Building block Configuration Guide
IF_Signavio_CALM_Process
July 2024
English

CUSTOMER

Community Solution: SAP Signavio Integration with SAP Cloud ALM

Content

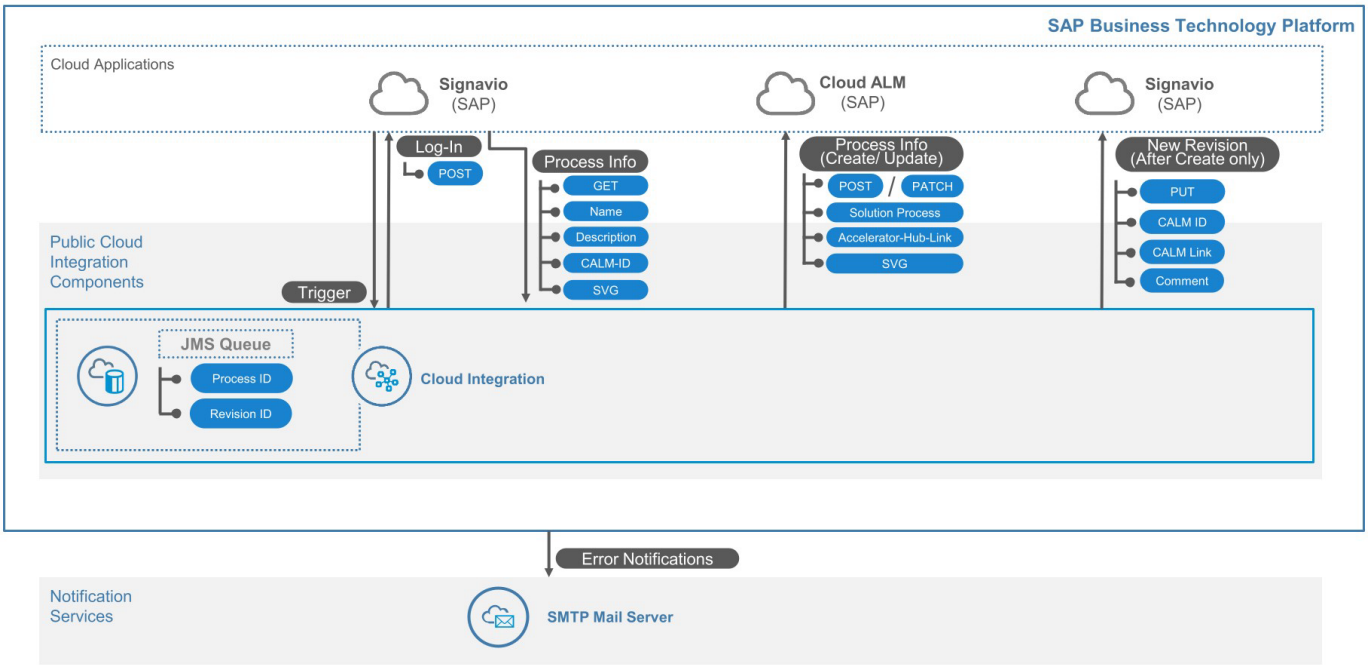
1 Introduction

By integrating SAP Signavio with SAP Cloud ALM, businesses can benefit from seamless data transfer for efficient business transformation. SAP Signavio offers powerful process modeling and analysis capabilities, enabling organizations to map out their current processes and identify areas for improvement. SAP Cloud ALM provides comprehensive application lifecycle management functionalities e.g. to implement new SAP solutions and process optimizations. This integration ensures that process changes can be effectively translated into requirements and deployed to production. Additionally, it fosters collaboration between business and IT teams, facilitating an extended approach to business transformation and driving overall organizational agility and efficiency.

SAP Cloud Integration is used in the following integration scenario to establish the communication between the systems SAP Signavio and SAP Cloud ALM as custom community solution. This integration is not an SAP standard product and therefore outside the scope of product support. It is rather a customizable community solution, offered by SAP, that enables organizations to enhance the template as desired, hence it falls within customer's accountability. It is possible to transfer process diagrams exclusively as .svg file with this community solution

This document lists the required set-up steps to be performed on SAP Cloud Integration, SAP Signavio and SAP Cloud ALM tenants to ensure a seamless integration of said systems and documents IFlow functionalities and information on security aspects.

How this integration is implemented is illustrated in the following diagram:



After the main flow has been triggered on the Cloud Integration Platform and the transferred process ID and revision ID have been stored via JMS queue, a log-in to Signavio is performed and subsequently information about the specific process is collected from there. This information is then used for either a create or an update of a Solution Process on Cloud ALM. In the case of a create operation, the final step involves a new revision of the process being put into Signavio, which contains additional information linked to the newly created solution process in Cloud ALM. If exceptions occur during the process an email server can be utilizes, sending a notification email.

Further details about the procedure are provided in the 'Documentation' chapter following hereafter.

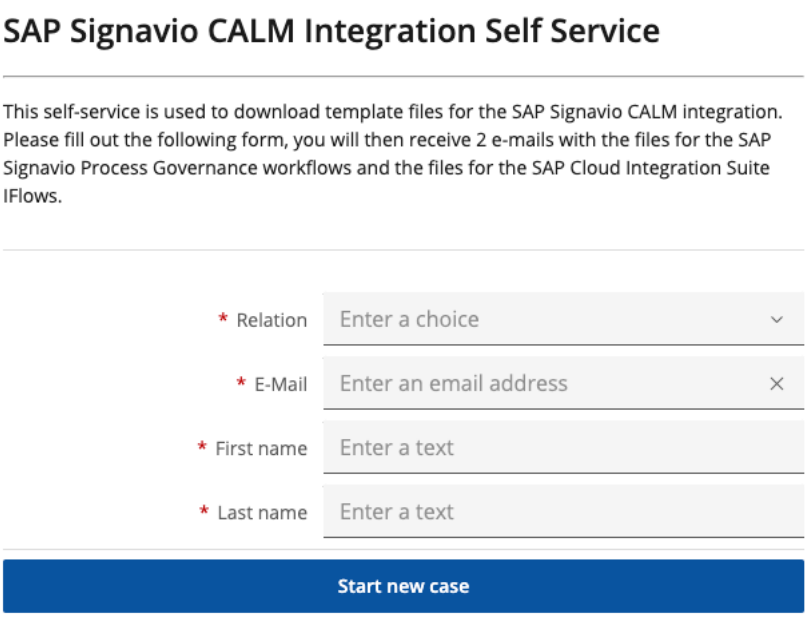
2 Self-Service

Before following this guide, we would recommend to use our self-service, which provides you the files for SAP Signavio Process Governance (bpmn) and for SAP Integration Suite (IFlows). You need to provide your e-mail, name and relation to SAP to use the self-service.

Link to self-service

https://workflow.signavio.com/public/start-form/6685410fd28aff198cd41546

Data to provide



Recommended: If you follow this documentation you will also find a guide on how to import the package from the Discovery section of your Integration Suite Tenant, which results in automatic maintenance due to automatic updates.

3 Prerequisites

Before starting the configuration, ensure that the following the steps described in this section have been performed:

3.1 SAP Integration Suite

Initial set-up of SAP Integration Suite:

The SAP Integration Suite is an open and versatile, multicloud-based Integration Platform as a Service (iPaaS) that is designed to support diverse needs of businesses. Please note that access to the appropriate SAP Cloud Platform cockpit is required in order to harness the functionalities of the SAP Integration Suite.

If this is the case, proceed with the following steps for an initial set-up:

1. Initial Sign-In and Access: Sign into the SAP Cloud Platform Cockpit. Use the correct account that allows you access to the SAP Integration Suite services.
2. Subscription to Process Integration Suite: Navigate to the Subscriptions pane in your subaccount. Look for the service *process-integration* (displayed as Process Integration Runtime). Here, subscribe to the service.
3. Setting Up Roles: In this step, you need to assign access permissions to the users for the SAP Integration Suite. Go to Security > Role Collections and create a new Role Collection. After it is created, add the desired roles to the new Role Collection.
4. Assigning Role Collection: Assign the Role Collection to the appropriate users, granting them access to the SAP Integration Suite.
5. Accessing SAP Integration Suite: It can be reached either via the SAP Cloud Platform Cockpit or directly through the URL (formatted like: https://XXXXX-iflmap.hcisbt.XX.hana.ondemand.com/itspaces). Once logged in, you can start the deployment and operation of IFlows.

A comprehensive guide on the initial set-up of the SAP Integration Suite can be found here.

Set-Up SAP Cloud Integration Tenant:

SAP Cloud Integration test and productive tenants are actively operational. Users within these tenants hold the permissions to copy the integration package, alongside configuring and deploying the IFlow. These abilities streamline the operations within SAP Cloud Integration and make the procedure more efficient and user-friendly. However, it is pertinent that in order to deploy security content, a user must be assigned the role of AuthGroup.Administrator. This specific role provides the user with the necessary permissions to deploy the security material within the tenant, thus maintaining the integrity and security of the SAP Cloud Integration platform.

Set-Up CPI-SMTP integration:

To establish a CPI-SMTP integration, it is crucial that the SAP Cloud Integration trusts the SSL certificate from the SMTP server we are integrating. To ensure this, the complete certificate chain from the server must be downloaded and imported into the SAP Cloud Integration tenant. Please refer to the relevant SMTP server's API documentation or their support teams for guidance on obtaining the certificate chain.

Proceed with the following steps to add the certificate:

1. Create an App Password for the SMTP server account as per their guidelines. Ensure that the password is secure and stored safely for future reference.
2. Have your SAP Cloud Platform Integration's Overview URL at hand. This URL should mirror the following format: https://xxxxx.hana.ondemand.com/itspaces, as would've been sent to you via email upon your subscription to SAP Cloud Integration.
3. Navigate to the *Monitor* page from the Overview page. Under the *Manage Security* section, click on *Security Material*. Set up User Credentials here using your SMTP server account details and the App Password created in Step 1.
4. In the *Monitor* page, perform a *Connectivity Test*. Download the certificates that authenticate the SMTP server against the SAP Cloud Integration from the resulting page.
5. Under the *Manage Security* section, click on *Keystore*. Here, import the certificates downloaded in Step 4.
6. Construct an integration flow IFlow. Make sure the *Credential Name* value matches the one created earlier while setting up the credential in Step 3.

In essence, configuring a CPI-SMTP integration revolves around creating an App Password for the SMTP server account, setting up credentials in CPI using this App Password, and importing and installing SMTP server certificates into CPI.

Set-Up Cloud ALM O Auth2 client credentials:

Proceed with the following steps to set up OAuth2 client credentials:

1. Access your SAP Cloud Platform Integration Suite and navigate to the *Monitor* view. Under the *Manage Security* section, select the *Manage Security Material* option.
2. In the *Manage Security Material* page, opt for *Add*, then select *OAuth2 Credentials.*

3. A dialog box for *Add OAuth2 Credentials* will open. Enter a distinct identifier in the *Name field*, such as *CLOUD_ALM_OAUTH2_CREDENTIALS.*
4. From the *OAuth2 Provider*, choose your respective Cloud ALM OAuth2 server.
5. Enter your specific *Client ID* and *Client Secret*—these should have been provided when your application was registered with the OAuth2 Provider.
6. After ensuring all pieces of information are accurately entered, click on *Deploy.*

Set-Up Auth for SAP Signavio

- Configure E-Mail, address password and tenant ID
- For security and audit reasons, we recommended that this user is a technical user assigned an *API Edition license* in SAP Signavio Process Manager. If you have no *API Edition* in your workspace, please create an incident in SAP for Me.

3.2 SAP Cloud ALM

Since the Community Solution implements an integration between SAP Signavio and SAP Cloud ALM some prerequisites must be fulfilled on SAP Cloud ALM side to be able to execute the transfer of process information.

In general, a full configured and accessible SAP Cloud ALM tenant needs to be available. How a SAP Cloud ALM tenant can be requested and configured can be found here: SAP Cloud ALM | SAP Help Portal and How_To_Get_Started_with_SAP_Cloud_ALM.pdf

Besides the general availability of the SAP Cloud ALM tenant, also administration rights on the BTP Global and Sub-Account on which the SAP Cloud ALM Tenant is entitled is needed.

3.3 SAP Signavio

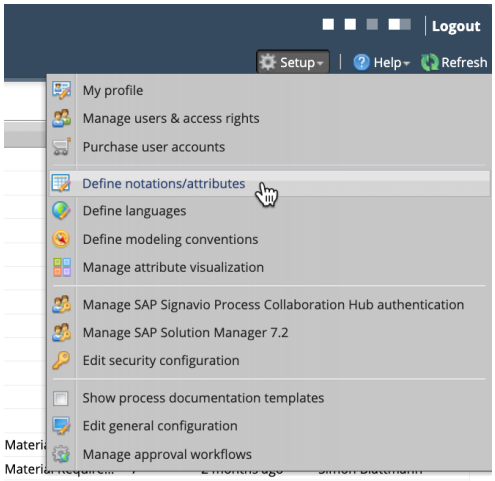
Besides a full configured Cloud ALM tenant also SAP Signavio must be in place and licensed. Following you can find the necessary prerequisites regarding licenses, access rights and actions needed as described below.

- Ensure that you have licenses and access to:
  - SAP Signavio Process Collaboration Hub
  - SAP Signavio Process Manager
  - SAP Signavio Process Governance, incl. established approval workflow

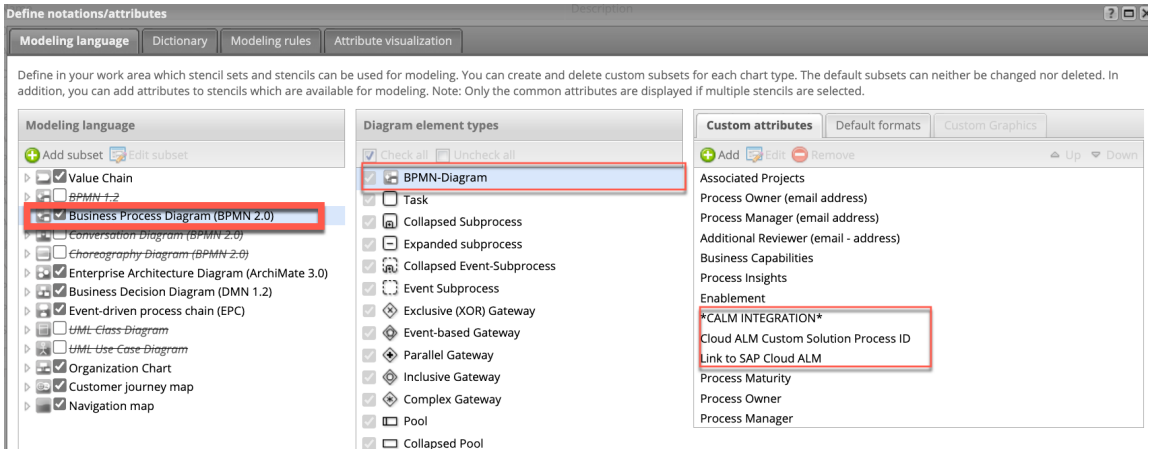
Create Custom Attributes in SAP Signavio Process Manager for CALM ID and URL

The community solution for the integration of SAP Signavio with SAP Cloud ALM technically uses two customer attributes. The first one to store information (CALM URL) and the second to update previous synced processes (CALM ID). Based on that technical concept, it is crucial to create those needed customer attributes first.

The configuration of Custom Attributes in SAP Signavio takes place in the Process Manager component underneath the setup option “Define notation/attributes”.

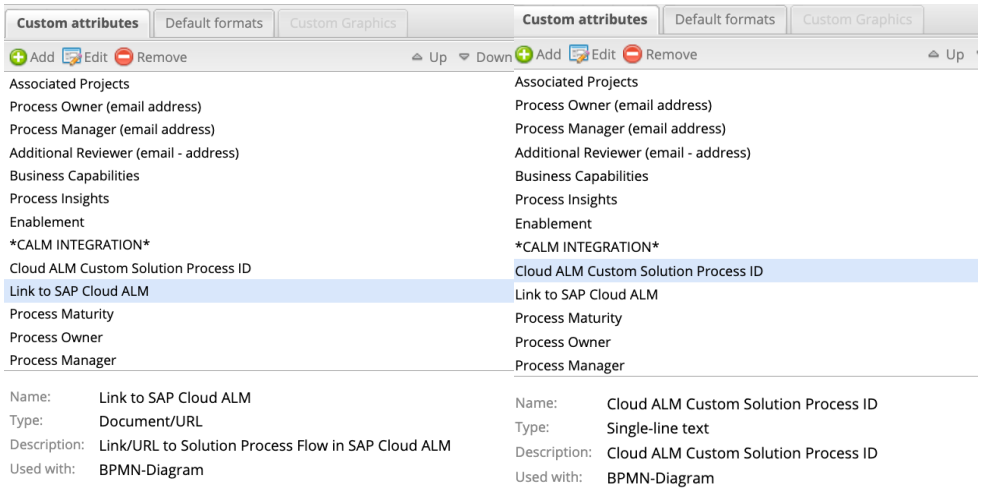


Inside the “Define notation/attributes” you are able to create custom attributes for different objects of SAP Signavio. Since we are transferring Process Diagram which were modelled as BPMN2.0 Diagrams, we need to create those two attributes underneath the element type BPMN-Diagram.



Since both custom attributes are used for different use cases the attribute types must be selected as follows:

- Cloud ALM Custom Solution Process ID = Single-line text
- Link to SAP Cloud ALM = Document/URL

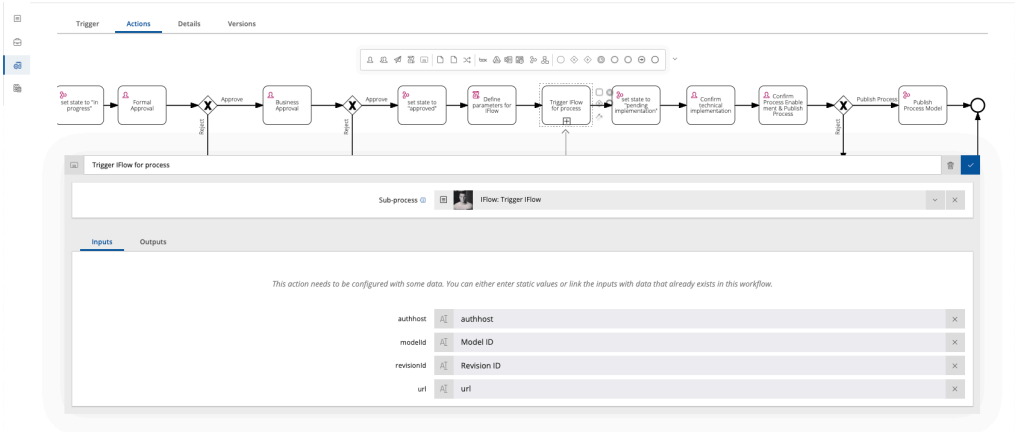


Setup trigger for SAP Integration Suite in SAP Signavio Process Governance Approval Workflow

Besides the Custom Attributes a trigger for calling the SAP Integration Suite is needed. With the Community solution we recommend using the SAP Signavio Process Governance Approval Workflow to trigger the synchronization and to call the SAP Integration Suite. For Methodology Recommendations please also look into the Methodology Usage Concept document attached to the community solution.

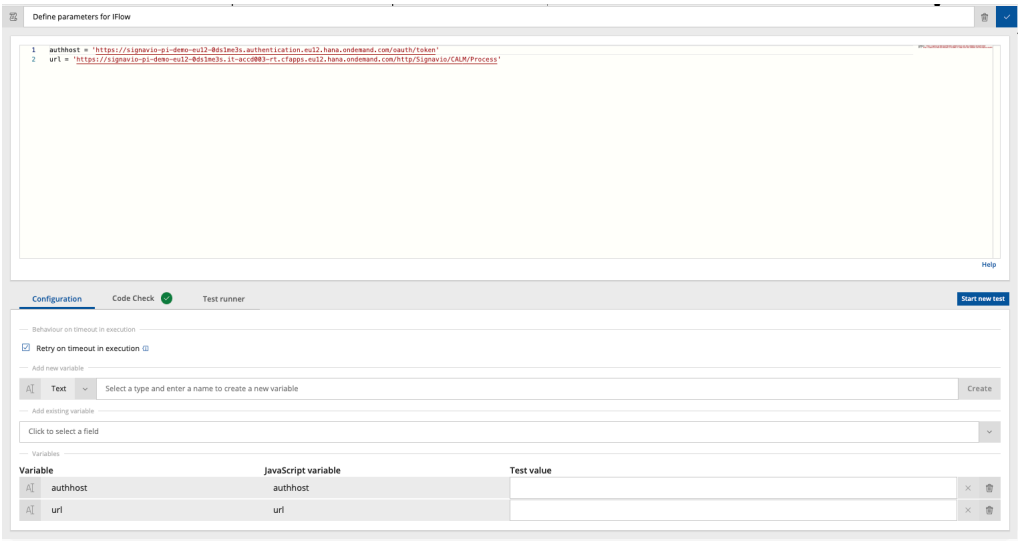
Step: Approval Trigger

The sub-process for triggering the IFlow is included in the approval process. It is recommended to include it after all approvals have been performed. To define the parameters, a JavaScript task is recommended in which authhost and url can be defined; alternatively, this step can also be carried out directly in the sub-process task.



- Inputs: authhost, Model Id, Revision Id, url
- Outputs: responseIflow (whole response), responseBodyIFlow (only the stringified body)
-

JavaScript Tasks



- Define authhost and url in this task.

Step: Trigger IFlow

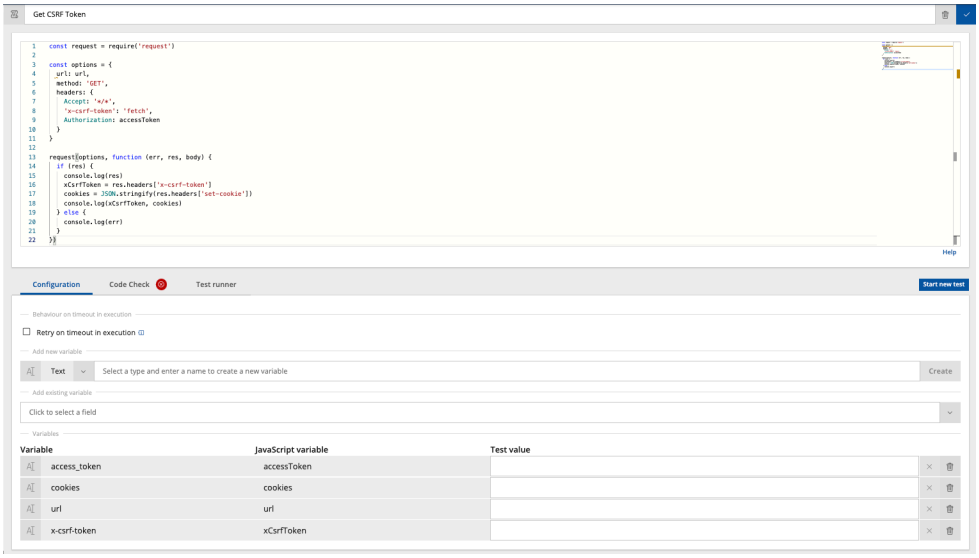
In the 'Trigger IFlow' sub-process, another sub-process is triggered which performs an OAuth using authhost and the credentials in the sub-process and returns the token. This token can now be used to retrieve the csrf token and the cookies for the actual triggering of the IFlow.

The IFlow is then called, and the model ID and revision ID are transferred. A detailed description of the subprocess is not necessary.

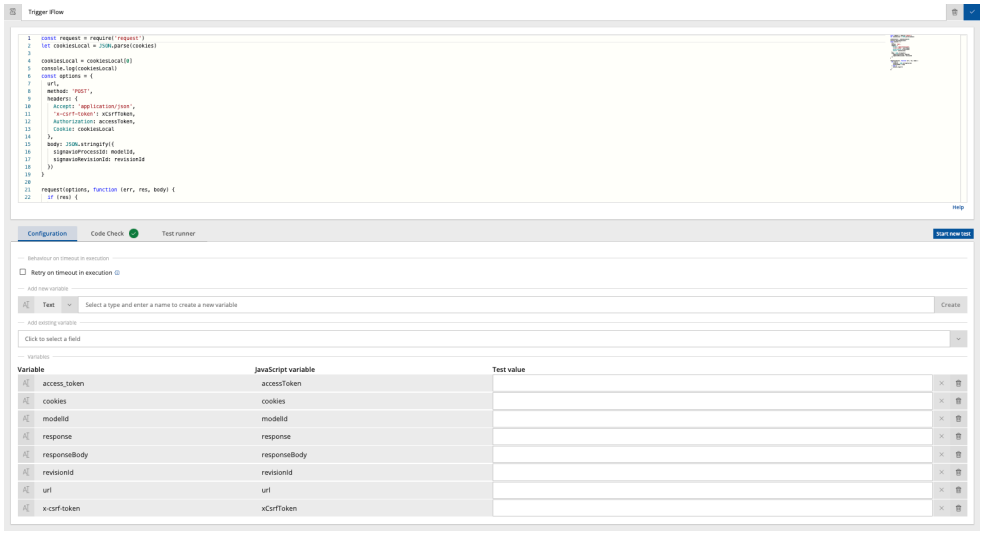
In this step the transfer of the authhost and the definition of the authtoken is important, as well as the definition of the credentials in the subprocess, see Screnshot 'JavaScript Tasks'.

- Inputs: authhost
- Outputs: access_token

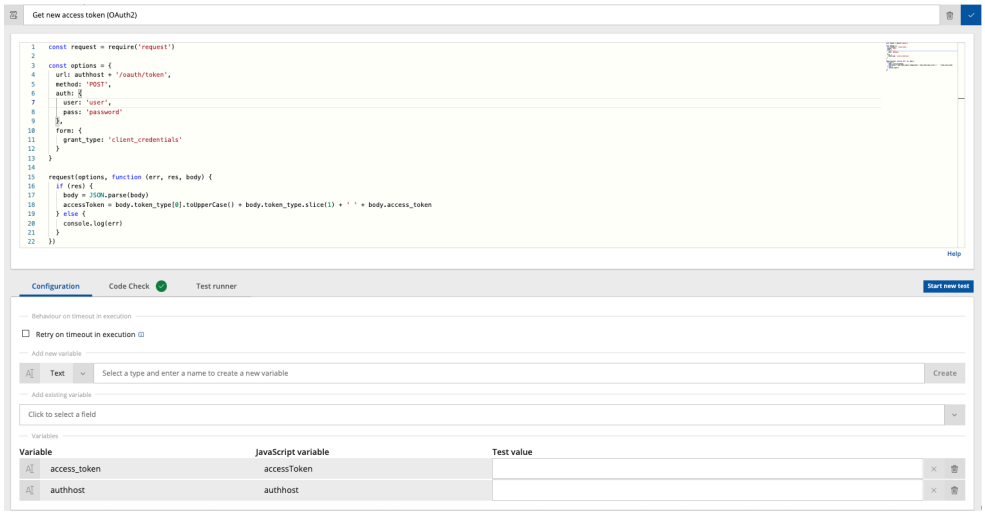
JavaScript Tasks



- In general, nothing needs to be done in this task



- In general, nothing needs to be done in this task



- Define user and pass in line 7 and 8

4 Documentation

The Integration Suite package contains the integration artifacts and the documentation for configuring the integration betweeen SAP Signavio and SAP Cloud ALM to import data between the two applications. This data includes general information, links and an image of the *Solution Process* flow.

The two IFlow artifacts the package contains are IF_Signavio_CALM_Process and IF_Send_Error_Notification_Email.

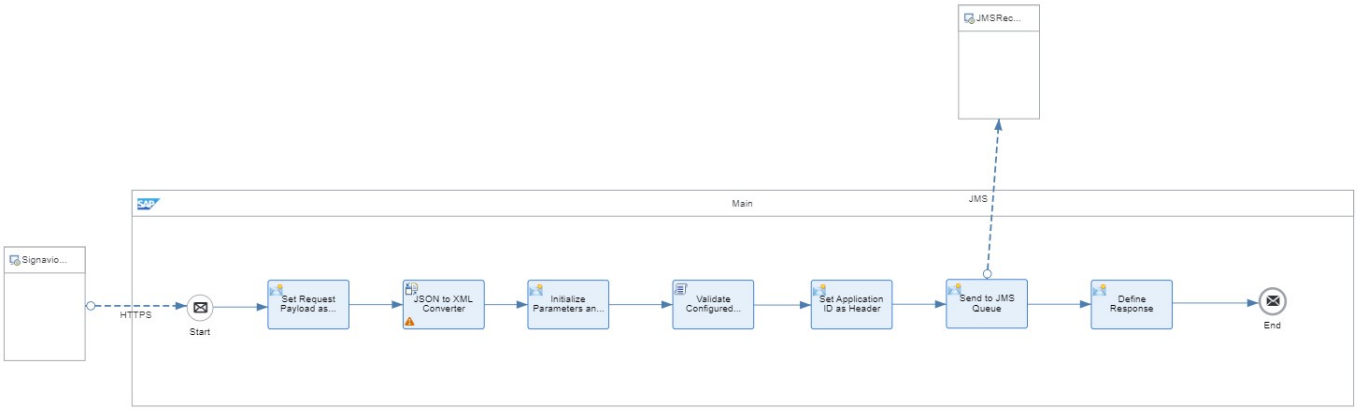
4.1 IF_Signavio_CALM_Process

This IFlow aims to synchronize processes between the applications SAP Cloud ALM and SAP Signavio. It features several configurable parameters including the fields for *Cloud ALM Credentials, Cloud ALM Region*, *Cloud ALM Tenant*, *ID Field of CALM Custom Solution Process*, *Link Field of CALM Custom Solution Process*, *Signavio Credentials*, *Signavio Host Link, Signavio Model Link*, *Signavio Tenant ID* and the options *Enable Pre-Exit Extension*, *Enable Post-Exit Extension, Enable Error Mail Notification* and *Enable Log Attachments*. Said options can be enabled using the value 'x', 'true' or 'yes'. Configurations regarding Sender systems (HTTPS-Trigger Adapter, JMS Sender) and Receiver systems (JMS Receiver, HTTP-CALM-Adapter, ProcessDirect-IFlow-Adaper) are also feasible. A variant of this IFlow useing the CPI-internal *Data Store* operations instead of a JMS queue is also available and can be requested as well.

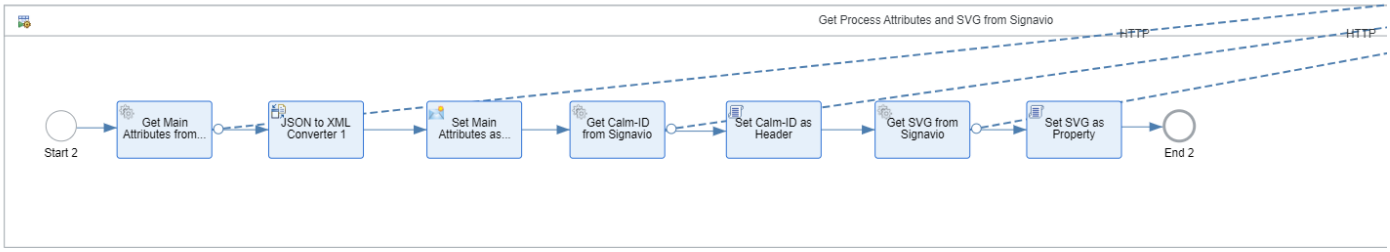
The IFlow is initially triggered via an HTTPS request coming from SAP Signavio after a certain process was scheduled to be published.

The request passes on two parameters in JSON format: *signavioProcessId* and s*ignavioRevisionId*. For instance, a transferred payload looks as follows:

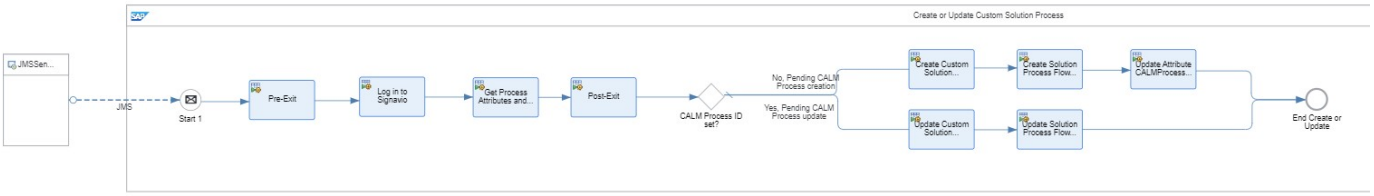
```
{
 "signavioProcessId": "aedcd0a4d8c543e7a7ab2f15f89eb65a",
  "signavioRevisionId": "7df632ad07d14f9fb5c801499a49c9c8"
}
```



After successful handover via JMS, the IFlow initiates the log- in to SAP Signavio, retrieves process attributes like *Description*, *Name*, and *Calm-ID* and fetches the corresponding *CalmCustomProcessID* to save it as Header. An image of the respective process in form of an SVG is stored as property hereafter.



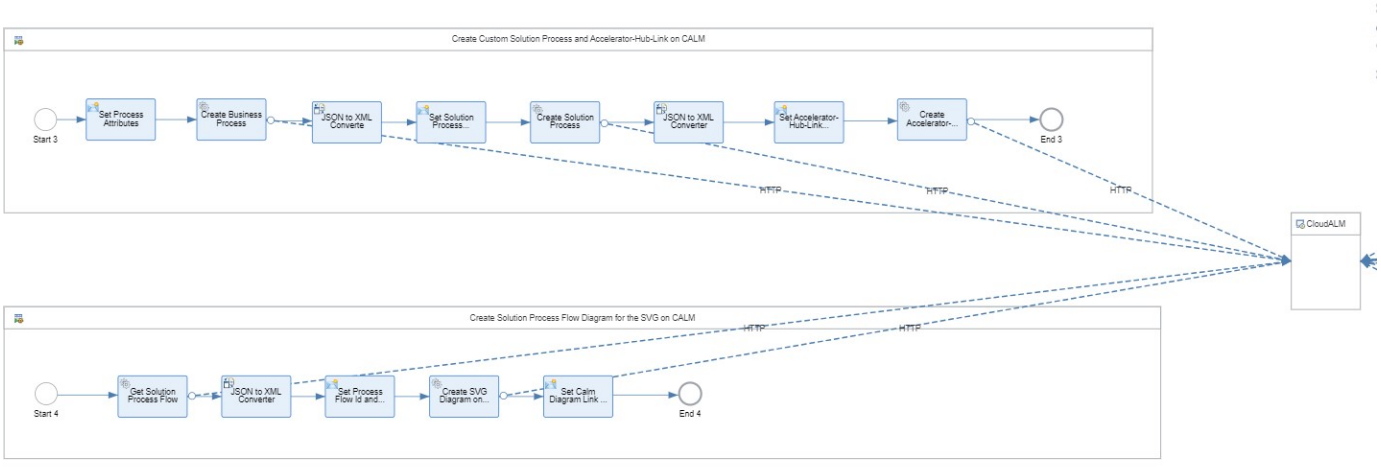
The subsequent router component checks, if the value of *CalmCustomProcessID* is equal to null. It accordingly directs an *Update Calm Process* path (if an ID already exists) or a *Create Calm Process path* (if the value is null).

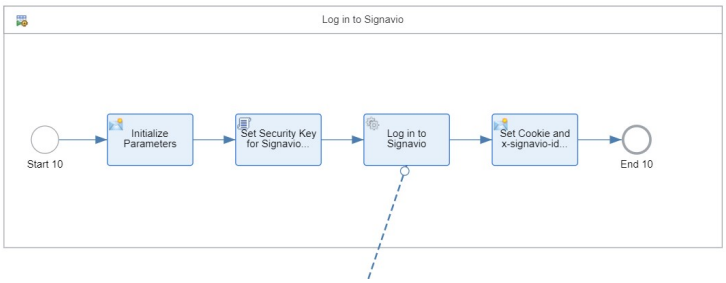


In case of the Create-Path, a *Business Process* as base and (associated to this *Business Process ID*) a subsequent *Solution Process* are created on SAP Cloud ALM as first step.

For that *Solution Process* an *Accelerator-Hub-Link* (that refers to the model on Signavio's Process Collaboration Hub) is created and added as well.

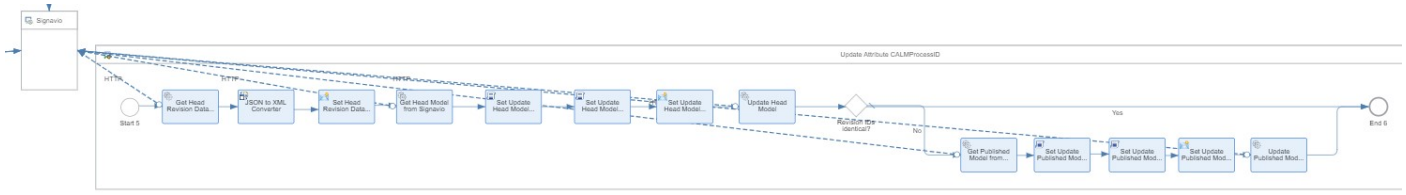
As second step, the generated *Process Flow ID* is retrieved from Cloud ALM and used to add the stored SVG to the *Solution Process*.





At this point an update of the process on SAP Signavio is performed by creating a new process revision on SAP Signavio's Process Collaboration Hub. that contains a link to the newly created process on Cloud ALM, as well as the generated *CALM ID* and a revision comment in which this ID is also mentioned.

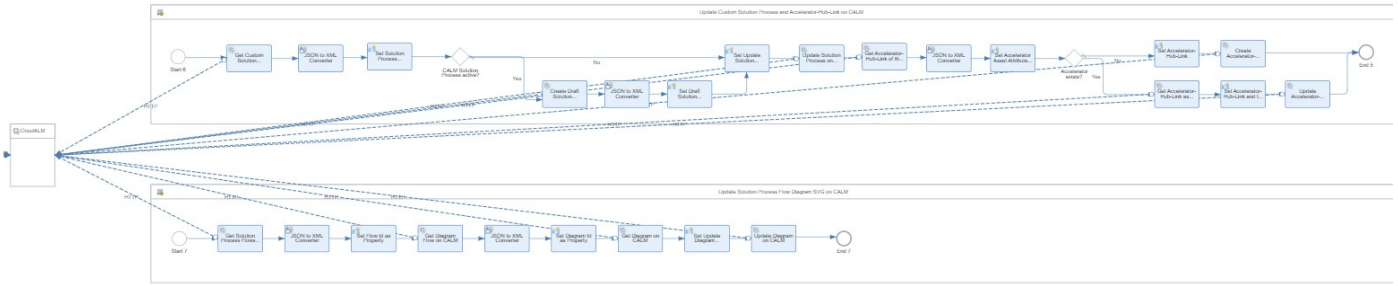
Required attributes for the payload to be transferred are retrieved from Cloud ALM and initially added to the Head-Revison in SAP Signavio via PUT request. By default, the *Head-Revision* the highest revision of the process in question with the given Process ID. A router component checks whether the *Head-Revision* is identical to the *Published-Revision* with the given *Revision ID*. If not, the revision of the published process is explicitly updated as well- in that case, the Process on Signavio Process Collaboration Hub obtains two additional revisions with identical comment, *CALM ID* and *CALM Link* but potentially deviating diagrams, as they rely on separate revisions as base.



In case of the Update-Path *name*, *description*, S*olution Process ID* and *external ID* (process ID from Signavio) of the *Solution Process* on Cloud ALM are updated as first step. The *Solution Process* is retrieved using the *CALM ID* and the attributes required for the PACTH request from CALM are obtained. A router component is then used to check whether the status of the Solution process is *ACTIVE* or not. If so, a new *Solution Process* with status *DRAFT* and associated Solution Process is created. Then, again in both cases, the mentioned attributes are replaced on the *Solution Process*.

The *Accelerator Hub Link* related to the *Solution Process* is also updated so that it points to the process with the specific revision of the process on Signavio that corresponds to the current *revision ID* and is therefore the reference for the current version on Cloud ALM. If no *Accelerator Hub Link* is assigned to the Solution process because the latter was newly created previously, a router initiates the *Create-Accelerator-Hub-Link* path, otherwise the *Update-Accelerator-Hub-Link* path is followed directly.

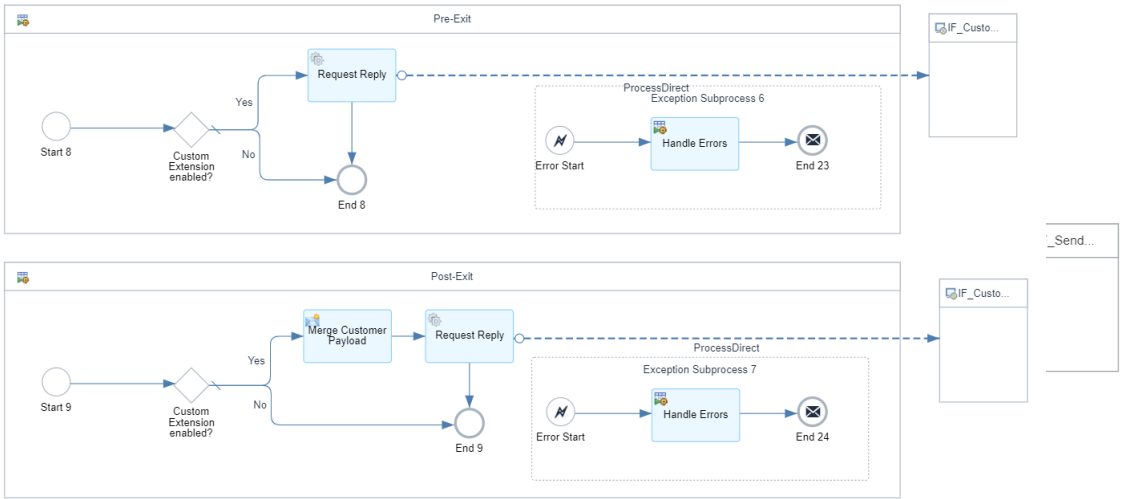
In the second step, the process model is updated in the form of SVG image and designation. The *Flow ID* and *Diagram ID* attributes required for the PATCH request are retrieved beforehand on Cloud ALM and then the update procedure takes place



for the process model as well.

In addition to the main path, the IFlow also offers features for custom enhancements in the form of pre and post exits.

In relation to error handling, the IFlow provides exception sub processes for each local integration process, which forward the error messages to the defined error handling. Depending on how the parameters for the log attachment and e-mail notification were set, it may issue the error to the *IF_Send_Error_Notification_Email* for further processing IFlow. In case of *an Service*



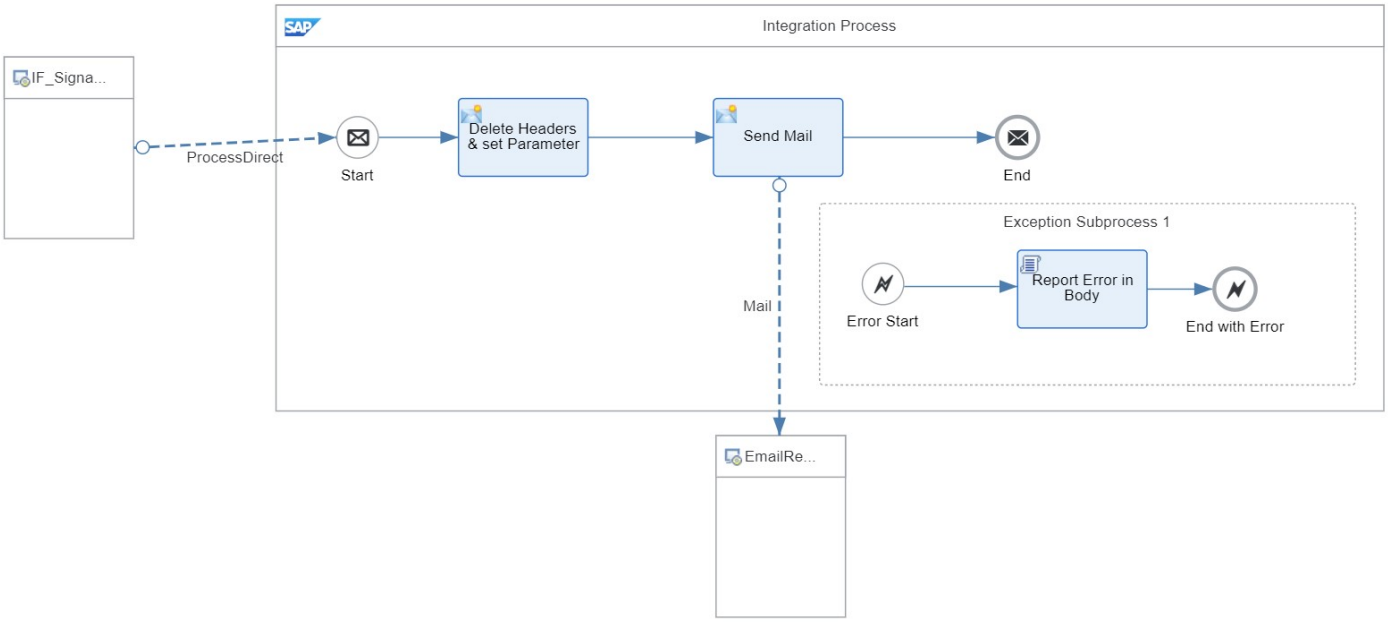
unavailable code error 503, the whole process ends with an *error end event* and the JMS queue starts retries according to the configured values. For any other error code, the whole process ends with an *escalation end event* and nor retries are triggered afterwards.

In summary, this IFlow ensures a synchronization between CALM and Signavio by either creating or updating Signavio-specific process information from Signavio to CALM and subsequent return of CALM-specific process information back to Signavio.

4.2 IF_Send_Error_Notification_Email

When the main IFlow *IF_Signavio_CALM_Process* fails and throws an exception and the configuration-field *Enable Error Mail Notification* is set on *Yes, true or x*, this IFlow sends an e-mail to a configured address.

It features configurations regarding connections or processing of the sender system in terms of ProcessDirect-IFlow-Adaper and Email-Receiver system. The option *Attach Exception Error* can be enabled using the value ‘x’, ‘true’ or ‘yes’.



After the *AttachExceptionError* property has been defined, an email with the subject *Error Notification for SAP Signavio Integration with SAP Cloud ALM* is sent to a configured mail address. The text of this email uses the body previously set in *IF_Signavio_CALM_Process* and contains the following information:

Error Notification for SAP Signavio Integration with SAP Cloud ALM

[redacted]@gmail.com
An Zoller, Isabel

Antworten | Allen antworten | Weiterleiten

Mon 15/04/2024 10:18

Integration Flow Name:	IF_Signavio_CALM_Process
Message Processing Log ID:	AGYc4qN7OladKPT3dKvSzmgILP2T
Message Processing Log Correlation ID:	AGYc4qKp2RV6Orbth4RZOH7RsK8-
Timestamp:	Mon Apr 15 08:17:40 UTC 2024
Process-ID:	0b7bd312d33a4c3a982fd14d4a50195c
Revision-ID:	aa844c54b1d84f9c8c5db3ae6852667f
Exception Message:	HTTP operation failed invoking https://[redacted]/api/calm-processauthoring/v1/businessProcesses with statusCode: 400
Response body:	{"error":{"code":"400","message":"Business Process name already exists"}}

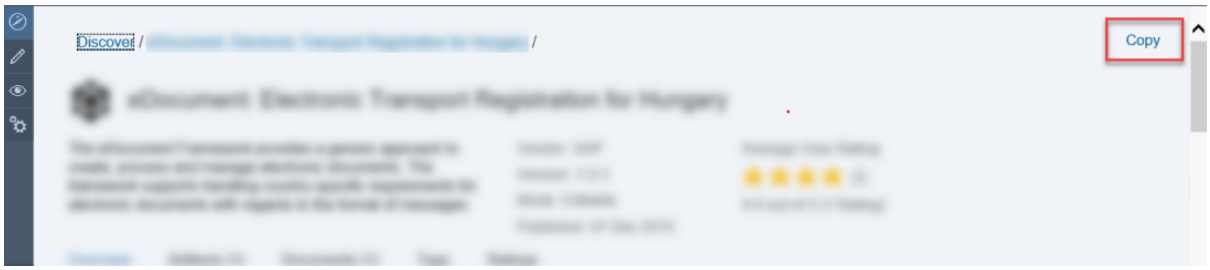
If during the mail receiver connection a malfunction occurs and triggers an exception, e.g. unavailable mail server address or incorrect mail credentials, the exception sub process is initiated. Here, with the help of a groovy script, the error message is summarized with exception class and exception message and (if the property *AttachExceptionError* is set to ‘yes’, ‘true’ or ‘x’) made available as attachment *ErrorDetails*.

5 Configuration steps on SAP Cloud Integration

5.1 General

Copy Published Package:

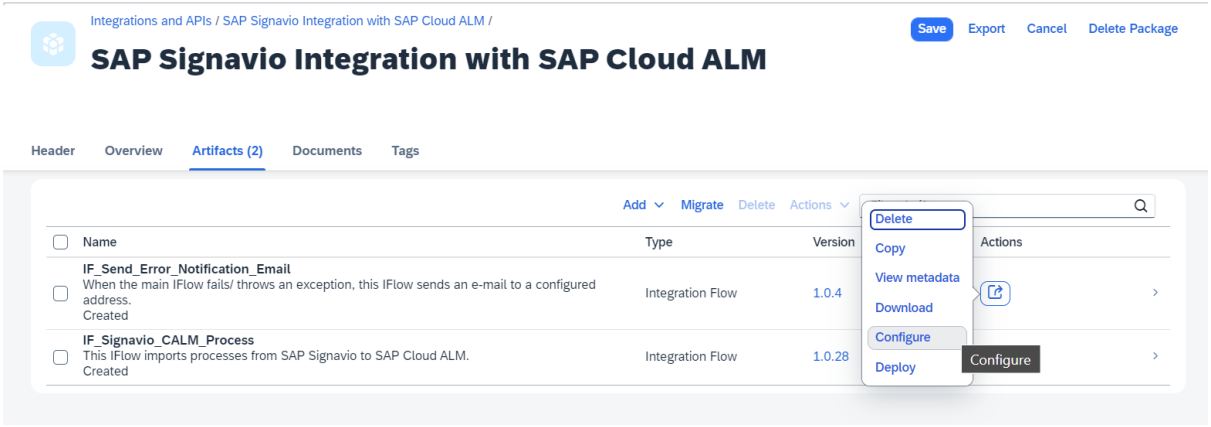
1. In the *Discover* section of your tenant, select the package *SAP Signavio Integration with SAP Cloud ALM*.
2. Select the package and choose *Copy*.



3. In the *Provide suffix* dialog box, leave the field blank and choose *Ok*.

Configure IFlow:

1. Choose *Design* from the upper left corner of the page.
2. Click on the package that you copied from the original *SAP Signavio Integration with SAP Cloud ALM*.
3. Go to the *Artifacts* tab page.
4. Click on *Actions* → *Configure* for either the *IF_Send_Error_Notification_Email* or the *IF_Signavio_CALM_Process* IFlow.



5. Choose one after the other the *Sender*, *Receiver* and *More* tab to enter the configurations listed below.
6. Click on *Deploy* in the lower right corner and wait until the message of the successful deployment pops-up.

5.2 IF_Signavio_CALM_Process

Configure Sender Adapter

JMS Sender Adapter	Queue Name, Retry Interval (in min), Maximum Retry Interval (in min)	Connection details include: - Name of the JMS Queue sending the process-ID messages - The retry interval, that describes the time between a failed process (due to server unavailability) is triggered again with the same process-ID message - The maximum retry interval, that describes the limit to avoid an endless increase of the retry interval caused by exponential backoff settings (i.e. time intervals between retry attempts to send a message after a failure increase exponentially)

HTTPS Adapter	Address, Authorization, CSRF Protected Checkbox, Body Size (in MB)	This HTTPS Adapter functions as sender from SAP Signavio that triggers the IFlow and subsequent process import to SAP Cloud ALM at the beginning. Connection details include: - Address from SAP Signavio sender for IFlow Trigger - Dropdown selection of authorization in terms of client authentication type - Checkbox, whether the adapter covers CSRF security measures (i.e. preventation of Cross-Site Request Forgery attacks through the use of unique session tokens) Connection details include: - The maximum body size that is being sent

Configure Receiver Adapter

JMS Receiver Adapter	Queue Name	Processing details include: - Name of the JMS Queue receiving and storing process-ID messages
ProcessDirect Adapter	Address (to /custom/pre_exit IFlow)	Connection details include: Address from sender IFlow for ProcessDirect Trigger to begin a pre-exit extension process (if applicable)
ProcessDirect Adapter	Address (to /custom/post_exit IFlow)	Connection details include: Address from sender IFlow for ProcessDirect Trigger to begin a post-exit extension process (if applicable)
ProcessDirect Adapter	Address (to IF_Send_Error_Notification_Email)	Connection details include: - Address from sender IFlow for ProcessDirect Trigger to begin the error notification process

Configure Parameters

Text Field	Cloud ALM Credentials	Name of created OAuth 2.0 Client Credentials via Security Material for SAP Cloud ALM Account Also configurable via: Receiver → Cloud ALM → Credential Name
Text Field	Cloud ALM Region	Cloud Foundry region identifiers e.g. 'eu20' or 'us10'
Text Field	Cloud ALM Tenant	The name of the tenant, the process is going to be imported to
Yes/No Option	Enable Error Mail Notification	Valid, positive values are: - 'yes', 'x' or 'true' (regardless of upper or lower case) Anything else is read as 'no'
Yes/No Option	Enable Log Attachments	Valid, positive values are: - 'yes', 'x' or 'true' (regardless of upper or lower case) Anything else is read as 'no'
Yes/No Option	Enable Post-Exit Extension	Valid, positive values are: - 'yes', 'x' or 'true' (regardless of upper or lower case) Anything else is read as 'no'
Yes/No Option	Enable Pre-Exit Extension	Valid, positive values are: - 'yes', 'x' or 'true' (regardless of upper or lower case) Anything else is read as 'no'

Text Field	ID Field of CALM Custom Solution Process	Given name of a custom field on SAP Signavio for the *SAP Cloud ALM Solution Process ID* (not the value itself) E.g. 'meta-cloudalmcustomsolutionproce'
Text Field	Link Field of CALM Custom Solution Process	Given name of a custom field on SAP Signavio for the Link to the *Solution Process Model* on SAP Cloud ALM (not the value itself) E.g. 'meta-linktosolutionprocessflowdi'
Text Field	Signavio Credentials	Name of created User Credentials via Security Material for SAP Signavio Account
Text Field	Signavio Host Link	Base-URL that directs to the Signavio website e.g. 'https://editor.signavio.com'
Text Field	Signavio Model Link	Extended URL that directs to a specific model, if a model-Id is appended to it e.g. 'https://editor.signavio.com/p/hub/model/'
Text Field	Signavio Tenant ID	Signavio-specific numerical ID of whichever tenant the process to be imported is located on

5.3 IF_Send_Error_Notification_Email

Configure Sender Adapter

ProcessDirect Adapter	Address (from IF_Signavio_CALM_Process)	Connection details include: - Address from sender IFlow for ProcessDirect Trigger

Configure Receiver Adapter

SMTP Adapter	Address, Credential Name, From, To, Subject	Connection details include: - Mail address (e.g. smtp.gmail.com:465) - Mail Credential name (created User Credentials via Security Material) Processing details include: - 'From' and 'to' mail addresses - Mail title

Configure Parameters

Yes/No Option	Attach Exception Error	Valid, positive values are: - 'yes', 'x' or 'true' (regardless of upper or lower case) - Anything else is read as 'no'

6 Security Aspects

SAP Integration Suite is designed with robust security measures, offering an encrypted and secure platform for data management and transfer. It promises enterprise-grade security, leveraging a variety of features including end-to-end security, advanced identity, and access management, regular auditing, updates, disaster recovery measures, and scalable solutions that grow with business.
The end-to-end security feature ensures that the data remains protected from the point of entry until it reaches its destination. SAP Integration Suite ensures this using HTTPS, SSL, and other secure protocols to encrypt data in transit.

In the realm of Identity & Access Management, the Integration Suite maintains strict authorization protocols. It ascertains that only the personnel with the correct permissions can gain access to specific data, mitigating the risk of unauthorized access. With state-of-the-art data encryption techniques, SAP ensures that data stays secure both when at rest and in transit. The platform meets industry standard encryption methods, offering advanced levels of protection.
It offers compliance support tools that simplify the management, tracking, and reporting of your compliance standing. Moreover, each setup procedure, be it for the SAP Cloud Integration Tenant, CPI-Gmail SMTP Integration, Cloud ALM OAuth2 Client Credentials, or Signavio User Credentials, has specific security considerations to be accounted for.

For the SAP Cloud Integration Tenant, the concept of role-based access control constitutes a critical security aspect that can prevent unauthorized access or misuse. Notably, a user must be assigned the AuthGroup.Administrator role to deploy security content, thereby ensuring only authorized personnel are granted these permissions, reducing the risk of breaches.
The CPI-Gmail SMTP Integration set-up process depends on the use of SSL certificates and one-time use passwords (App Passwords) to secure communication with the Gmail SMTP server. However, a careful approach to storing these application passwords is needed to further enhance security.
For Cloud ALM OAuth2 Client Credentials, the use of unique client credentials (client ID and client secret) ensures secure communication between the SAP Cloud Platform Integration Suite and the OAuth2 server. Protecting these client credentials from exposure is essential.
Lastly, the Signavio User Credentials set-up deals with sensitive user data used for authentication, which must be securely managed.
Particular attention is brought here to the necessity of password encryption and secure handling to prevent unauthorized access.

Regardless of the robust and secure ecosystem, there is a specific security risk due to the technical requirements for the Signavio login in the *IF_Signavio_CALM_Process* IFlow. In the local integration process *Log in to Signavio*, the groovy script component *SetSignavioLogInBody* sets a body and passes it to an SAP Signavio API. This body has the following structure:

tokenonly=true&name=Max.Mustermann@sap.com&password=Eg12345&tenant=6p08f41ce7pc4a6ga92461e1ca2a0d1w

The password retrieved by the SecureStoreService is therefore converted to plain text when it is URL-encoded as request payload.
As a result, this password is visible in plain text for an administrator in case the IFlow trace function is activated. This poses a potential security risk as malicious actors, given access to the trace, could exploit this plain text visibility.

In conclusion, SAP Integration Suite provides multi-faceted security measures. However, certain security gaps like the plain text password visibility within the *IF_Signavio_CALM_Process* trace, underscore the importance of constant vigilance and optimization in the realm of data security. Regular security audits, password updates, role assessments, and sensitive data handling considerations can play a substantial role in maintaining the security integrity of SAP Integration Suite. Therefore, security risks regarding the provided package with respective IFlow artifacts for the *SAP Signavio* and *SAP Cloud ALM* integration in question must be considered on a case-by-case assessment.