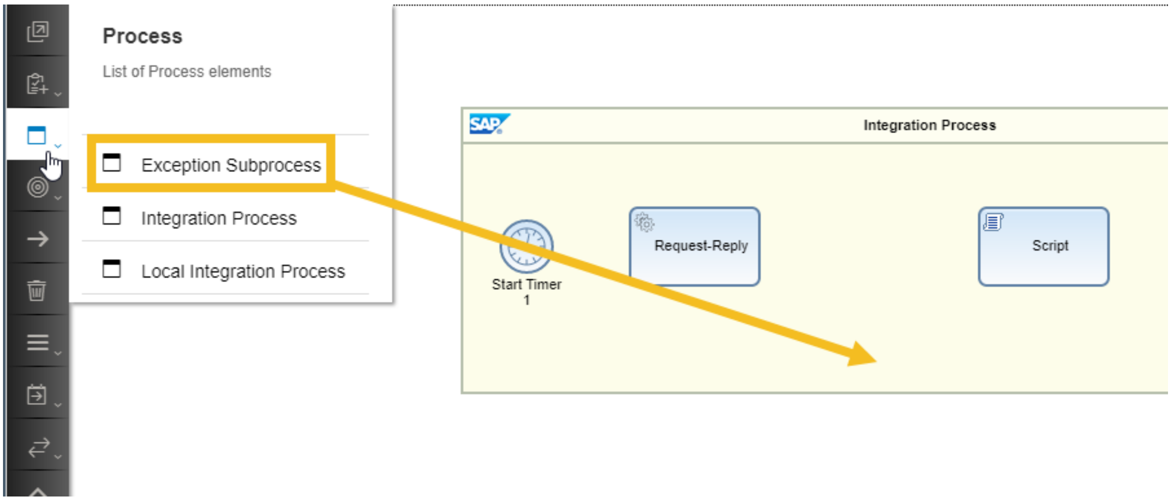


```
/*
 The integration developer needs to create the method processData
 This method takes Message object of package com.sap.gateway.ip.core.customdev.util
which includes helper methods useful for the content developer:
The methods available are:
    public java.lang.Object getBody()
        public void setBody(java.lang.Object exchangeBody)
    public java.util.Map<java.lang.String,java.lang.Object> getHeaders()
    public void setHeaders(java.util.Map<java.lang.String,java.lang.Object> exchangeHeaders)
    public void setHeader(java.lang.String name, java.lang.Object value)
    public java.util.Map<java.lang.String,java.lang.Object> getProperties()
    public void setProperties(java.util.Map<java.lang.String,java.lang.Object> exchangeProperties)
       public void setProperty(java.lang.String name, java.lang.Object value)
 */
import com.sap.gateway.ip.core.customdev.util.Message;
import java.util.HashMap;
def Message processData(Message message) {
    //Body
       def body = message.getBody();
       message.setBody(body + "Body is modified");
       //Headers
       def map = message.getHeaders();
       def value = map.get("oldHeader");
       message.setHeader("oldHeader", value + "modified");
       message.setHeader("newHeader", "newHeader");
       //Properties
       map = message.getProperties();
       value = map.get("oldProperty");
       message.setProperty("oldProperty", value + "modified");
       message.setProperty("newProperty", "newProperty");
       return message;
}
```

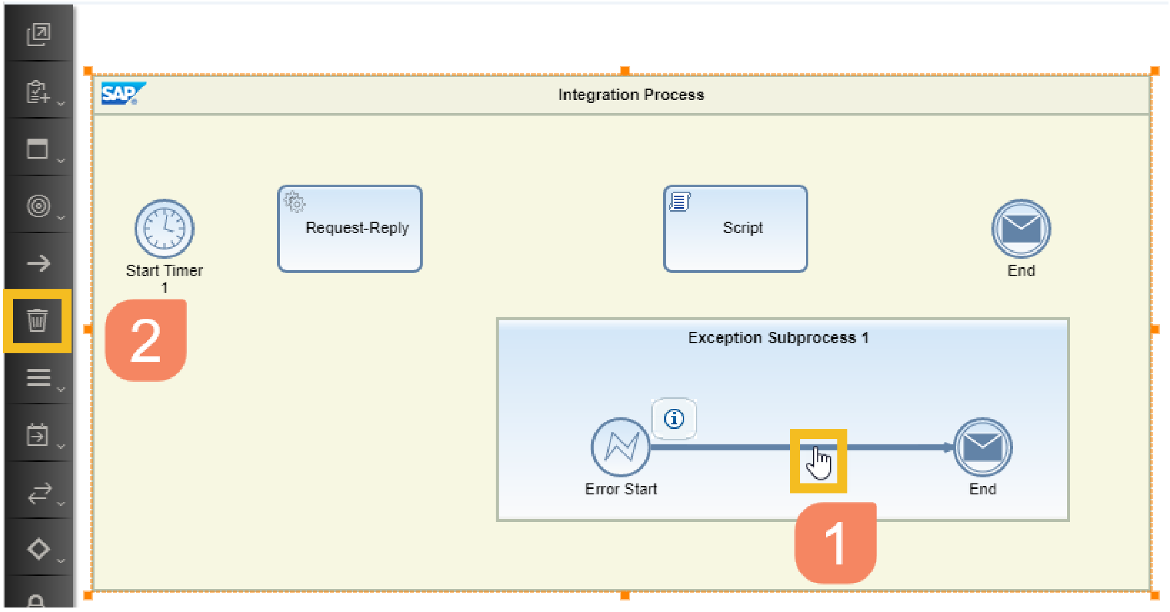
15. Replace the contents of the *Script Editor* with the following script and choose *OK*.

```
import com.sap.gateway.ip.core.customdev.util.Message;
import java.util.HashMap;
def Message processData(Message message)
{
    def body = message.getBody(java.lang.String) as String;
    def messageLog = messageLogFactory.getMessageLog(message);
    if(messageLog != null)
    {
    messageLog.addAttachmentAsString("Log current Payload:", body, "text/
plain");
     }
    return message;
}
```

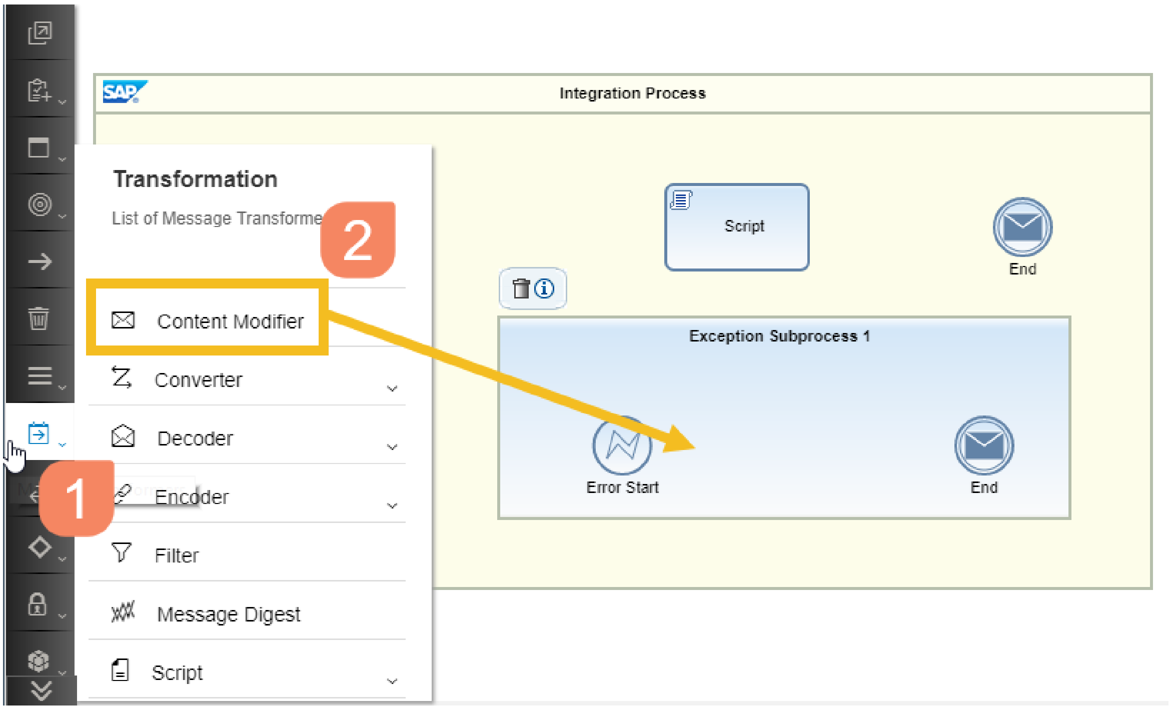
16. Select ▷ ▭ ▷ *Exception Subprocess* ▷ and add it to the integration process.



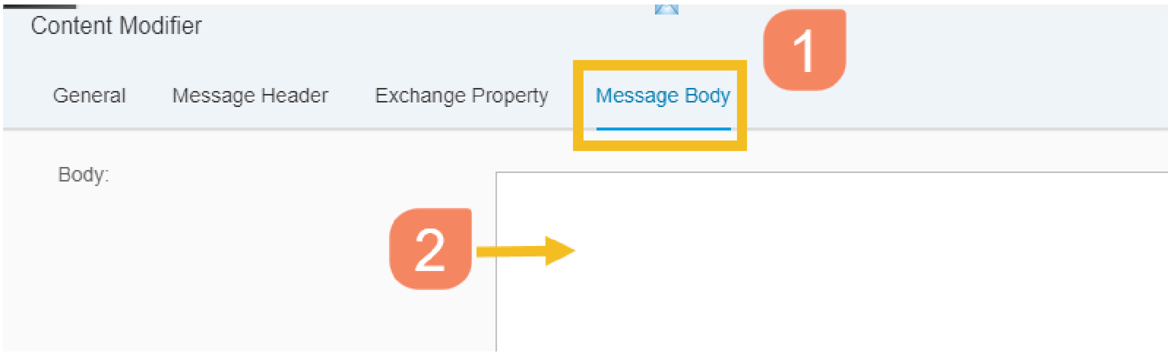
17. Delete the message path between *Error Start* and *End* by selecting the message path and choosing 🗑 (*Delete*).



18. Choose ▷ ⍈ ▷ *Content Modifier* ▷ and add it inside*Exception Subprocess 1*.



19. Go to the *Message Body* tab. In the *Body* field, enter **`The service is unavailable at the moment. Please try again after some time..`**

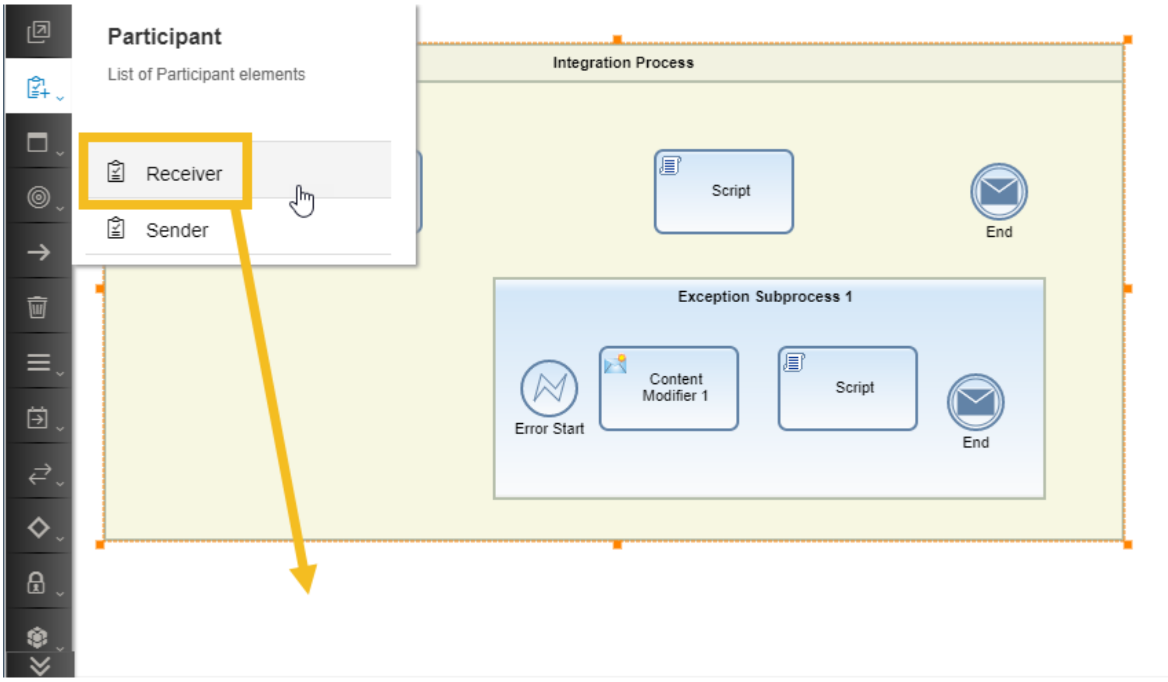


20. Select > Script > GroovyScript > and add it inside *Exception Subprocess 1*.
21. Replace the contents of the *Script Editor* with the following script and choose *OK*, just like you did in **Step 15**.

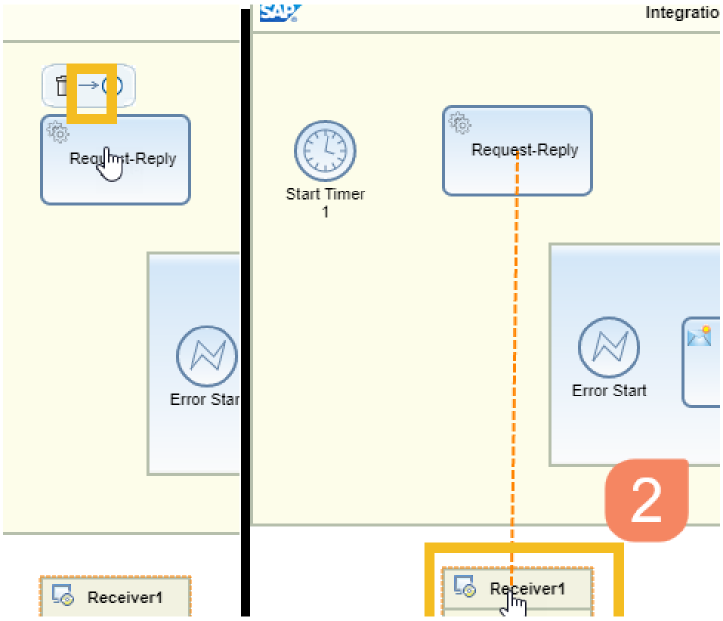
```
import com.sap.gateway.ip.core.customdev.util.Message;
import java.util.HashMap;
def Message processData(Message message)
{
    def body = message.getBody(java.lang.String) as String;
    def messageLog = messageLogFactory.getMessageLog(message);
    if(messageLog != null)
    {
    messageLog.addAttachmentAsString("Log current Payload:", body, "text/
plain");
     }
    return message;
}
```

> → Tip
>
> Rearrange the integration flow steps in *Exception Subprocess 1* to ensure that you can easily define the message path.

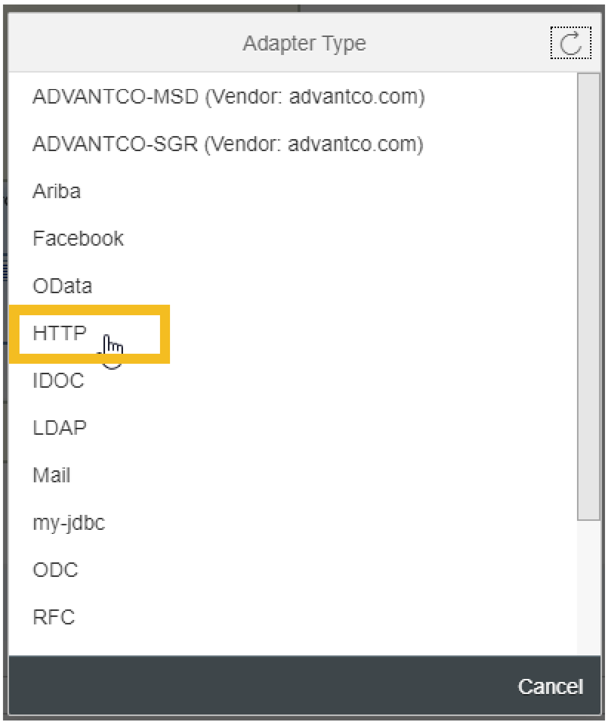
22. Select ▶ > *Receiver* > and add it outside the integration process.



23. Choose the message path icon from *Request-Reply* and define a message path to *Receiver1*.



24. In the *Adapter Type* prompt, select *HTTP*.



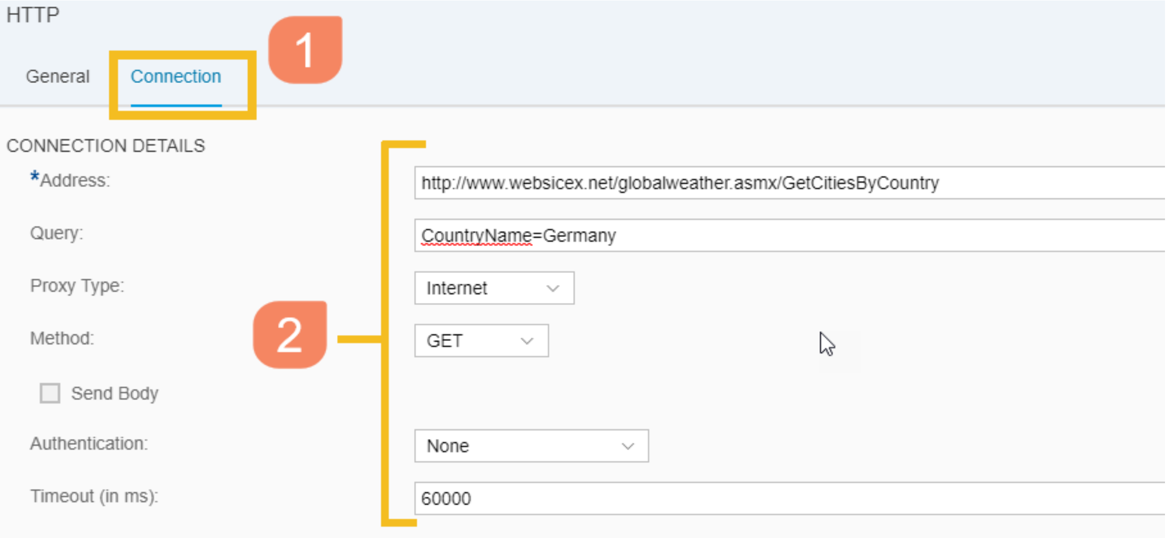
Adapter Type

ADVANTCO-MSD (Vendor: advantco.com)
ADVANTCO-SGR (Vendor: advantco.com)
Ariba
Facebook
OData
HTTP
IDOC
LDAP
Mail
my-jdbc
ODC
RFC

25. In the adapter properties, go to the *Connection* tab. Enter the following values for the fields:

Field	Description
Address	http://www.webservicex.net/globalweather.asmx/GetCitiesByCountry
Query	CountryName=Germany **i Note** You can provide any country name you want.
Proxy Type	Internet
Method	GET
Authentication	None

Ensure that the *Send Body* checkbox is selected.



HTTP

CONNECTION DETAILS

*Address: http://www.websicex.net/globalweather.asmx/GetCitiesByCountry

Query: CountryName=Germany

Proxy Type: Internet

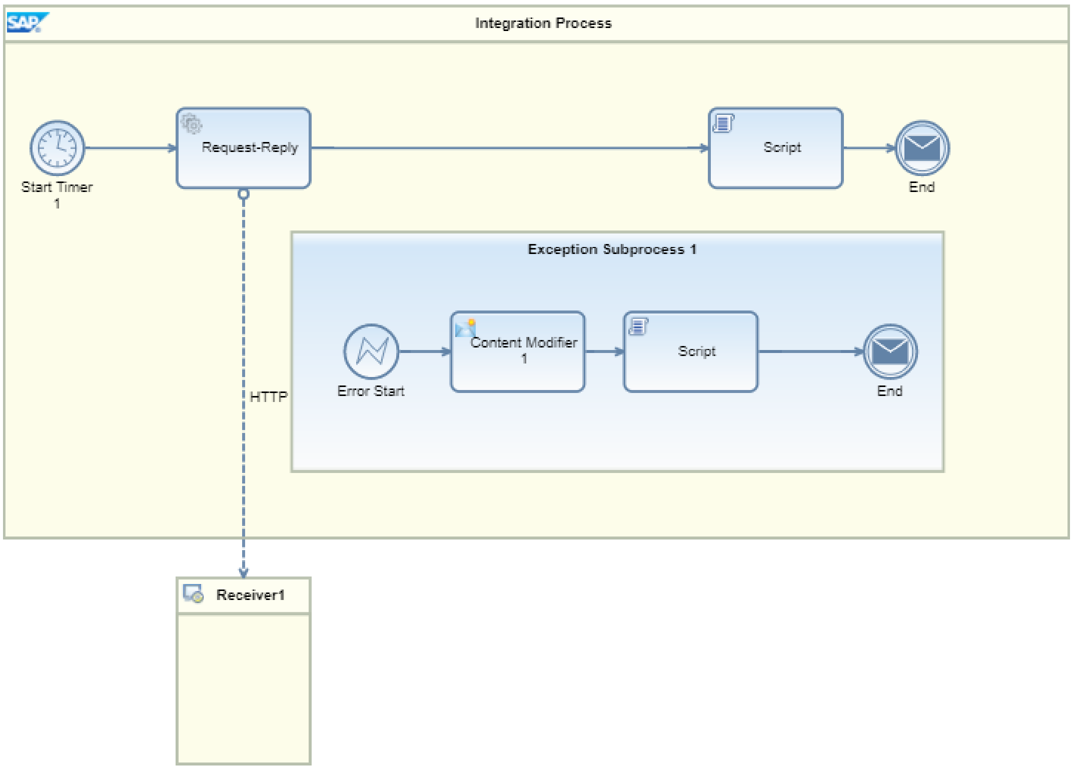
Method: GET

□ Send Body

Authentication: None

Timeout (in ms): 60000

26. Define the other message paths just like you did in step 23, and complete the integration flow as shown below.



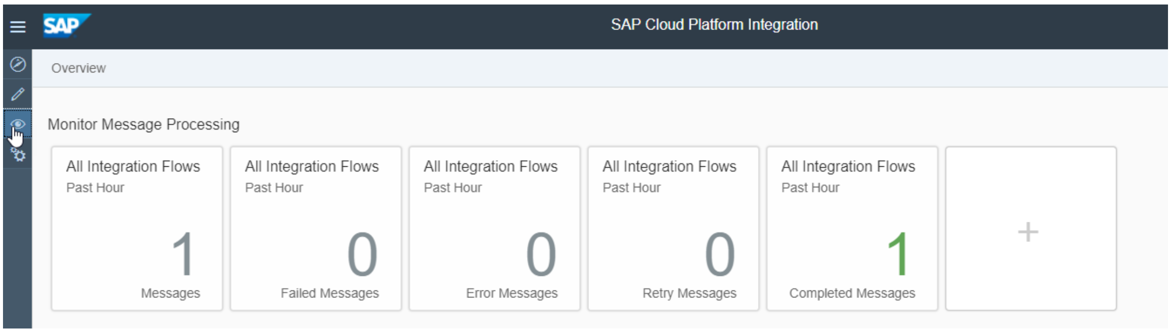
27. Choose *Save*. This saves the integration flow with the input that you have provided.
28. Choose *Deploy*.
29. Choose *OK* in the confirmation prompt.

    You see a message that the integration flow *Smoke Test* has been deployed successfully.

    You have to go to the monitoring tab to see the status of your integration flow.

30. Choose to go to the *Monitoring* tab.

    You see the overview of the monitoring section.



SAP Cloud Platform Integration

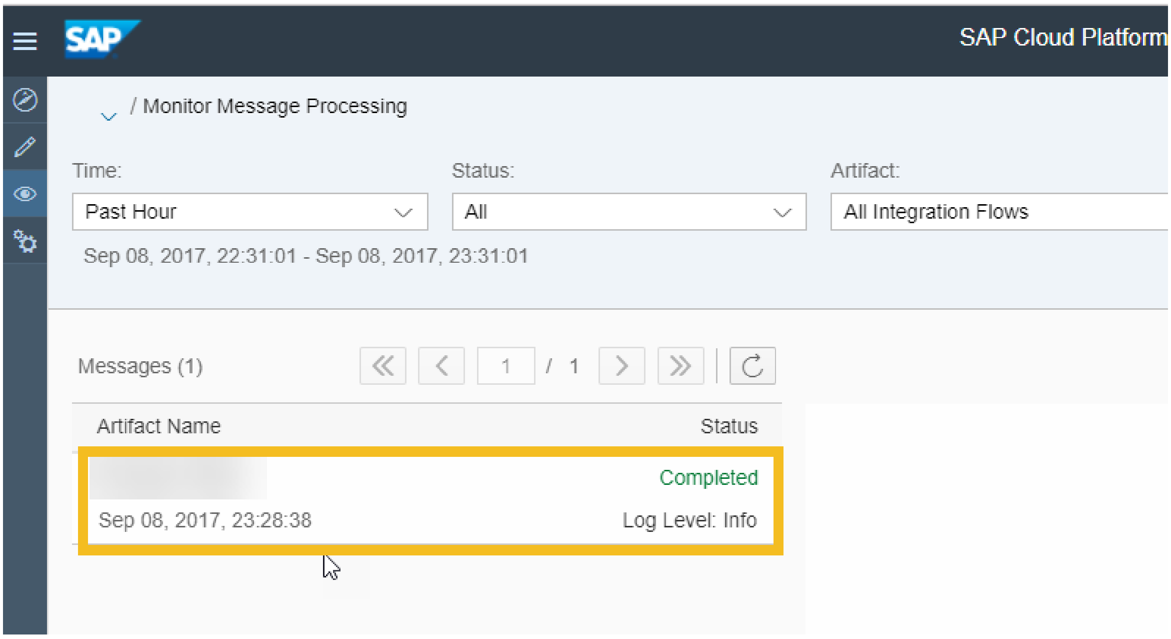
Overview

Monitor Message Processing

All Integration Flows Past Hour	All Integration Flows Past Hour	All Integration Flows Past Hour	All Integration Flows Past Hour	All Integration Flows Past Hour	+
1 Messages	0 Failed Messages	0 Error Messages	0 Retry Messages	1 Completed Messages	

31. Select *All Integration Flows*.

    You see the integration flow that you deployed in the *Artifact Name* column with status *Completed*.



SAP Cloud Platform

/ Monitor Message Processing

Time: Past Hour

Status: All

Artifact: All Integration Flows

Sep 08, 2017, 22:31:01 - Sep 08, 2017, 23:31:01

Messages (1)

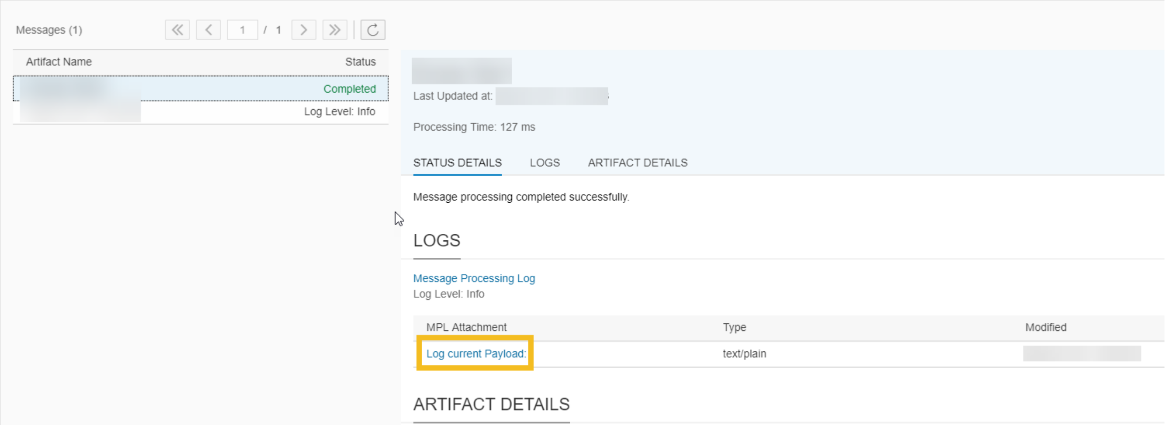
1 / 1

Artifact Name	Status
	Completed
Sep 08, 2017, 23:28:38	Log Level: Info

32. Select the entry.

    You see more information about the deployed integration flow. The *Status Details* tab shows that message processing completed successfully.

33. In the *MPL Attachment* column, choose *Log Current Payload*.



[redacted] Completed

Log Level: Info

[redacted]

Last Updated at: [redacted]

Processing Time: 127 ms

Message processing completed successfully.

LOGS

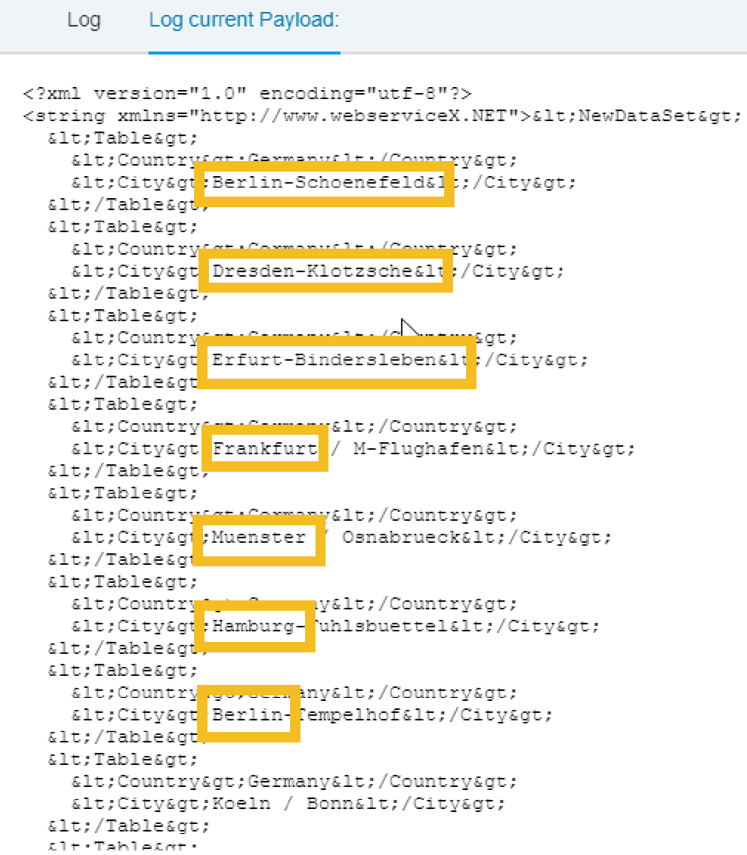
Message Processing Log

Log Level: Info

MPL Attachment	Type	Modified
Log current Payload:	text/plain	[redacted]

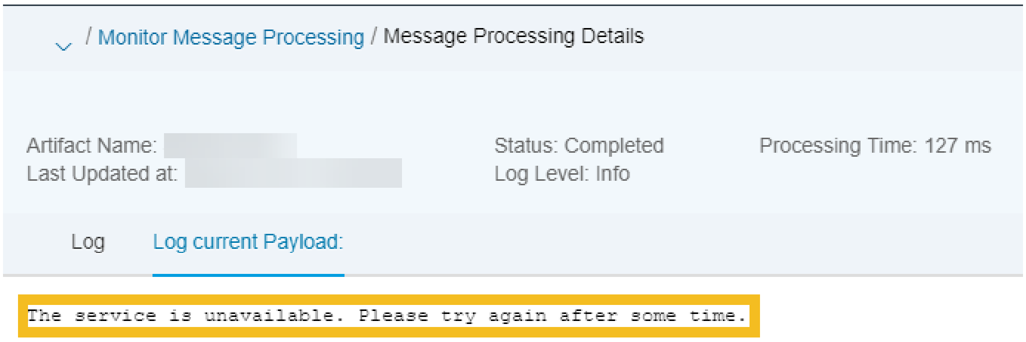
ARTIFACT DETAILS

34. You see a list of cities from the country you entered in step 25. In this case, you entered **Germany**, so you see a list of cities in Germany.



```
<?xml version="1.0" encoding="utf-8"?>
<string xmlns="http://www.webserviceX.NET">&lt;NewDataSet&gt;
  &lt;Table&gt;
    &lt;Country&gt;Germany&lt;/Country&gt;
    &lt;City&gt;Berlin-Schoenefeld&lt;/City&gt;
  &lt;/Table&gt;
  &lt;Table&gt;
    &lt;Country&gt;Germany&lt;/Country&gt;
    &lt;City&gt;Dresden-Klotzsche&lt;/City&gt;
  &lt;/Table&gt;
  &lt;Table&gt;
    &lt;Country&gt;Germany&lt;/Country&gt;
    &lt;City&gt;Erfurt-Bindersleben&lt;/City&gt;
  &lt;/Table&gt;
  &lt;Table&gt;
    &lt;Country&gt;Germany&lt;/Country&gt;
    &lt;City&gt;Frankfurt / M-Flughafen&lt;/City&gt;
  &lt;/Table&gt;
  &lt;Table&gt;
    &lt;Country&gt;Germany&lt;/Country&gt;
    &lt;City&gt;Muenster / Osnabrueck&lt;/City&gt;
  &lt;/Table&gt;
  &lt;Table&gt;
    &lt;Country&gt;Germany&lt;/Country&gt;
    &lt;City&gt;Hamburg-Fuhlsbuettel&lt;/City&gt;
  &lt;/Table&gt;
  &lt;Table&gt;
    &lt;Country&gt;Germany&lt;/Country&gt;
    &lt;City&gt;Berlin-Tempelhof&lt;/City&gt;
  &lt;/Table&gt;
  &lt;Table&gt;
    &lt;Country&gt;Germany&lt;/Country&gt;
    &lt;City&gt;Koeln / Bonn&lt;/City&gt;
  &lt;/Table&gt;
  &lt;Table&gt;
```

35. If the weather service that you accessed is unavailable, you see the message '**The service is unavailable. Please try again after some time.**'.



Artifact Name: [redacted]
Last Updated at: [redacted]

Status: Completed
Log Level: Info

Processing Time: 127 ms

```
The service is unavailable. Please try again after some time.
```

Results

If you see either a list of cities (step 34) or a message (step 35), this means that the smoke test was executed successfully and you can start using SAP Cloud Platform Integration for processes productively.

9 Security FAQs

How can new users and authorizations be added once a customer gets the SAP Cloud Platform Integration tenant? Who is authorized to add new users?

When SAP provides a tenant, administrator permissions are given to the S-user ID provided by the customer in the order form during contract signing. This administrative user can go to the SAP Cloud Platform cockpit and add additional users, and assign them roles and authorizations. Since SAP Cloud Platform Integration uses SAP Cloud Identity provider by default, all the users must have valid S-user or P-user IDs.

You can also configure Cloud Integration to use your own custom identity provider.For more information, see .

Where can I find a list of all roles and authorizations that can be assigned to users?

More information:

Which recommendations are given for assigning roles to users?

The customer has full control on giving permissions to users on a tenant.

A key part of an integration project is the development and deployment of integration content (for example, integration flows). The related permissions are defined by the authorization group `AuthGroup.IntegrationDeveloper` and `AuthGroup.Administrator`. Note that this authorization group provides extensive permissions. Therefore, take into account special considerations when assigning this authorization group to a user.

More information:

How can I contact SAP Cloud Platform Integration Operations support for information or issues related to tenant provisioning and security?

Create a ticket on component LOD-HCI-PI-OPS.

Are CA-signed certificates mandatory for transport-level authentication? Which scenarios require CA-signed certificates?

More information:

Transport Level Security [page 33]

Where can I find a list of CAs approved by SAP?

Load Balancer Root Certificates Supported by SAP

I want to use the same signed certificate for multiple systems. Can I put * in the Common Name field (for example, *.xxxxx.com) while the certificate is being signed by the CA? Does SAP allow this?

SAP recommends using the full host name in the Common Name (CN) field for both inbound and outbound scenarios, but technically does support the wildcard character in the CN field (for certificate-based client authentication only). For HTTPS outbound scenarios (where SAP manages the CA-signed key pairs), SAP uses the full host name in the CN field.

Can I use self-signed certificates for HTTPS certificate-based client authentication (also referred to as dual authentication)?

No, self-signed certificates are not supported for inbound connections to SAP Cloud Platform Integration. For outbound connections, we recommend using a CA-signed base certificate.

Which scenarios support self-signed certificates? Can I use them for message-level encryption and signing?

You can use self-signed certificates for message-level encryption and signing. However, we recommend using CA-signed certificates.

Who maintains and manages the keystore? Can control be given to the end customer?

SAP provides some keys by default, but keystore management is now a self-service, so you can manage your keystore yourself.

More information:

What is the procedure for using certificates for message-level encryption and signing?

You can use the certificates that are in the keystore provided by SAP during tenant provisioning. If you want to use your own key pair, you can manage it yourself using the self-service. There are different ways in which you can sign and encrypt message content (for example, PGP, X.509).

More information:

Message Level Security.

Do I need to make any special requests when connecting to the SFTP/SMTP server?

The following ports are opened by default:

- For SFTP/SSH: port 22
- For SMTP: ports 25, 465, and 587

Do I need to make any special requests for HTTP(S) for outbound connectivity?

By default, port 443 and all HTTP ports 1024 and higher are opened.

Which IP addresses for the SAP Cloud Platform Integration landscape do I need to configure in my own firewall for inbound connections (IP whitelisting)?

See Virtual System Landscapes.

Where can I find details on SAP Data Centers and security?

You can find this information on the SAP website under SAP Data Centers Information.

More information: https://www.sap.com/about/cloud-trust-center/data-center.html

What is SAP Cloud Platform Cloud Connector (SAP Cloud Connector)? Is it mandatory?

SAP Cloud Connector is a complementary offering. It needs to be installed on premise and is an integral component of SAP Cloud Platform. It acts as a reverse proxy and creates a secure tunnel with the customer's own SAP Cloud Platform Integration account. SAP Cloud Platform Integration can route calls via SAP Cloud Connector for HTTP-based protocols (for example, SOAP, OData IDoc XMLs). SAP Cloud Connector is the preferred mode of communication for SAP Cloud Platform customers. However, it is not mandatory and customers can use other reverse proxy software (for example, Web Dispatcher).

More information:

9.1 Transport Level Security

Cloud Integration Inbound Connection

Protocol	Related Adapters	Authentication Method	Required Certificates	Where to Get Required Certificates	CERT Usage in Customer Sender or Receiver Systems	Customer-CA Signed CERT Required?	CERT Usage in Cloud Integration Keystore
HTTPS	HTTP, SOAP, IDoc, OData and other HTTP based sender adapters	Basic Authentication	Root CA of SAP Cloud Platform Integration/ Load Balancer	You can use the self-service provided by SAP	Need to import Root CA of SAP SAP Cloud Platform Integration/ Load Balancer in the backend system's key store	No	Not required **Note:** Users requiring basic authentication must be have the role *ESBMessaging.send* role in SAP Cloud Platform Integration tenant. It needs to be assigned on the IFLMAP node.
HTTPS	HTTP, SOAP, IDoc, OData and other HTTP based sender adapters	Certificate based client authentication	Root CA of SAP Cloud Platform Integration/ Load Balancer	You can use the self-service provided by SAP	Need to import Root CA of SAP Cloud Platform Integration/ Load Balancer in the backend system's key store	No	Not required

Protocol	Related Adapters	Authentication Method	Required Certificates	Where to Get Required Certificates	CERT Usage in Customer Sender or Receiver Systems	Customer-CA Signed CERT Required?	CERT Usage in Cloud Integration Keystore
			Public key for certificate based client authentication	Customer must generate a key pair using any tool, generate CSR (certificate signing request) and get it signed by CA. List of allowed CAs are mentioned in the operations guide.	Customer needs to import the signed key pair along with Root CA in their sender's system keystore.	Yes	Not Required **Note:** Customer needs to provide the public key of the signed CA client certificate in the integration flow configuration on sender system after selecting authentication type as certificate based.

Cloud Integration Outbound Connection

Protocol	Related Adapters	Authentication Method	Required Certificates	Where to Get Required Certificates	CERT Usage in Customer Sender or Receiver Systems	Customer-CA Signed CERT Required?	CERT Usage in Cloud Integration Keystore
HTTPS	HTTP, SOAP, IDoc, OData and other HTTP based sender adapters	Basic Authentication	Root and intermediate CAs of the customer	Root and intermediate CAs should be provided by the customer	Not required	Yes	The root and intermediate certificates of the CA approved certificate needs to be added to the SAP Cloud Platform Integration keystore. You can use the self-service to add it to the keystore. **Note:** Users needing basic authentication must be deployed as user credentials on SAP Cloud Platform Integration and name of this credential should be specified in the respective technical adapter settings

Protocol	Related Adapters	Authentication Method	Required Certificates	Where to Get Required Certificates	CERT Usage in Customer Sender or Receiver Systems	Customer-CA Signed CERT Required?	CERT Usage in Cloud Integration Keystore
HTTPS	HTTP, SOAP, IDoc, OData and other HTTP based sender adapters	Certificate based client authentication	Root and intermediate CAs of the customer	Root and intermediate CAs should be provided by the customer	Not required	Yes	The root and intermediate certificates of the CA approved certificate needs to be added to the SAP Cloud Platform Integration keystore. You can use the self-service to add it to the keystore.
			SAP Cloud Platform Integration Public Key for certificate based client authentication	You can use the self service to manage keystore.	Public Key (or client certificate should be imported in customer server's keystore. Root and intermediate certificate should be imported in the customer server trust keystore.	No (yes only if customer wants to use own key pair for client authentication)	SAP will generate the signed certificate and will upload it in the keystore of SAP Cloud Platform Integration tenant (or will store the certificates provided by customer). Customer would need to mention the alias name of the certificate in adapter settings.
HTTP	HTTP	Basic Authentication	NA	NA	NA	NA	NA

Protocol	Related Adapters	Authentication Method	Required Certificates	Where to Get Required Certificates	CERT Usage in Customer Sender or Receiver Systems	Customer-CA Signed CERT Required?	CERT Usage in Cloud Integration Keystore
LDAP	LDAP	Simple Authentication	NA	NA	NA	NA	NA

Direction	Protocol	Related Adapters	Authentication Method	Required Certificates	Where to Get Required Certificates	CERT Usage in Customer Sender or Receiver Systems	Customer-CA Signed CERT Required?	CERT Usage in Cloud Integration Keystore
SAP Cloud Platform Integration inbound/ outbound	SSH	SFTP (Poll from SAP Cloud Platform Integration)	Certificate based client authentication	Public key for certificate based client authentication	SAP generates a key pair and shares the public key with the customer. If you wants to use your own key pair, you can use the self service to generate it and add it to the keystore.	You have to import/add this public key in designated location at SFTP server	Optional	SAP cloud ops team will generate a key pair and create an alias "id rsa" or "id dsa" in keystore and will deploy it on SAP Cloud Platform Integration tenant. Public key from this key pair will be provided to the customer.

Direction	Protocol	Related Adapters	Authentication Method	Required Certificates	Where to Get Required Certificates	CERT Usage in Customer Sender or Receiver Systems	Customer-CA Signed CERT Required?	CERT Usage in Cloud Integration Keystore
				Public key fingerprint of SFTP server	Public key fingerprint of SFTP server will be provided by SFTP administrator or SAP cloud ops team.		Optional	Public key of SFTP sever must be mentioned in "known host" file and deployed on Cloud Integration SAP Cloud Platform Integration. Customer must provide it to SAP and this task will be done by SAP cloud ops.
SAP Cloud Platform Integration Outbound	SMTP	Mail	Basic Authentication/CEAM-MD5	Root and intermediate CAs from the mail server for TLS	Root and intermediate CAs from the mail server for TLS	Not required	Yes	You can manage your keystore using the self-service.

10 References

For more advanced help and information,see also the following standard resources for creating integration scenarios:

- SAP Cloud Platform Integration Community
- SAP Cloud Platform Integration Product Documentation
- SAP Cloud Platform Integration Roadmap on SMP
- SAP Cloud Platform Integration Learning Maps Link on Learning Hub
- SLAs and Maintenance Window
- SAP Data Privacy and Security Policy
- SAP Cloud Platform Integration Tools Information
- Available Standard Pre-Packaged Content

If you experience any technical issues, please create a ticket on **LOD-HCI**.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon ➦ : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
    - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
    - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon ➦: You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

www.sap.com/contactsap

THE BEST RUN SAP