

Integration Guide

CUSTOMER

SAP SuccessFactors Employee Central

Version: May 2024

SAP SuccessFactors Employee Central to SAP Access Control Integration Using SAP Cloud Integration

Contents

1	Introduction	5
1.1	Target Group	5
1.2	Prerequisites.....	5
1.3	Related Guides.....	6
2	Integration Overview.....	9
2.1	Overview Illustration	9
2.2	SuccessFactors Integration Scenarios.....	10
2.2.1	Add New Employee.....	10
2.1.2	Change Employee Job Data	11
2.1.4	Terminate Employee.....	12
3	Configuring SAP SuccessFactors Employee Central.....	13
3.1	Web Service Setup.....	13
3.2.1	Set Permissions for API User	16
4	Configuring SAP Access Control	17
4.1	Prerequisites.....	17
4.2	Activating the Web Services	19
4.3	Create Binding for WS	22
4.4	Creating Request Types.....	24
4.5	Creating Request Priorities	27
4.6	Maintaining Settings for HR Trigger	28

4.7	Configuring the BRF+ Application SFEC_HR_TRIGGER_APP	30
4.8	Mapping the BRF+ Function ID to SAP Access Control.....	36
4.9	Maintaining Rule-to-Role Mapping	38
4.10	Generating the BRF+ Function for Access Rule-to-Role Mapping	42
4.11	Configuring the BRF+ Decision Table.....	45
4.12	Mapping BRF+ to SAP Access Control Application IDs	64
4.13	Locating URLs for SAP Cloud Integration	66
5	Configuring SAP Cloud Integration Process	68
5.1	Configure SAP Cloud Connector Settings	68
5.2	Configure User Credentials for SFEC and GRC System	70
5.2.1	Configure GRC User Credentials	70
5.2.2	Configure SFEC User Credentials	71
5.3	Configure and Deploy iFlows	72
5.3.1	Configure and Deploy iFlow - SuccessFactors Employee Central to SAP GRC Access Control Integration for Employee Authorization_OData.....	78
5.3.1.1	How to get the SFEC OAuth2 SAML Bearer Assertion	82
5.3.1.2	How to Register OData Service in GRC system.....	85
5.3.1.3	- How to configure Cloud Connector.....	86
5.3.1.4	How to schedule new background job.....	88
5.3.2	Configure and Deploy iFlow - SAP SFEC to SAP GRC AC Integration for Employee Authorization_PP.....	89
5.3.2.1	Configuring Principal Iflow Trigger.....	94

5.3.2.2	Configuring OAuth2 Client Credentials in CPI Security Material.....	96
5.3.2.3	Configuring Cloud Connector and Backend on-Premises GRC system.....	98
5.3.2.4	Configure the SAP Gateway.....	103
5.4	How to get the SAP Cloud Integration Client Certificate	108
5.5	View and Extend the Deployed iFlows using SAP Eclipse (Optional).....	108
5.5.1	Download the iFlow Projects on Your Desktop.....	109
5.5.2	View the configured certificates and externalized parameters.....	110
5.5.3	Extend the project in Eclipse and Deploy	110
6	Monitor Phase: Monitor Messages Across Systems	111
6.1	Initial Load	111
6.2	Delta Load	111
6.3	Field Mapping in SAP Cloud Integration.....	112
7.	Data Integration Concepts	117
7.1	Transferring Employee Change Data	118
7.2	Staging Tables	119
7.3	OData Services and SOAP Messages.....	120
7.4	Extending the Data Transfer Process.....	121
8	Monitoring the Integration Process	122
8.1	SAP Web Service Utilities	123
8.1.1	SAP Message Monitor	124
8.2	SAP Application Log	125

8.3	Employee Central SFAPI Audit Log.....	127
8.4	Process Reporting in SAP Cloud Integration	129
8.4.3	Messages in SAP Web Service Utilities	130

1 Introduction

The purpose of this guide is to document the integration of SAP SuccessFactors Employee Central with SAP Access Control using SAP Cloud Integration.

After executing the steps described in this document you will be able to transfer SAP SuccessFactors Employee Central data to SAP Access Control to perform user provisioning.

Caution

Usage of any integration software and content provided with the SAP Business Suite or SAP Access Control and applicable to integration between the SAP Business Suite or SAP Access Control and SAP SuccessFactors Employee Central is permitted only with SAP Access Control and a valid, current contract for SAP SuccessFactors Employee Central.

1.1 Target Group

The intended audience for this guide is:

- SAP Access Control professional services and consultants
- SAP SuccessFactors consultants
- SAP Cloud Integration consultants
- System/cloud administrators

1.2 Prerequisites

We assume that readers of this guide have basic knowledge in the following areas:

- SAP Access Control configuration and operation
- BRF+
- SAP SuccessFactors Employee Central configuration and operation
- SAP SuccessFactors provisioning
- SAP HANA Cloud Integration

1.3 Related Guides

The table below shows other guides that might be relevant in the integration of SAP SuccessFactors Employee Central with SAP Access Control.

Related guide	Type of the related guide	Content of the related guide	How is the guide related to the current guide?
<p><i>Employee Central Master</i></p> <p>For the most current version of the guide see the SAP Help Portal at:</p> <p>http://help.sap.com/cloud4hr under <i>Employee Central</i> → <i>Implementation Guides</i>.</p>	Implementation Guide	How to set up Employee Central	Before transferring employee change data to SAP Access Control, you need to set up Employee Central itself.
<p><i>SF API Programmer's Guide</i></p> <p>For the most current version of the guide see the SAP Help Portal at:</p> <p>http://help.sap.com/hr_api</p>	General programming guidelines		Contains a list of URLs Compound Employee API endpoints for SAP SuccessFactors Employee Central

Related guide	Type of the related guide	Content of the related guide	How is the guide related to the current guide?
<p><i>Implementing the Compound Employee API</i></p> <p>For the most current version of the guide see the SAP Help Portal at</p> <p>http://help.sap.com/hr_api/ under <i>SuccessFactors HCM Suite</i> → <i>Employee Central</i></p>	User Guide	Explains the Compound Employee application programming interface (API) for SAP SuccessFactors Employee Central	Describes how to enable the <i>Compound Employee API</i> in provisioning and role-based permissions Implementation is required to run the integration and read data from Employee Central.
<p><i>SAP Access Control Documentation</i></p> <p>http://help.sap.com/grc-ac :</p> <ul style="list-style-type: none"> • Application Help • Configuration Settings Guide 	Application Help Configuration Settings Guide		Provides information about SAP Access Control functionality.
<p>SAP Access Control IMG</p> <p>In the SAP Access Control system, choose transaction <i>SPRO</i> → <i>SAP Reference IMG</i> → <i>Governance, Risk, and Compliance</i> → <i>Access Control</i> → <i>User Provisioning</i></p>	Configuration for user provisioning	Steps to set up user provisioning in SAP Access Control	Provides detailed instructions for configuring SAP Access Control.
<p>Business Rule Framework Cookbook</p> <p>SAP Community Network – http://scn.sap.com</p>	Tutorial	Basics of using BRF+	Provides information on how BRF+ works.

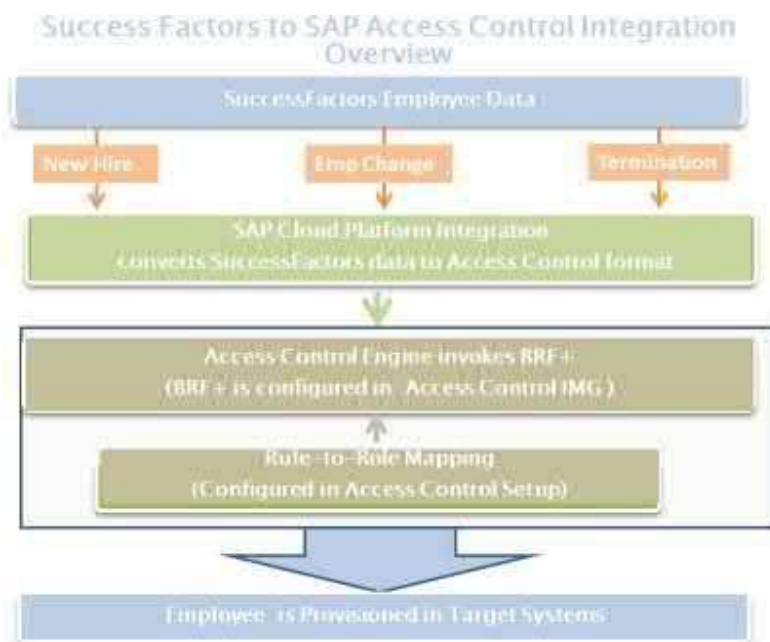
<p>HANA - Secure Connections</p> <p>For the most current version of the guide see:</p> <p>https://cloudintegration.hana.ondemand.com/PI/help</p> <p>Scroll down to the section <i>Designing and Operating Cloud Integration Content – PDF Documentation</i>.</p> <p>Open the document <i>Connecting a Customer System to SAP Cloud Integration</i>.</p> <p>Go to → <i>Concepts of Secure Communication</i> → <i>Basics</i> → <i>HTTPS-Based Communication</i> → <i>Load Balancer Root Certificates Supported by SAP</i>.</p>	<p>Integration</p>	<p>List of all the supported certification authorities.</p>	<p>How to establish secure HANA connections</p>
---	--------------------	---	---

2 Integration Overview

2.1 Overview Illustration

Figure 1 shows an overview of the SAP SuccessFactors to SAP Access Control integration process.

Figure 1: Integration Overview



- 1) Employee data resides in SAP SuccessFactors Employee Central.
- 2) The integration scenario covers three events in the SuccessFactors HR system:
 1. Add new employee
 2. Change employee job data (update employee records such as business unit or position)
 3. Terminate employee
- 3) SAP Cloud Integration retrieves changed employee data from Employee Central and converts it to a format that can be used by SAP Access Control.
- 4) SAP Access Control imports the data from SAP Cloud Integration. Using decision tables that are configured in the Business Rule Framework (BRF+) and in Rule-to-Role mapping, SAP Access Control creates access requests that contain the appropriate roles and actions for the employee.

-
- 5) SAP Access Control provisions the employee in the correct target systems with the appropriate role assignments (role assignments are removed in the case of employee termination).

2.2 SuccessFactors Integration Scenarios

The SuccessFactors to SAP Access Control integration supports three scenarios:

1. Add New Employee
2. Change Employee Job Data
3. Terminate Employee

2.2.1 Add New Employee

Figure 2 shows the SuccessFactors screen that you use to add a new employee. The data that you enter here is transferred to SAP Cloud Integration.

Figure 2: Add New Employee in SuccessFactors

The screenshot shows the 'Add New Employee' screen in SuccessFactors. The page title is 'My Employee File' and the user is 'Admin User (admin)'. The breadcrumb trail is 'Home > Admin Tools > Add New Employee'. A red arrow points to the 'Add New Employee' link in the breadcrumb. Below the breadcrumb, there are fields for 'File Date' (08/03/2015), 'Company' (Acme German (ACC_USU)), and 'Event Reason' (No Selection). The main form is divided into two sections: 'Name Information' with fields for 'First Name' and 'Last Name', and 'Biographical Information' with fields for 'Date of Birth' and 'Country of Birth'.

2.1.2 Change Employee Job Data

Figure 3 shows an example of how you change employee job information in SuccessFactors. The data that you enter here is transferred to SAP Cloud Integration.

Figure 3: Change Employee Data in SuccessFactors

successfactors[™]
An SAP Company

My Employee File ▾


Admin User (admin) ▾


Employee Files Help & Tutorials

Back to: Employment Information


Update Employee Records

What changes are you proposing for SFEMP1 TEST?

- Change Job and Compensation Info 
 - Job Information
 - Job Relationships
 - Compensation Information
- Spot Bonus
- Employment Details
- Leave Of Absence
- Add Employment Details
- Add Global Assignment Details
- Terminate/Retire

When do you want your changes to take effect? 07/30/2015 

Job Information

Organizational Information 

Company

2.1.4 Terminate Employee

Figure 4 shows an example of how you terminate an employee in SuccessFactors. The data that you enter here is transferred to SAP Cloud Integration.

Figure 4: Terminate Employee in SuccessFactors

The screenshot shows the SuccessFactors interface for updating employee records. The page title is "My Employee File" and the sub-header is "Update Employee Records". The main heading asks "What changes are you proposing for SFEMP11 SFEMP11?". A list of options includes "Change Job and Compensation Info", "Spot Bonus", "Employment Details", "Leave Of Absence", "Add Employment Details", "Add Global Assignment Details", and "Terminate/Retire", which is selected. A success message in a dark box says "Your changes were successfully saved". Below, the "Terminate/Retire" section is highlighted with a red arrow. It contains a "Termination Date" field with the value "08/19/2015" and a "Termination Reason" dropdown menu set to "Early Retirement (TERERLRT)".

3 Configuring SAP SuccessFactors Employee Central

SAP SuccessFactors Employee Central must be configured as described in the *Employee Central Master Guide*. In addition, the *Compound Employee SOAP API* must be enabled as described in the *Implementing the Compound Employee API* available at http://help.sap.com/hr_api/.

Note

For more information about how to set up Employee Central, refer to the *Employee Central Master* at http://help.sap.com/hr_ec?current=hr_ec#section4.

3.1 Web Service Setup

The *Compound Employee API* uses the *SF API* operations login and logout. You must enable the Application Programming Interface, which uses the Employee Central Compound Employee API to replicate the employee master data from Employee Central to SAP Access Control.

Procedure

1. Login to *Provisioning* using your provisioning URL. The access URL differs for different data centers. The URL and users will be provided to you by SAP. See the example below for a sample URL.

Example

https://salesdemo4.successfactors.com/provisioning_login

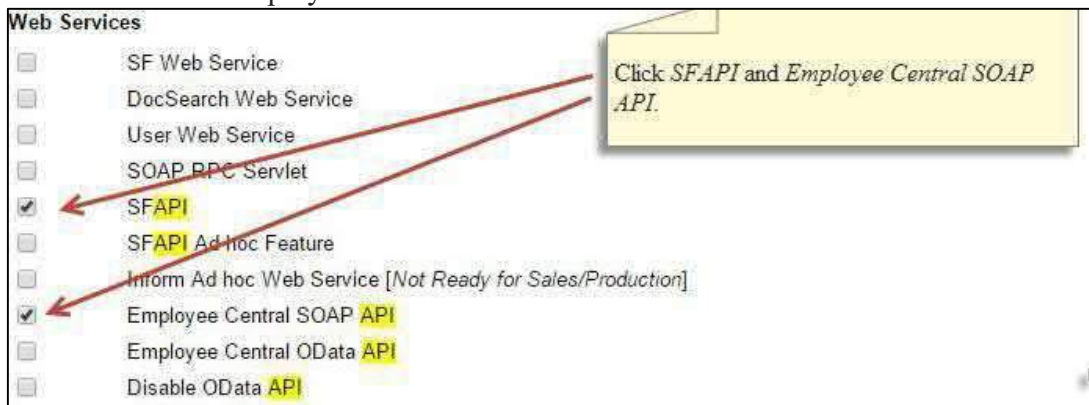


Once signed on, you see all the companies assigned to your name.

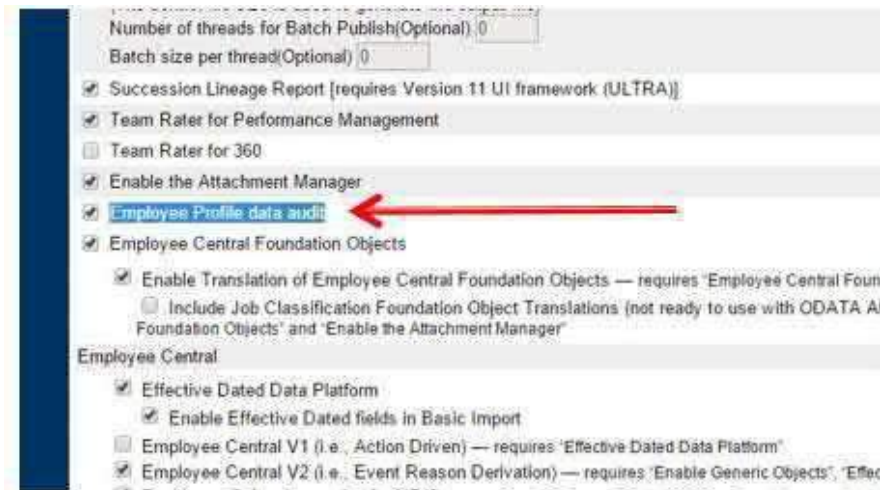
2. Click to choose your company. In the sample screenshot, this is *ACE1321*.



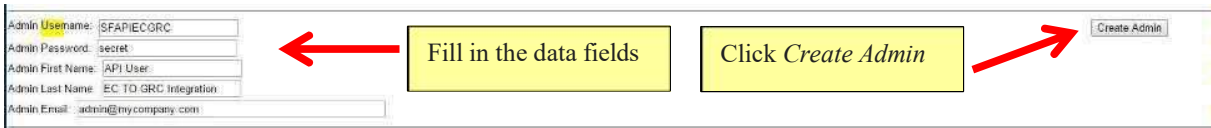
3. Click Company Settings.
4. Scroll down to *Web Services*.
5. Click SFAPI and Employee Central SOAP API to select them.



6. Create the API Login User.
On the same page as the *Web Service Settings* above, scroll down or search this page for *Employee Profile data audit* and select the checkbox.



7. Create the API Login User *SFAPI* by filling in the fields as indicated below.



The screenshot shows a form with the following fields: Admin Username (SFAPICORC), Admin Password (secret), Admin First Name (API User), Admin Last Name (EC TO GRC Integration), and Admin Email (admin@mycompany.com). A red arrow points to the form fields with the text 'Fill in the data fields'. Another red arrow points to the 'Create Admin' button with the text 'Click Create Admin'.

1. Click the *Create Admin* button.
2. Click *Save*.
3. Define role-based permissions for the API user as described in section 3.2.1.


i Note

This configuration is typically done by SAP consultants, not by customers.

i Note

You must activate the data audit log to record all employee data changes; otherwise, you will receive an error message.

4. On the Company Settings page, search for **Enable performance improved XML rendering**.
5. Select the checkbox enable performance improved XML rendering.



The screenshot shows the 'SFAPI Feature Settings' page. Under 'SFAPI Compound Employee', the checkbox 'Enable performance improved XML rendering' is checked and highlighted with a red box. Other options include 'Enable data access via JDBC'. A 'Save' button is visible at the bottom right.

➔ Recommendation

For more features and improved performance, we strongly recommended that you make this setting.

3.2.1 Set Permissions for API User

Procedure

1. Go to *Admin Center*. In the *Tools* search field, enter *Manage Permission Role* and add the following permissions to a role granted to your API user:
 - a. General User Permission: API User Login
 - b. Employee Central API: Employee Central HRIS SOAP API

a)

Permission Role Detail

1. Name and description

Role Name: APIAccessRole

Description: Compound Employee API role

2. Permission settings

Specify what permissions users in this role should have.

Permission...

▼ Permission not requiring target

- General User Permission
 - SFAPI User Login
- Employee Central API
 - Employee Central HRIS SOAP API

b)



Caution

These permissions give the user access to use the API. They do not grant any user interface logon.

2. Assign the API user to a group and adjust the corresponding permission settings.
3. You can test that the API works by using tools such as the SOAP UI tool.

4 Configuring SAP Access Control

4.1 Prerequisites

The following are prerequisites to configuring SAP Access Control for integration with SAP SuccessFactors Employee Central.

- Configure SuccessFactors Employee Central:
 - a) Employee Central must be configured as described in the *Employee Central Master* guide.
 - b) The *Compound Employee SOAP API* must be enabled as described in *Implementing the Compound Employee API* available at http://help.sap.com/hr_api/.
- SAP Cloud Integration is set up.
- The following SAP Access Control components are installed:

For this component you need this software component version
SAP NetWeaver	SAP_BASIS 740 SP05 or higher
SAP Access Control	GRC 10.1 SP 10 or higher

i Note

See the section *Related Guides* for more information.

- The required SAP Notes are installed

The following note must be added on top of SAP Access Control 10.1 SP 10:

SAP Note Number	Title	Description	Contained in Support Package
2180164	Integrate SuccessFactors Employee Central with SAP Access Control	This note supports the integration of SAP SuccessFactors Employee Central with SAP Access Control for the following three scenarios:	SAP Access Control 10.1 SP 10

		<ul style="list-style-type: none">• A new employee is added• Employee job data is changed• Employee is terminated	
--	--	---	--

i Note

Make sure that you have the current version of each SAP Note, which you can find on SAP Service Marketplace at <https://support.sap.com/notes>.

To search for SAP Notes that are relevant for the integration of SAP SuccessFactors Employee Central to SAP Access Control, in the application area enter GRC-SAC-ARQ and GRC_SAC_ARQ-SF.

4.2 Activating the Web Services

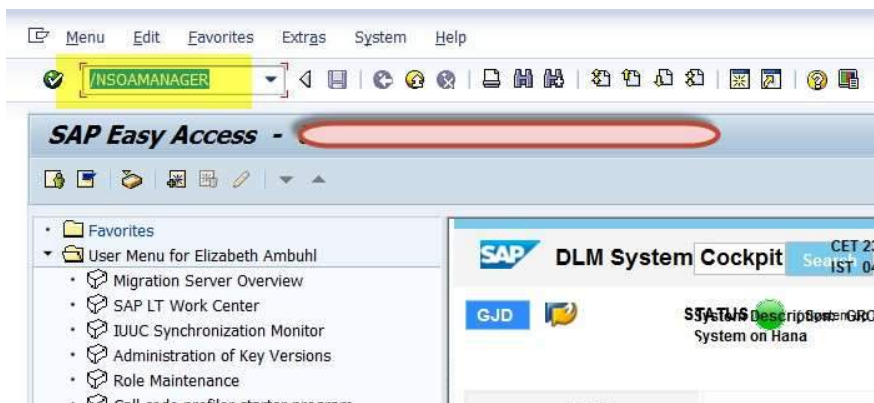
The following Web services must be activated in SAP Access Control:

HR Trigger Scenarios	Object Type	Service Interface Name (Web Service Definition Name)	Software Component
Add New Employee	Employee change details	GRAC_SFEC_HR_TRIGGER	GRCFND_A
Change Employee Job Data			
Terminate Employee			

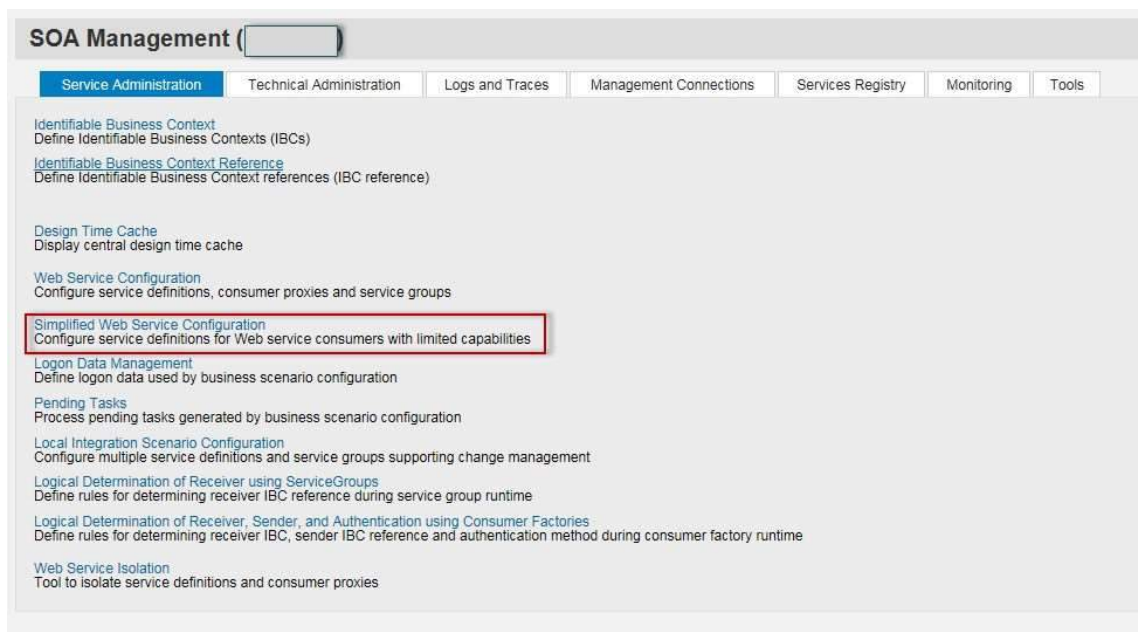
Follow the steps below to activate the necessary web services.

Procedure

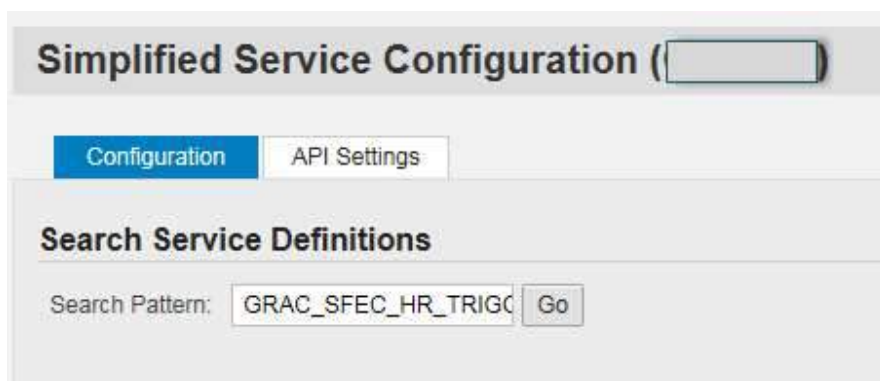
1. Enter transaction *SOAMANAGER*.



2. Click *Simplified Web Service Configuration*.



3. Enter the Web service definition name, for example, **GRAC_SFEC_HR_TRIGGER**.



4. Click *Go*.

5. Select the *User Name / Password (Basic)* checkbox

The screenshot shows the 'Simplified Service Configuration' interface. At the top, there are tabs for 'Configuration' and 'API Settings'. Below that is a search bar with the text 'Search Service Definitions' and a search pattern 'GRAC_SFEC_HR_TRIGGER'. The main section is 'Configure Service Definitions', which includes a 'Save' button (highlighted with a red box), 'Show Details', 'Show Changes', and an 'Information' dropdown menu set to 'Standard'. Below this is a table with columns for 'Internal Name', 'User Name/Password (Basic)', 'X.509 Client Certificate', and 'SAP Logon Ticket'. The row for 'GRAC_SFEC_HR_TRIGGER' has a checked checkbox under 'User Name/Password (Basic)' (also highlighted with a red box) and unchecked checkboxes under 'X.509 Client Certificate' and 'SAP Logon Ticket'.

Internal Name	User Name/Password (Basic)	X.509 Client Certificate	SAP Logon Ticket
GRAC_SFEC_HR_TRIGGER	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

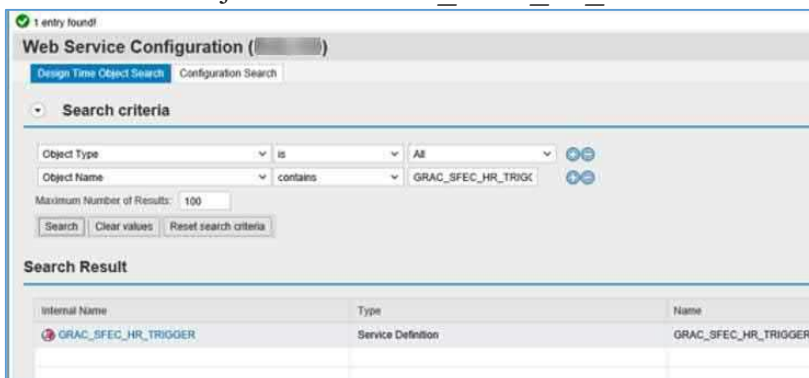
6. Click *Save*. The Web Service is activated.

4.3 Create Binding for WS

1. Execute transaction *SOAMANAGER* and click **Web Service Configuration**.



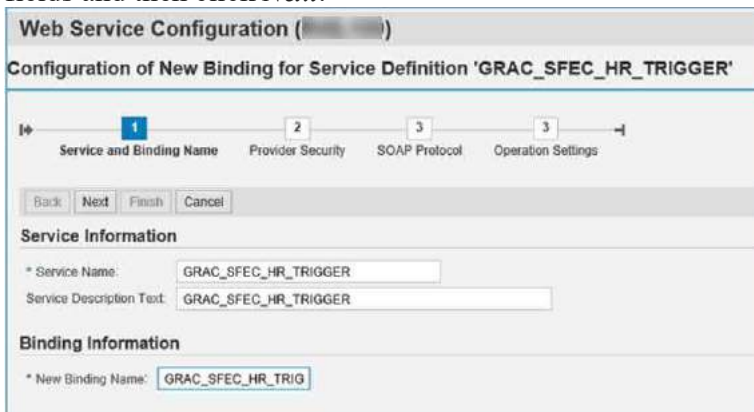
2. Search for the Object Name: *GRAC_SFEC_HR_TRIGGER*.



3. Click the web service to display the configuration screen and click *Create Service*.

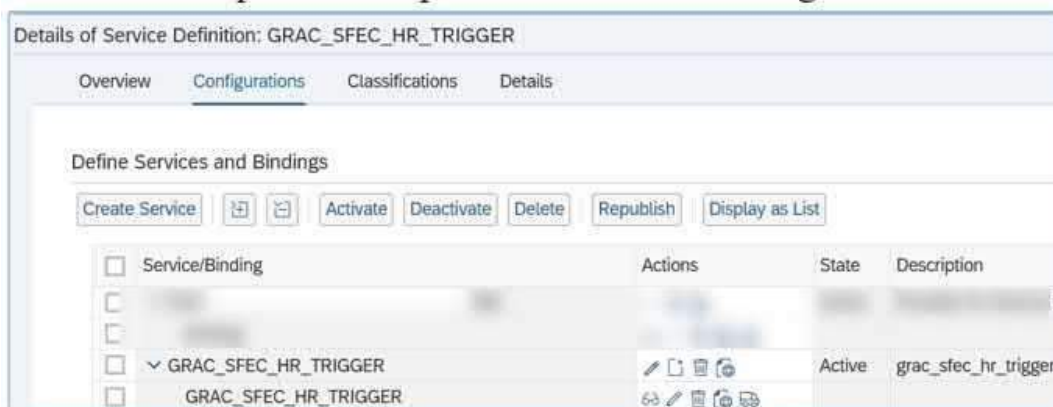


- On the **Service and Binding** screen, fill in the *Service Name* and *New Binding Name* fields and then click *Next*.



- On the Provider Security screen, select **Transport Channel Authentication = User ID/Password**, and then click *Next*. You can leave all other attributes as default.
- On the SOAP Protocol screen, leave the defaults, and click *Next*.
- On the Operation Settings screen, leave the default values, and click *Finish*.

This is an example of a completed web service binding.



Service/Binding	Actions	State	Description
GRAC_SFEC_HR_TRIGGER	[Icons]	Active	grac_sfec_hr_trigger

4.4 Creating Request Types

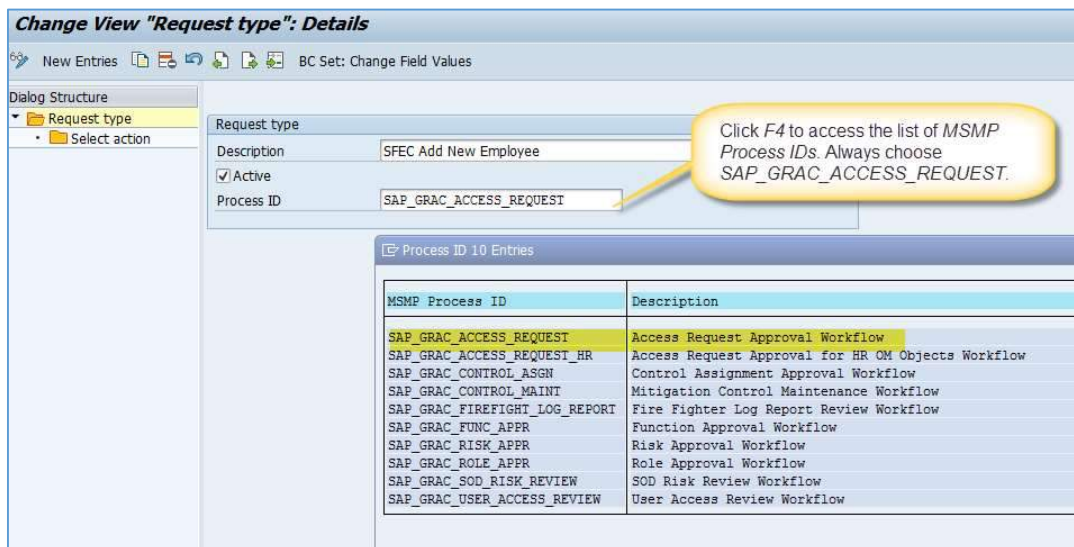
In the SAP Implementation Guide (IMG), you must define an SAP Access Control request type for each of the three SuccessFactors integration scenarios: Add New Employee, Change Employee Job Information, and Terminate Employee.

Procedure

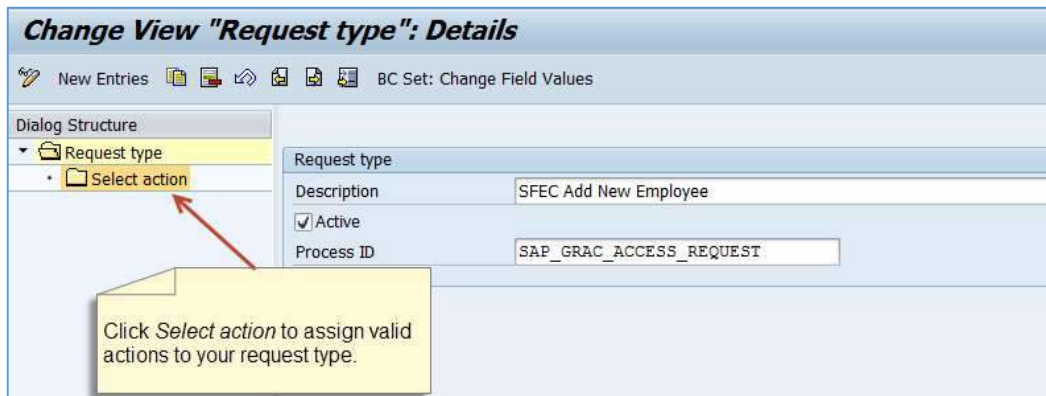
1. In the SAP Reference IMG, choose Governance Risk, and Compliance → Access Control → User provisioning → Define Request Type,
2. Click New Entries.



3. Add a Description.
4. In the *Process ID* field, click *F4* on and choose *SAP_GRAC_ACCESS_REQUEST*.



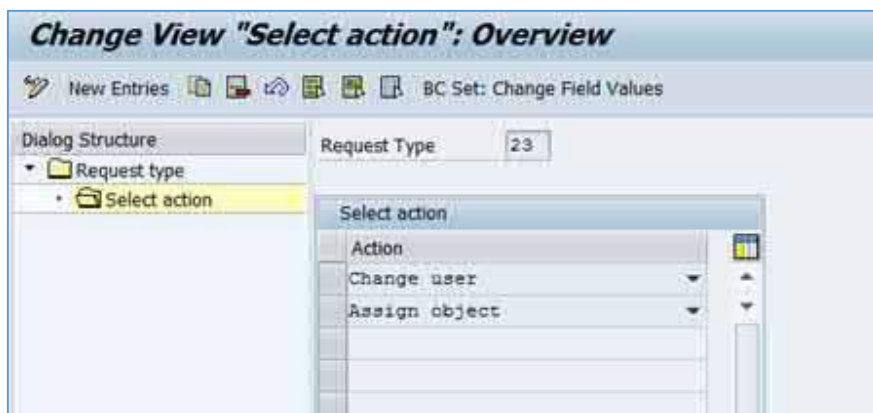
5. Assign the appropriate actions to each request type as illustrated in the screenshots below.



i Note

For information about the possible *Actions*, see the IMG node documentation.

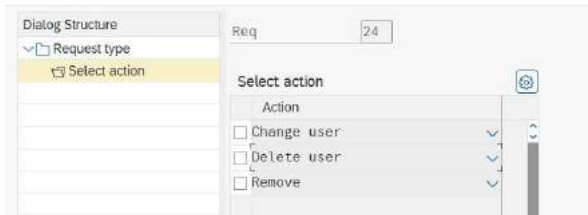
- a) Add New Employee: assign the following actions:
- Change User
 - Assign Object



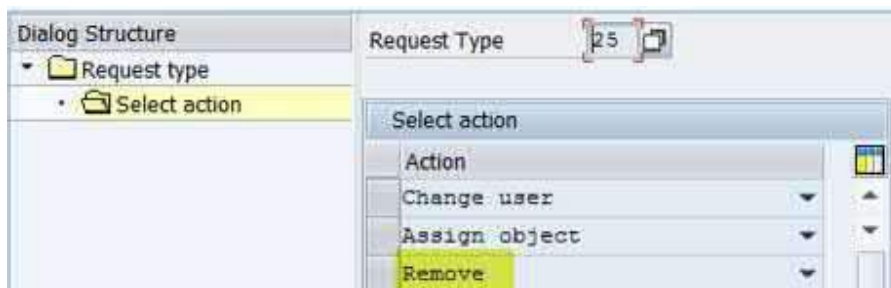
-
- b) Terminate Employee: assign the following actions:
- i. Change user / Change & lock user
 - ii. Delete user
 - iii. Remove

 **Caution**

Future termination is not supported. The employee is terminated immediately.



- c) Change Employee Job Data: assign the following actions:
- i. Change user
 - ii. Assign Object
 - iii. Remove



 **Caution**

The Employee Change request type should always include the action *Remove*.

6. *Save* your entries.

4.5 Creating Request Priorities

In the IMG, you must designate a priority for each of the three integration scenarios. The *Request Priority* is used in workflow configuration.

Procedure

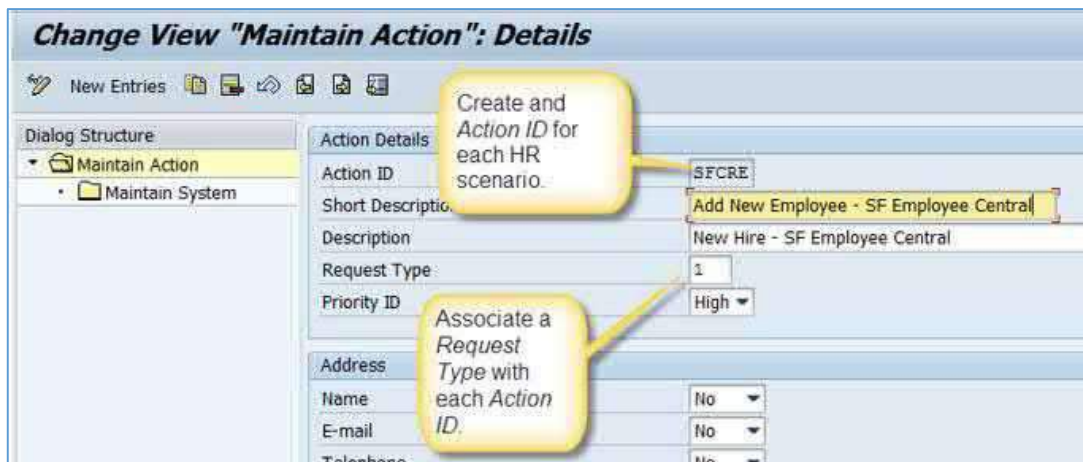
1. In the [SAP Reference IMG](#), choose Governance Risk, and Compliance → Access Control → User provisioning → Maintain Priority Configuration.
2. Click *New Entries* and add any necessary priority types.

4.6 Maintaining Settings for HR Trigger

In the SAP Implementation Guide, you must define a separate action for each of the three SuccessFactors integration scenarios. You do this by maintaining the HR trigger actions.

Procedure

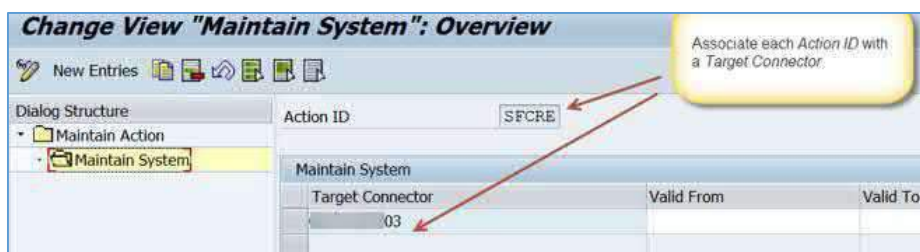
1. In the SAP Reference IMG, choose Governance Risk, and Compliance → Access Control → User provisioning → Maintain Settings for HR Trigger
2. On the screen Change View “Maintain Action”: Overview, add an entry for each of three scenarios: Add New Employee, Change Employee Job Data, and Terminate Employee:
 - a) Choose New Entries.
 - b) Fill in the Action ID, Description, Request Type, and Priority ID for each scenario.



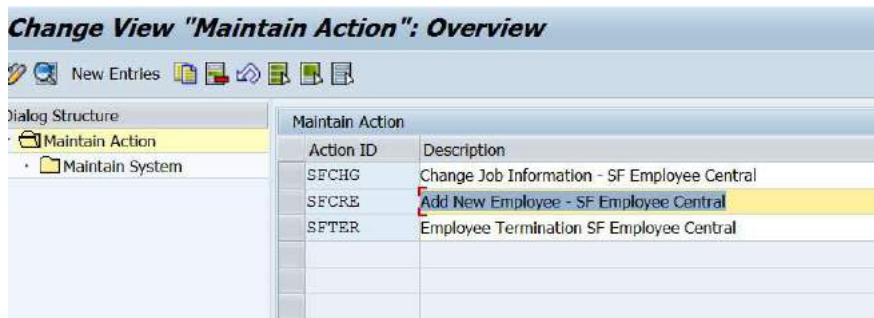
Note

The *Request Types* and *Priority IDs* are different for each customer depending on configuration.

3. Click *Maintain System* to assign a target connector to each *Action ID*.



4. *Save* your entries. The results will look similar to the example below:



The screenshot shows the SAP Change View 'Maintain Action': Overview. The interface includes a 'Dialog Structure' pane on the left with 'Maintain Action' and 'Maintain System' folders. The main area displays a table with the following data:

Action ID	Description
SFCHG	Change Job Information - SF Employee Central
SFCRE	Add New Employee - SF Employee Central
SFTER	Employee Termination SF Employee Central

You have now defined the actions for each integration scenario.

4.7 Configuring the BRF+ Application SFEC_HR_TRIGGER_APP

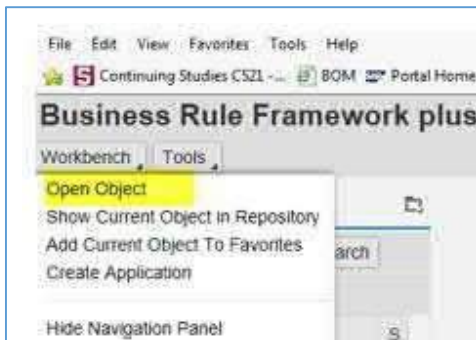
This BRF+ application determines the SAP Access Control actions: create, change, or terminate. You start by evaluating the delivered BRF+ function.

Evaluate the Delivered Function

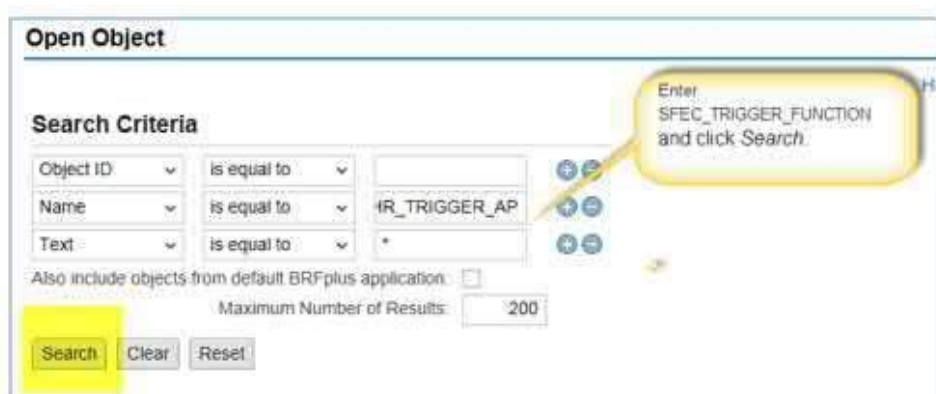
You must first decide whether you can use the BRF+ application SFEC_HR_TRIGGER_APP as delivered or if you need to copy and change it. Follow the steps below to view the delivered function.

Procedure

1. In the SAP system, enter transaction *BRF+* to access the Business Rule Framework.
2. Choose Open Object.



3. Search for the object SFEC_TRIGGER_FUNCTION.



4. BRF+ retrieves the function.

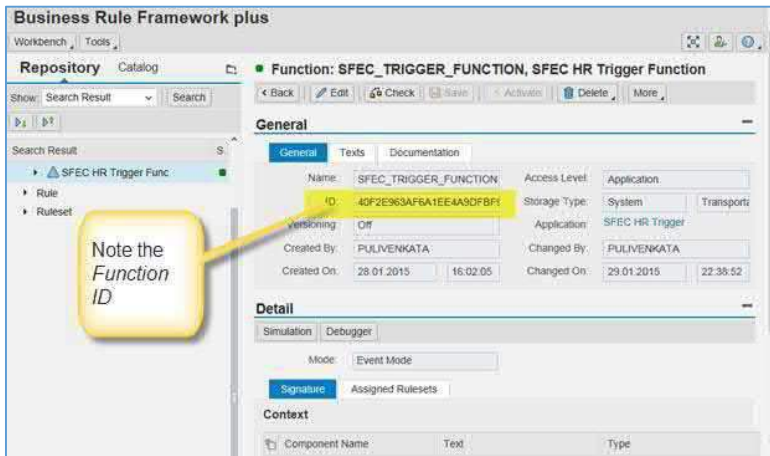
The screenshot shows the 'Open Object' search interface. It includes search criteria for Object ID, Name, and Text, all set to 'is equal to'. The Name field contains 'sfec_*' and the Text field contains '*'. There are buttons for '+', '-', 'Search', 'Clear', and 'Reset'. A callout box says 'Double click the object to select it.' Below the search criteria, it says 'Result list: 4 objects found'. A table lists the objects:

Object	Status	Type	Application
▲ SFEC HR Trigger Func	●	Function	SFEC HR Trigger
📄 Process Rule1	●	Rule	SFEC HR Trigger
📄 Process Rule2	●	Rule	SFEC HR Trigger
📄 HR Trigger Ruleset	●	Ruleset	SFEC HR Trigger

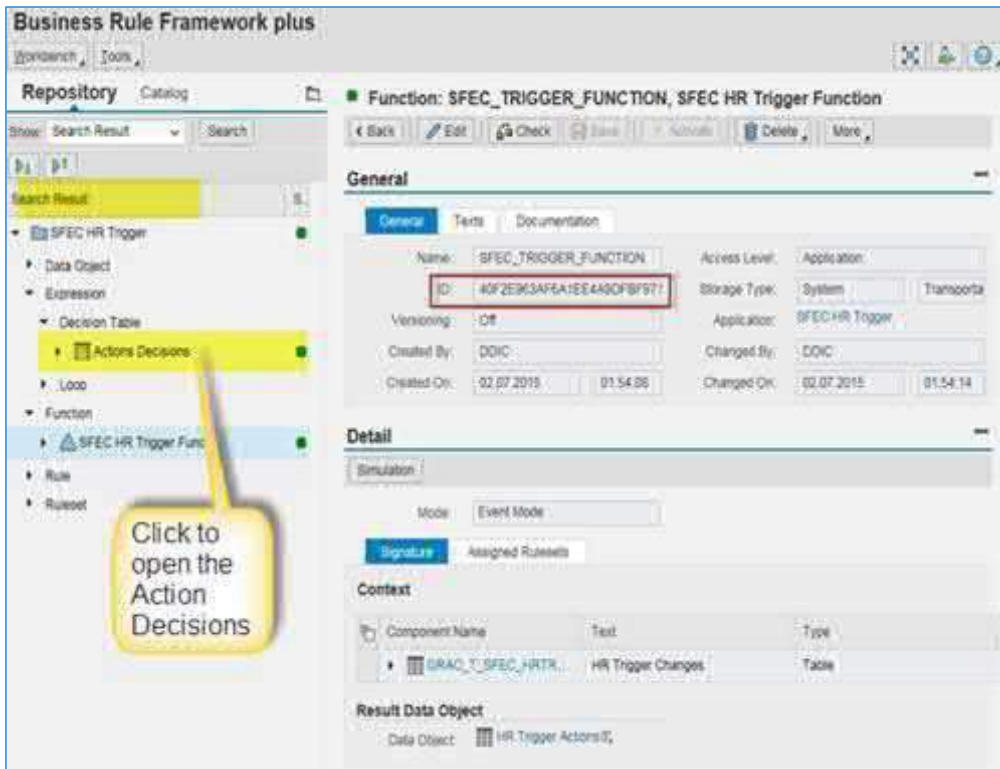
5. Click the Collapse Tray.

The screenshot shows the 'Business Rule Framework plus' object editor for the object 'Function: SFEC_TRIGGER_FUNCTION, SFEC HR Trigger Function'. The interface includes a 'Repository' pane on the left, a 'General' tab, and a 'Detail' section. A callout box points to a collapse icon in the top right corner of the main editor area, with the text 'Click the Collapse Tray to display the General fields.'

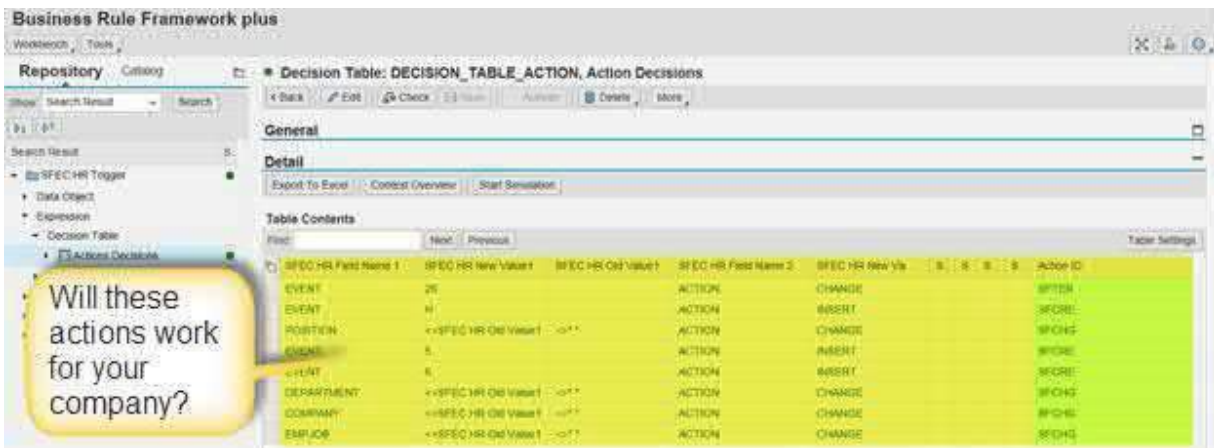
6. Make a note of the *Function ID* for later use.



7. In the *Search Result* box, scroll up. Expand the *Expression* node and then expand the *Decision Table* node.



8. Click Actions Decisions to view the Actions Decisions table.



9. Decide if the delivered action decisions work for you. If not, you must create your own.

i Note

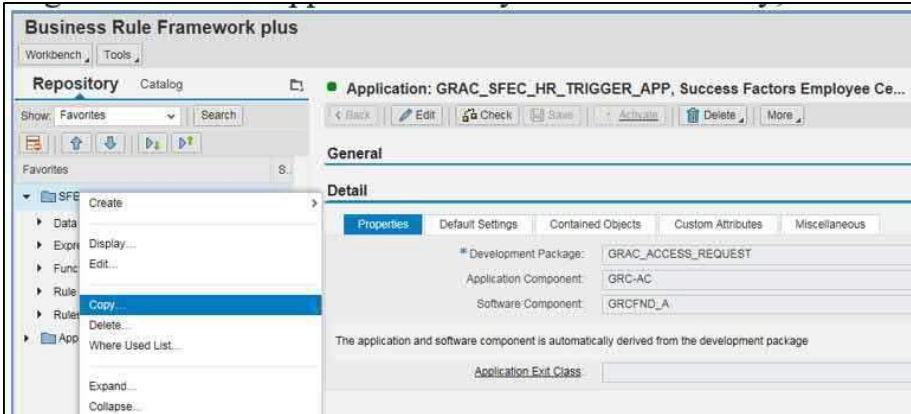
You can use the delivered configuration or copy the BRF+ configuration and modify it for your needs.

a)

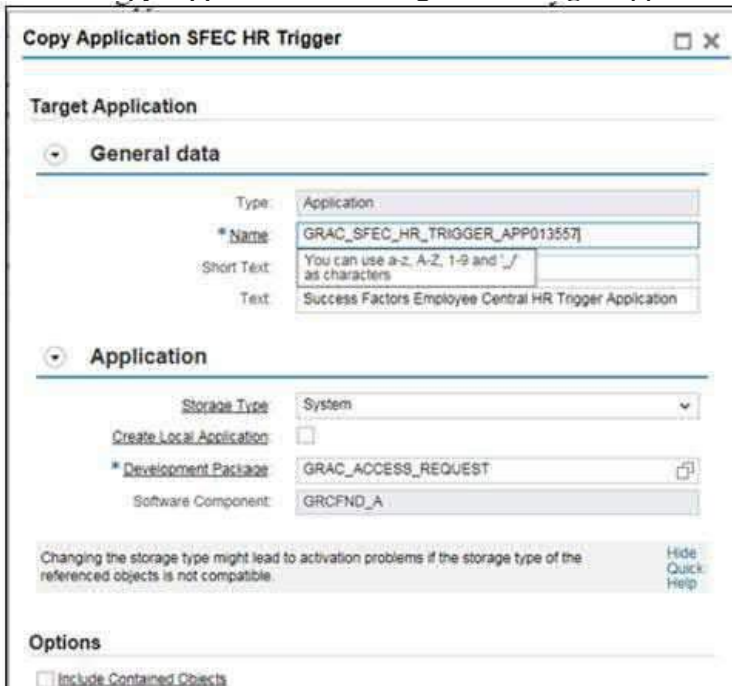
Modify the Delivered Decision Table

If the delivered actions do not work for you, you must copy the delivered application:
SFEC_HR_TRIGGER_APP and modify the actions to suit your needs.

1. Right-click on the application that you want to modify, and select *Copy*.



2. On the Copy Application screen, give the *Target Application* a name and description.



-
3. Change the *Decision Tree* entries to suit your needs.

 Note

For more information, see the section *Configuring the BRF+ Decision Table*.

 Caution

Once you copy the BRF+ application, you can change the decision table entries. You cannot change the delivered BRF+ application.

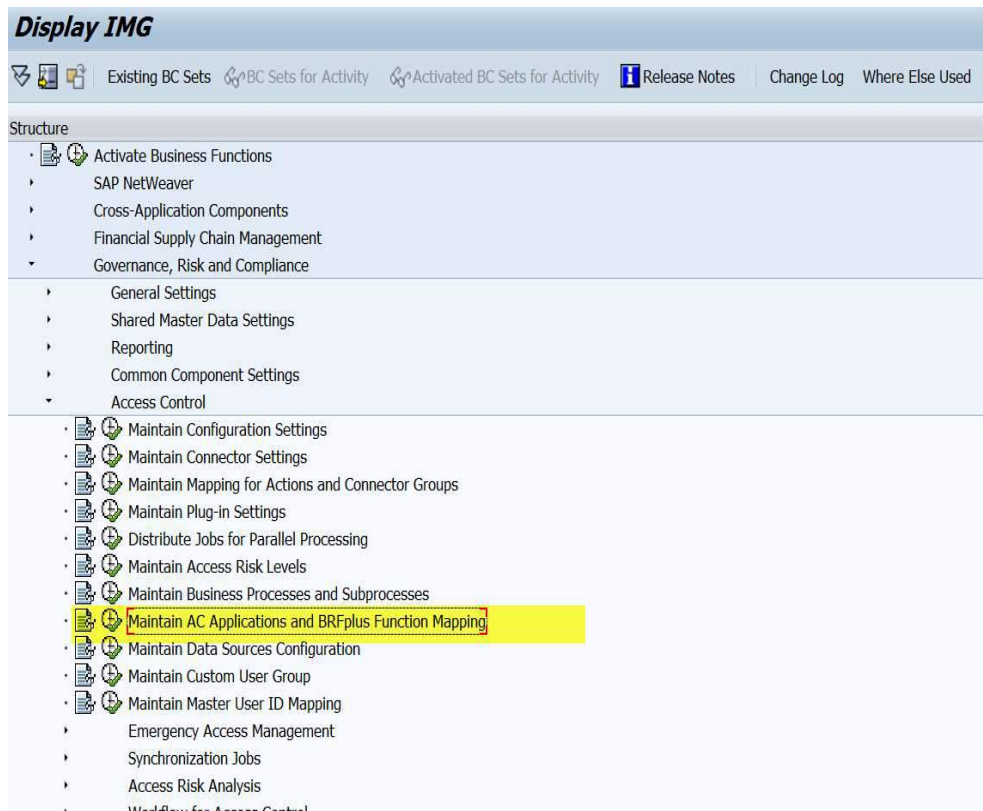
4. Click *Copy*.

4.8 Mapping the BRF+ Function ID to SAP Access Control

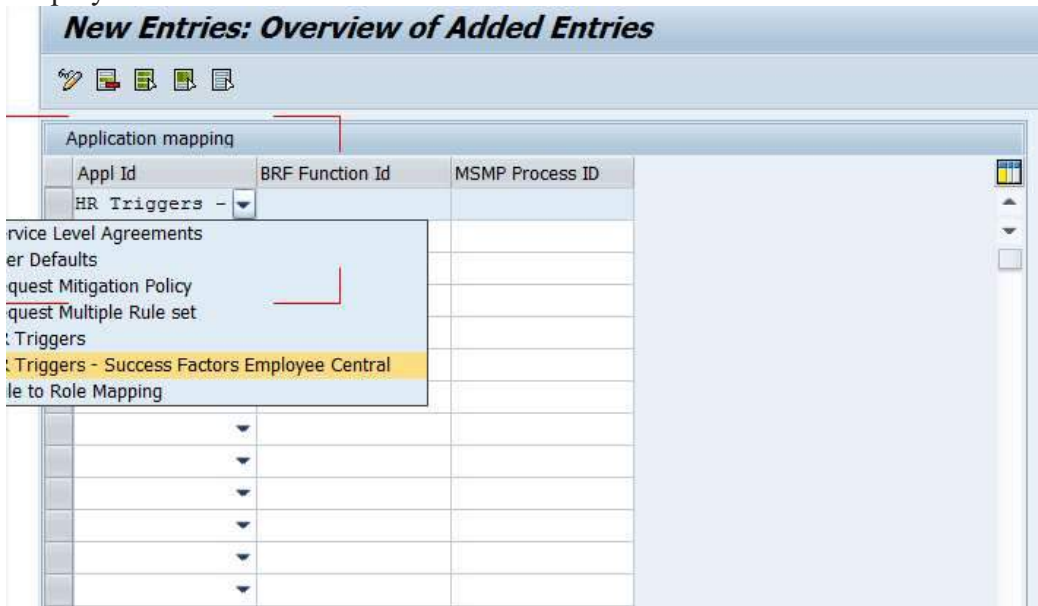
Once you have defined your BRF+ application, you must map its BRF+ function ID to an SAP Access Control's *Application ID*. The SAP Access Control Application IDs are delivered.

Procedure

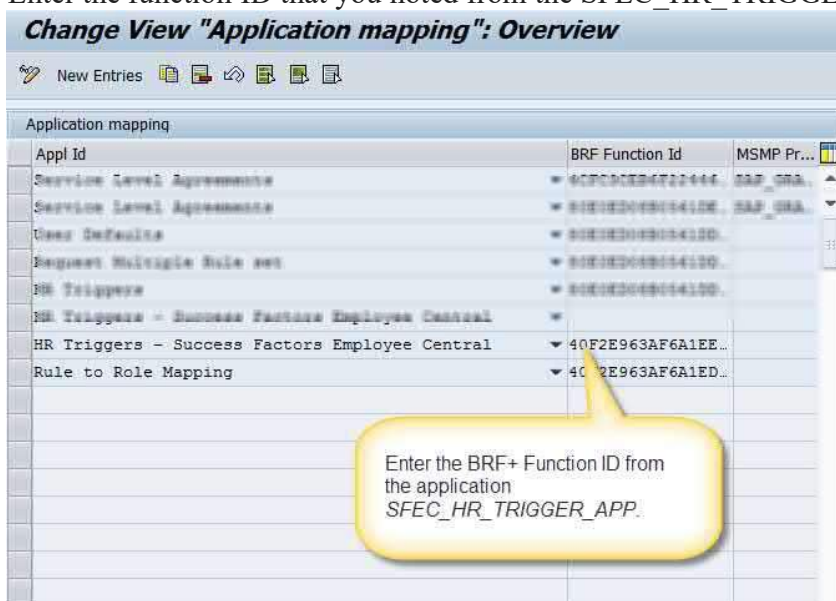
1. In the SAP Reference IMG, choose Governance Risk, and Compliance → Access Control → Maintain AC Applications and BRF+ Function Mapping



- Choose New Entries.
- Click the drop down menu for Appl ID and select HR Triggers – SuccessFactors Employee Central.



- Enter the function ID that you noted from the SFEC_HR_TRIGGER_APP.



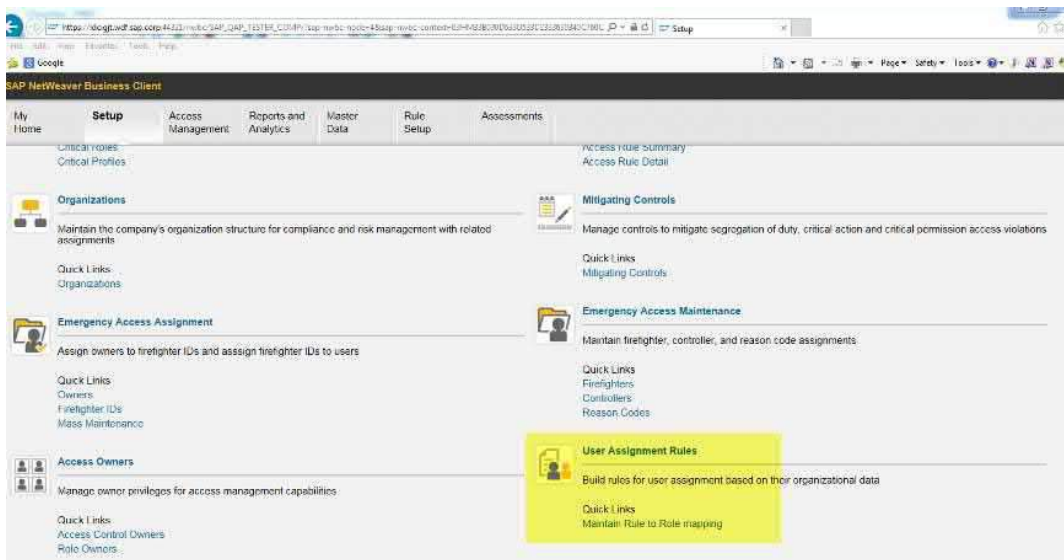
- Click Save.

4.9 Maintaining Rule-to-Role Mapping

In SAP Access Control, you create rules for use in BRF+ and map them to roles. This mapping can be done by an administrator or a role owner.

Procedure

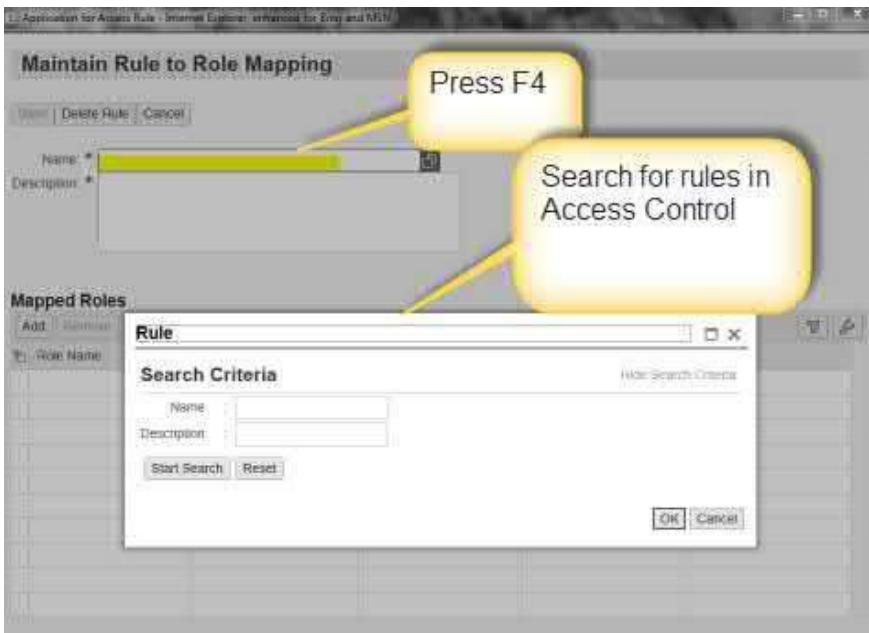
1. From SAP Access Control transaction *NWBC*, navigate to *Setup* → *User Assignment Rules*.
2. Click *Maintain Rule to Role Mapping* as shown in the screenshot below.



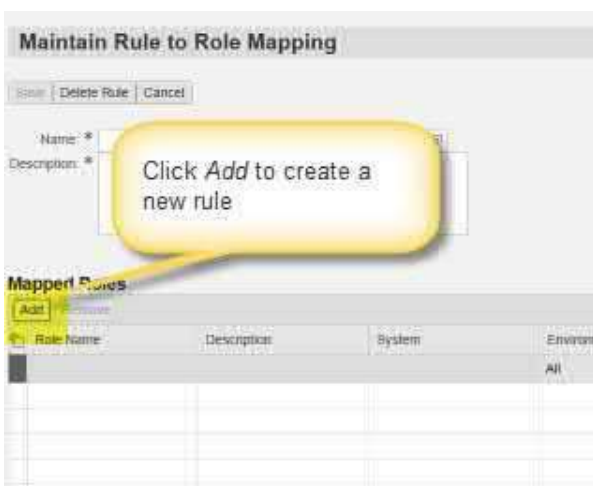
3. With the cursor in the *Name* field, press *F4* to display the Rule Search dialog box.

i Note

Here you can search all the existing rules in SAP Access Control. If no rules are defined, the search will be empty.



4. To add a new rule, click *Add*.



5. On the *Select Roles* screen, search for the roles that you want to include in your rule. Enter your search criteria and click *Search*.
6. Select the desired role(s) and click *OK*.

Select Roles

Search Criteria
 Maximum number of result rows:

Business Process is

System is

Role Type is

Role / Profile Name is

Company is

Enter your search criteria and click Search.

When your desired role displays in the Available section, click to select it.

Available
 View: [Standard View]

Role Name	System	Description	System Description	Role Type	Default Roles
Z*ROLE*1	GI7CLNT600		GI7CLNT600	Single Role	Doesn't Exist
Z.FI_AR_ER	GH7CLNT600		GH7CLNT600	Single Role	Exists (1)
Z.FI_AR_ER	GI7CLNT600		GI7CLNT600	Single Role	Doesn't Exist
Z0CPSSNT-A_BUSINES_DISPLAY_015A	GI7CLNT600	Addon Role: SISNET Business Expert Display Role	GI7CLNT600	Single Role	Doesn't Exist
Z0CPSSNT-A_CHANGE_CORD_CRO_017A	GI7CLNT600	Addon Role: SISNET Change Request Owner Role	GI7CLNT600	Single Role	Doesn't Exist

Use the down arrow to copy the desired role into the Selected section. The role moves from the Available section to the Selected section.

Selected
 View: [Standard View]

Role Name	System	Description	System Description	Role Type
Z.ROLE.001.002	GI7CLNT600	Role Z.ROLE.001.002	GI7CLNT600	Single Role

Click OK

7. The *Maintain Rule to Role Mapping* screen displays. Give the rule a name and a description.

Maintain Rule to Role Mapping

Save Delete Rule Cancel

Name: * SuccessFactors New Hire

Description: * BRF+ rule used in SuccessFactors to Access Control Integration. Add New Employee scenario

Give the rule a name and a description. Then click Save.

Mapped Roles

Add Remove

Role Name	Description	System	Environment	Role Type
Z.ROLE.001.002	Role Z.ROLE.001.002	G17CLNT600	Production	Single Role

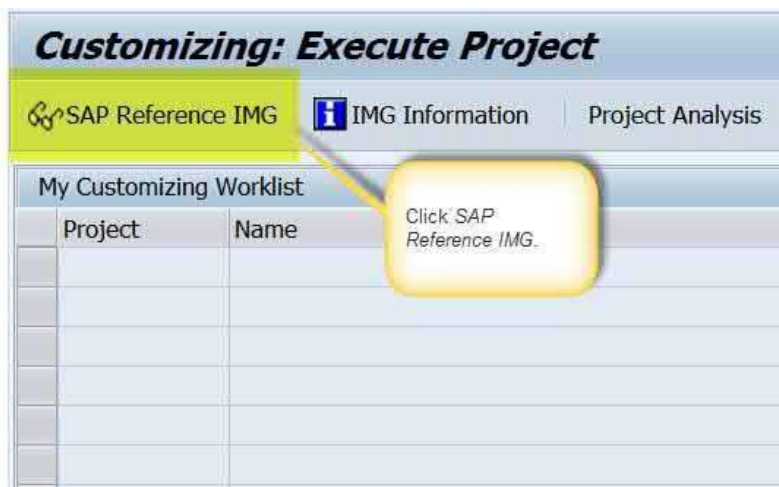
8. Click *Save*.

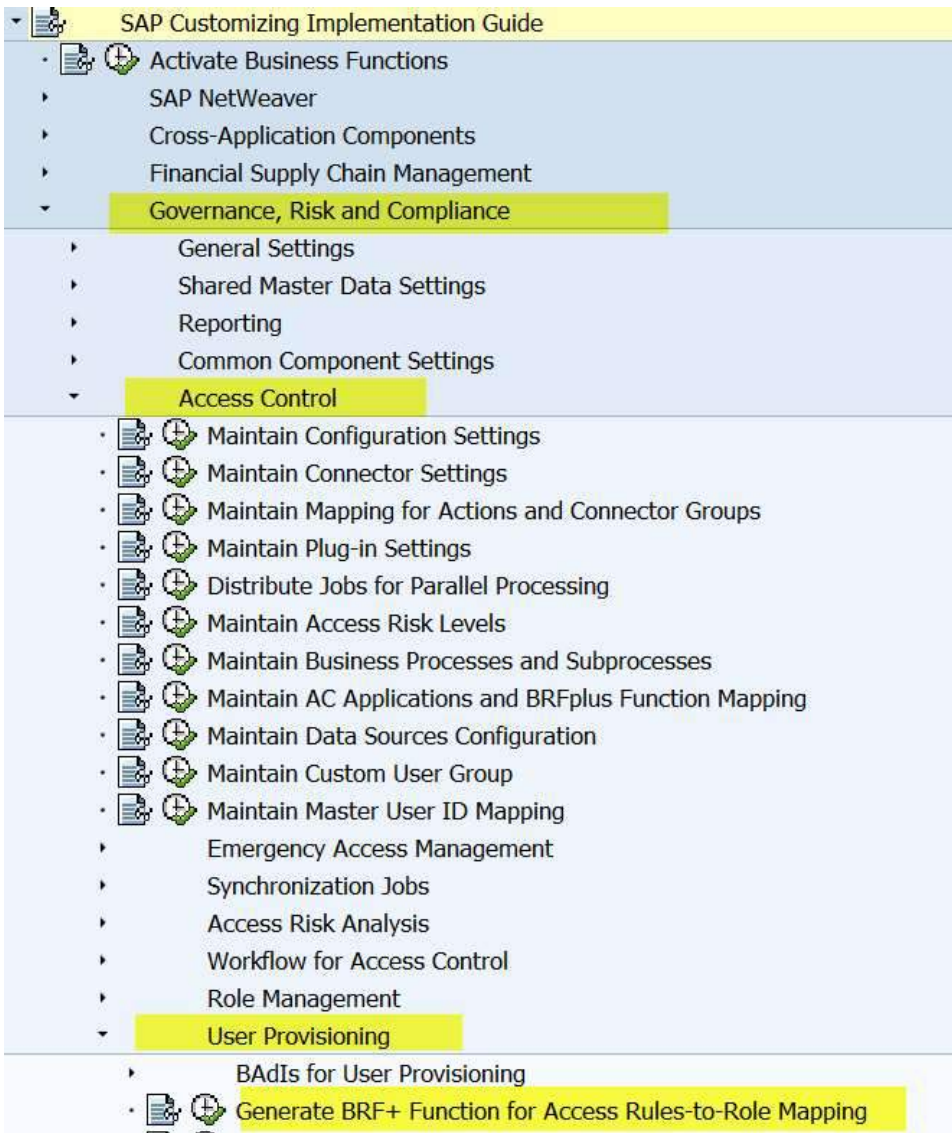
4.10 Generating the BRF+ Function for Access Rule-to-Role Mapping

Once you create the necessary rules for each integration scenario, you must generate a BRF+ application to connect the SuccessFactors events with the correct roles when users are provisioned. This BRF+ application determines which roles to assign to employees based on the employee's attributes.

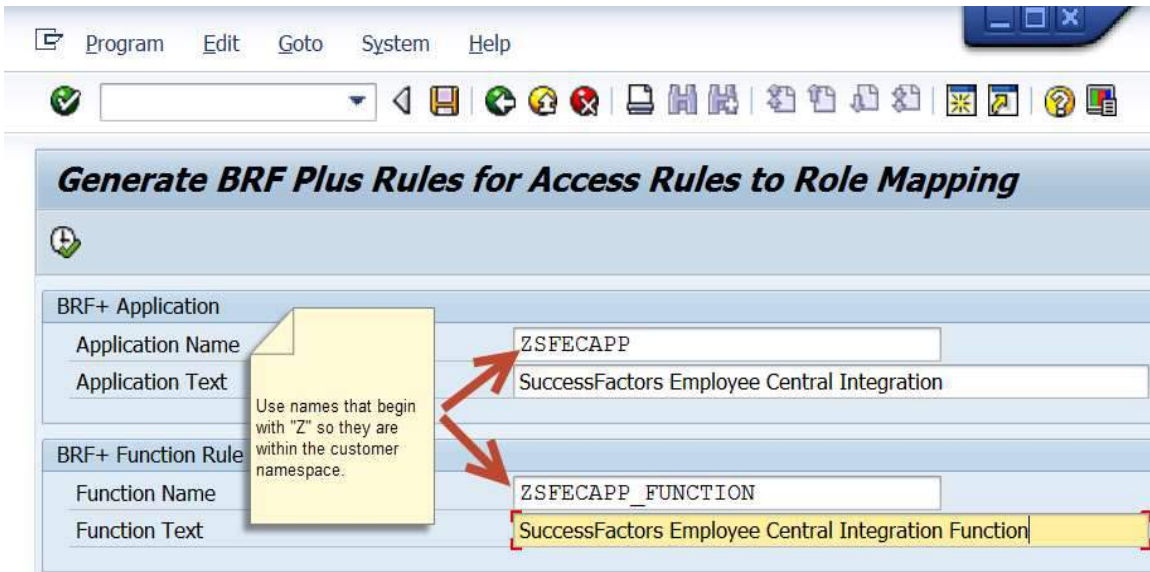
Procedure

1. In the SAP Reference IMG, choose Governance Risk, and Compliance → User provisioning → Generate BRF+ Function for Access Rules-to-Role Mapping.





2. The screen Generate BRF Plus Rules for Access Rules to Role Mapping displays.

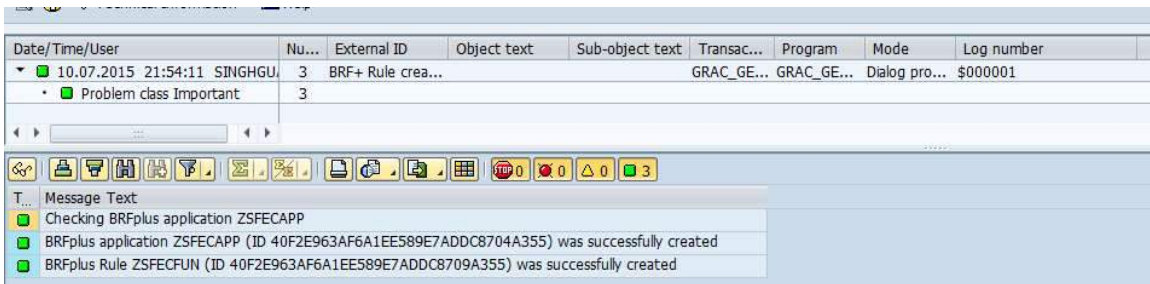


3. Enter an *Application Name* and description and a BRF+ *Function Name* and description.

i Note

- b) Create names that start with “Z” so they fall in the customer name space.
- c)

4. *Save* your entry. The following screen appears.

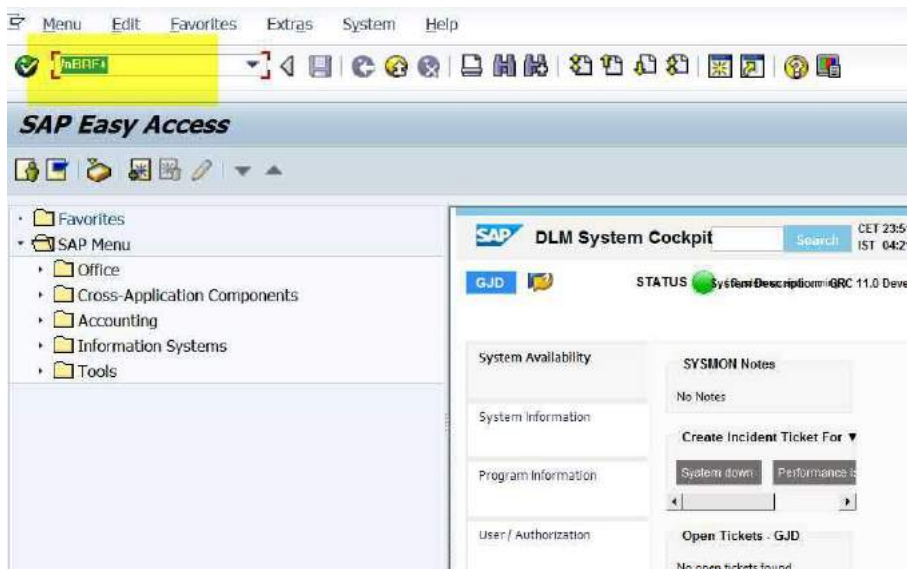


4.11 Configuring the BRF+ Decision Table

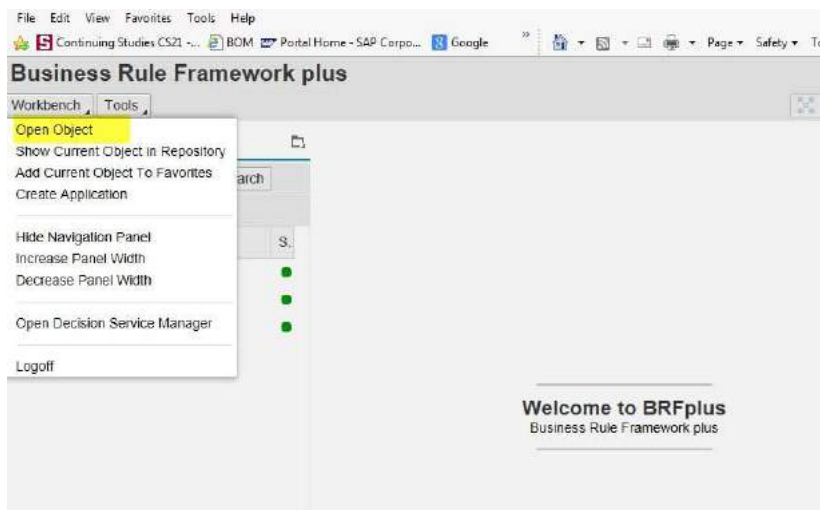
Once you create the BRF+ function in the previous step, you access it and add a decision table.

Procedure

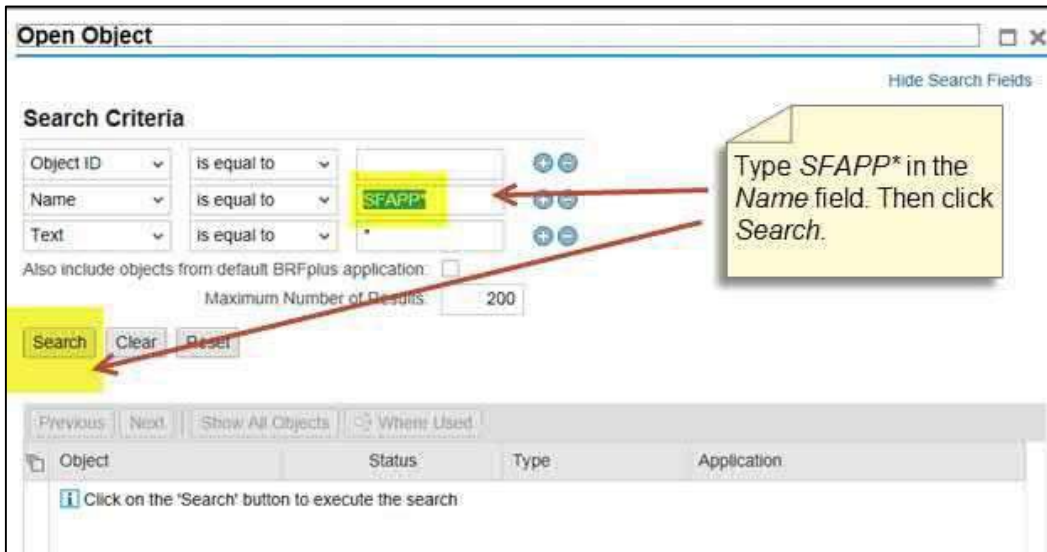
1. Open BRF+ using transaction *BRF+*.



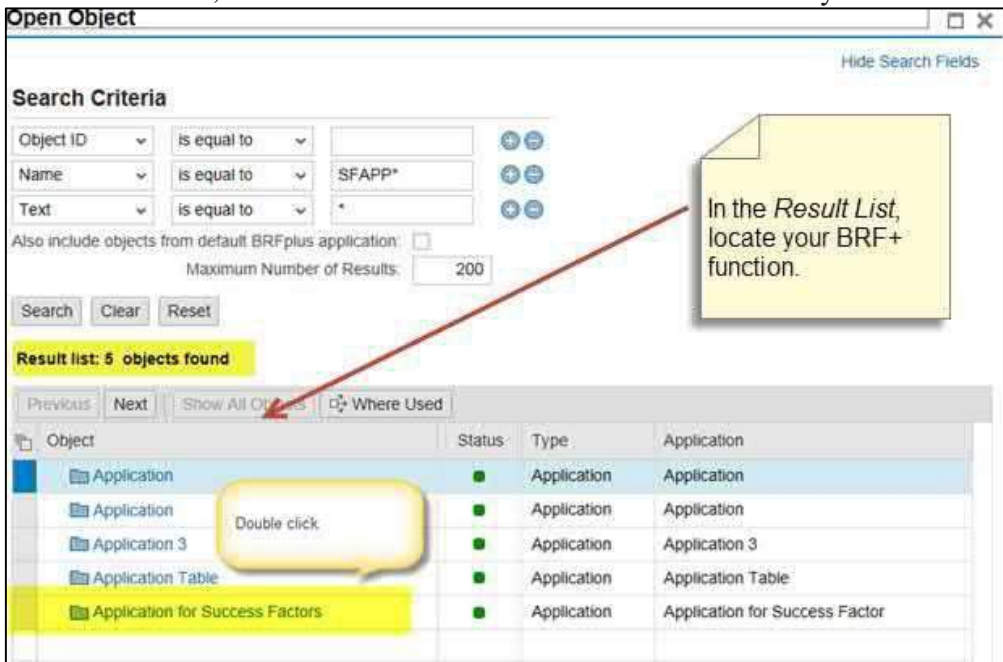
2. Choose Workbench → Open Object.



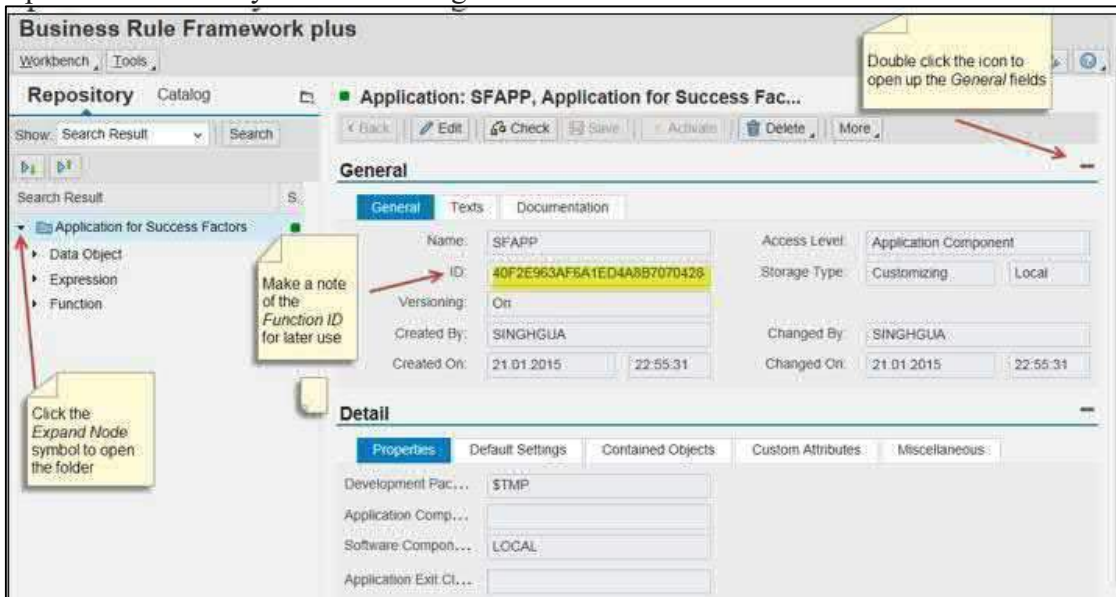
3. Search for *SFAPP**.



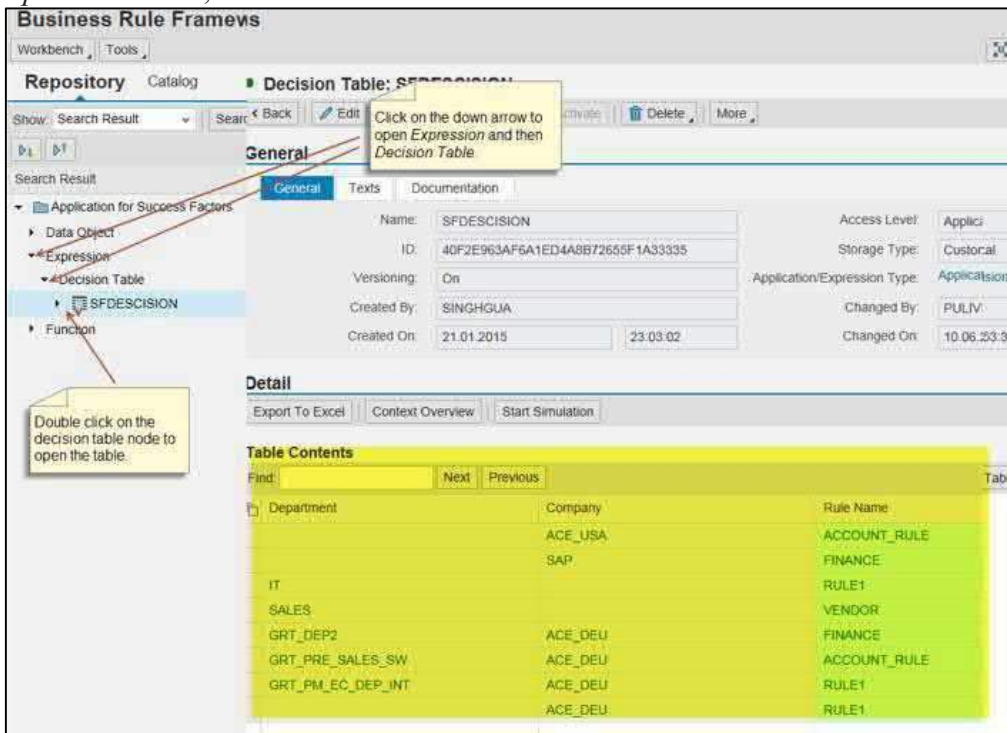
4. In the *Result List*, locate and double click the BRF+ function that you created earlier.



- Open the function by double clicking it. Note the *Function ID*.



- To open the decision table, click *Expand Node* to open the folder, then click the *Expression Node*, and then click *Decision Table*.

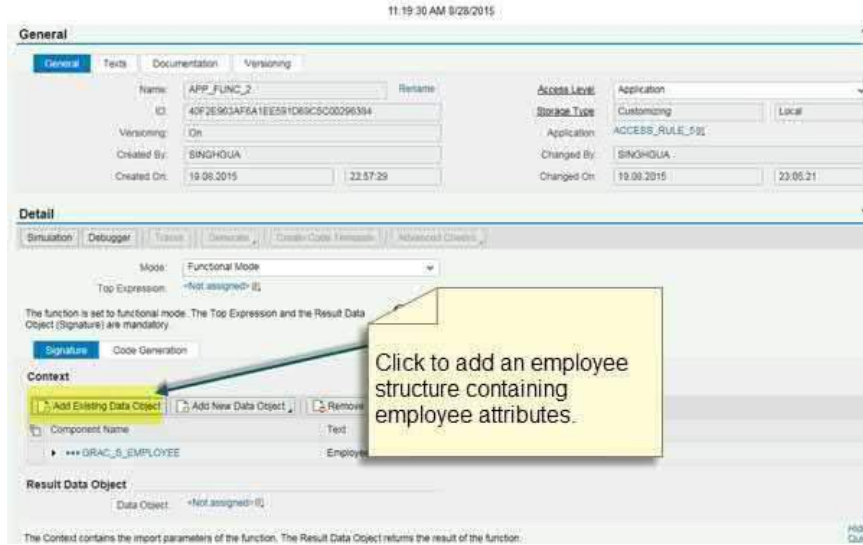


You must configure your decision table for this function. The decision table is based on employee attributes that can be selected by clicking the *Table Settings* button.

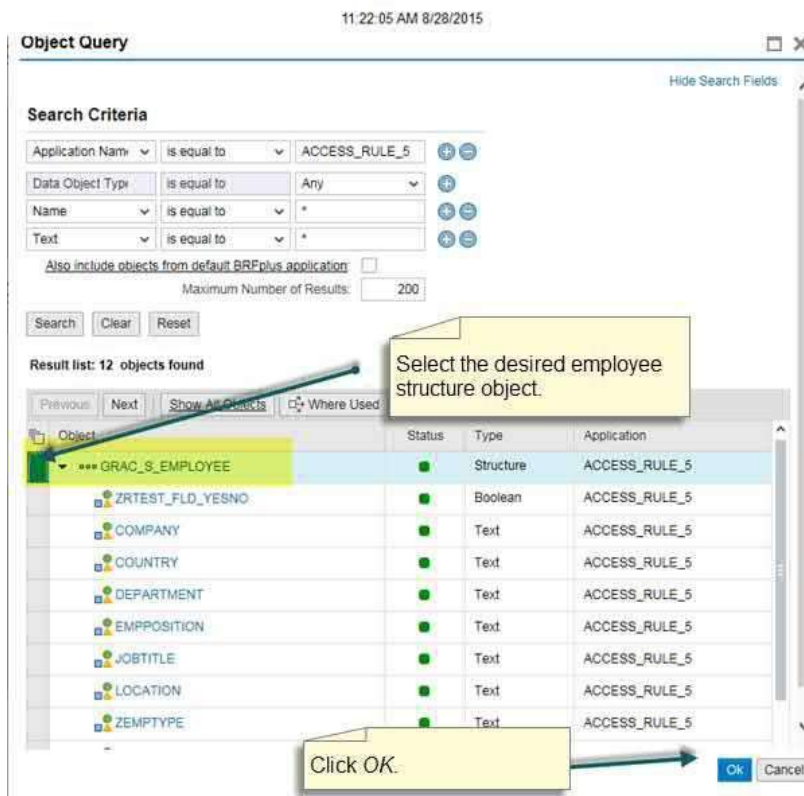
Example

The example below shows how to add a decision table from scratch

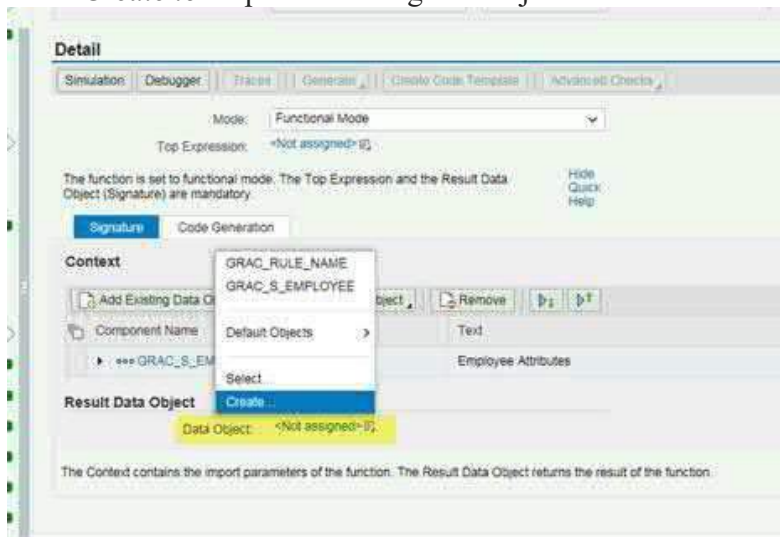
1. Open the *Detail* section of the screen.



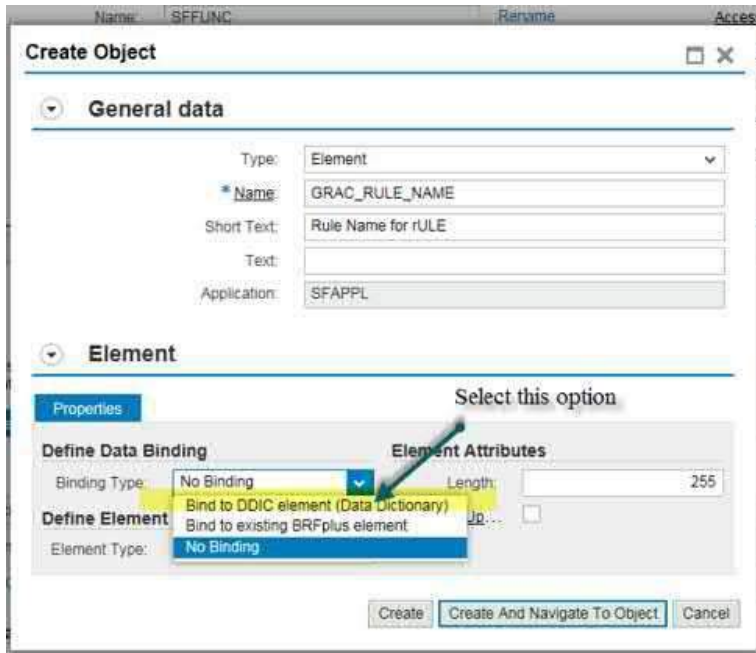
2. Select the desired employee structure.



3. Click *Create* to map the resulting data object.

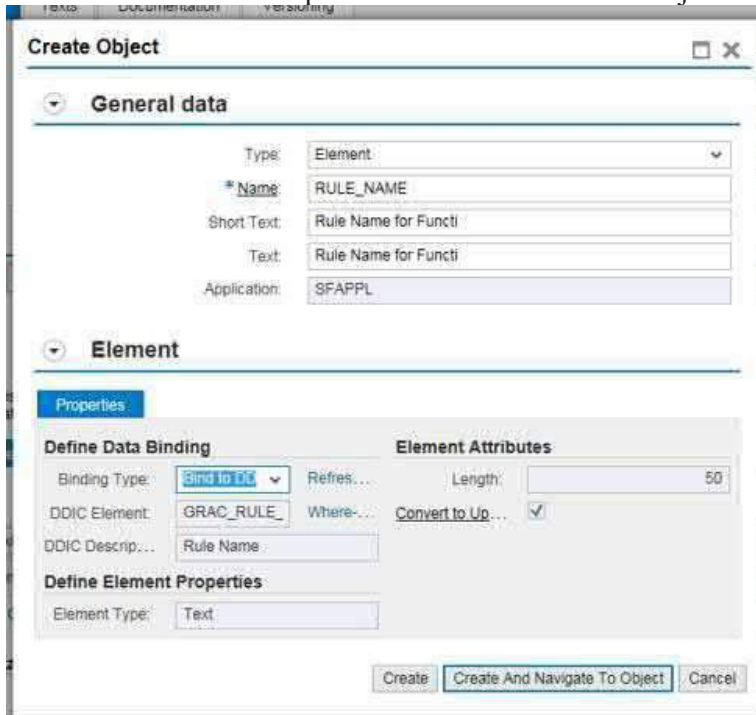


4. Select Bind to DDIC element.

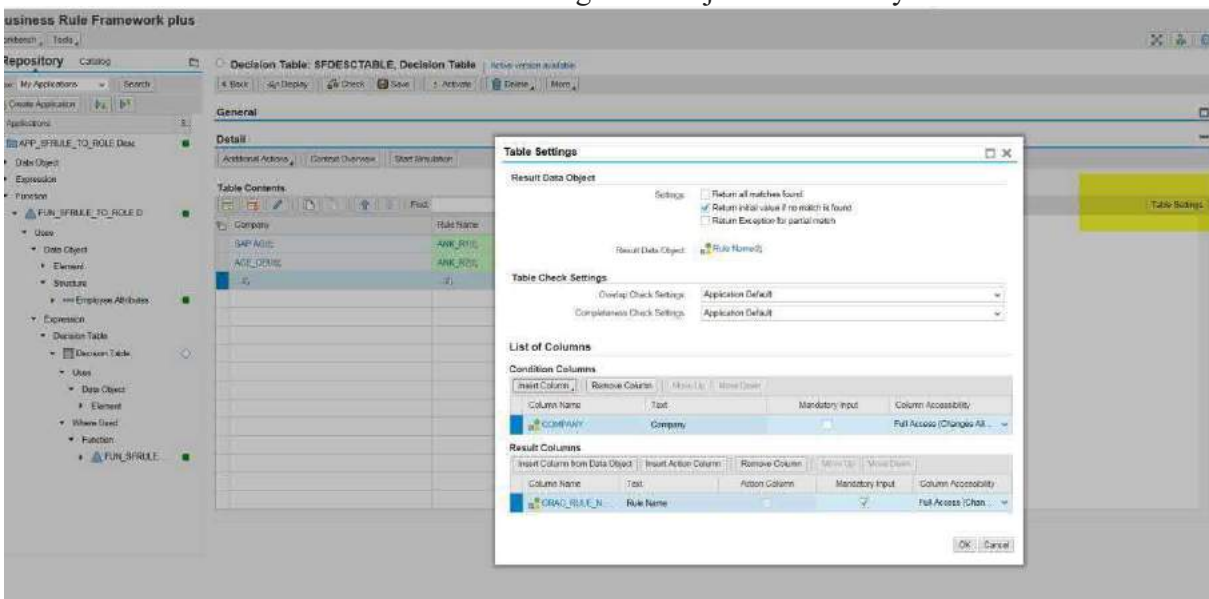


5. Give the DDIC Element a name. Click *OK*.

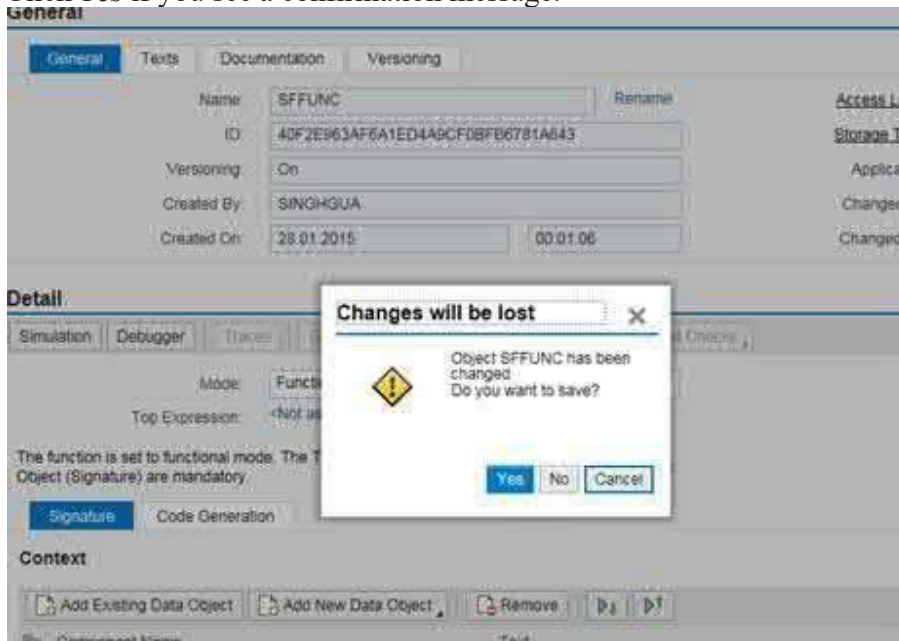
6. Enter a name and description for this rule result set object.



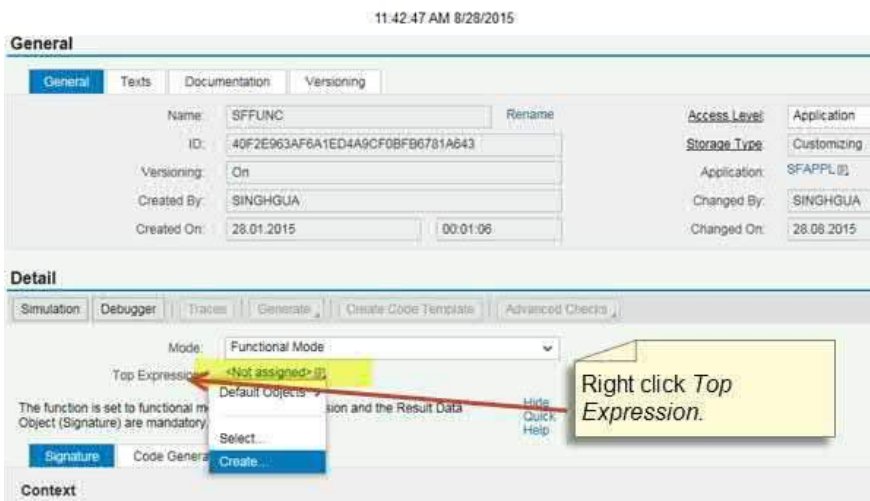
7. Click either Create or Create and Navigate to Object followed by Save and Activate.



- Click *Yes* if you see a confirmation message.



- To create the decision table expression, in the *Details* section, right click *Top Expression*.



10. In the **Type** field, select *Decision Table*. Then click *Create And Navigate to Object*.

11. Enter values for the attributes as shown in the sample below.

11:53:35 AM 8/28/2015

Create Object

General data

Type: Decision Table

* Name: SFDECISION2

Short Text: Decision Table 2

Text: Decision Table 2]

Application: SFAPP3

Is Reusable:

Result

For the result, you can choose data objects from the list below. If you choose more than one object, a new structure containing all chosen objects is created as result object. Instead of selecting objects from the **Possible Result Data Objects** list, you can also decide to use the predefined "Actions" table data object as expression result by clicking the checkbox provided for that purpose. Assigning the "Actions" table or objects from the list is mutually exclusive.

Result Name: GRAC_RULE_NAME Text: Rule Name

Possible Result Data Objects

Add Result Data Object

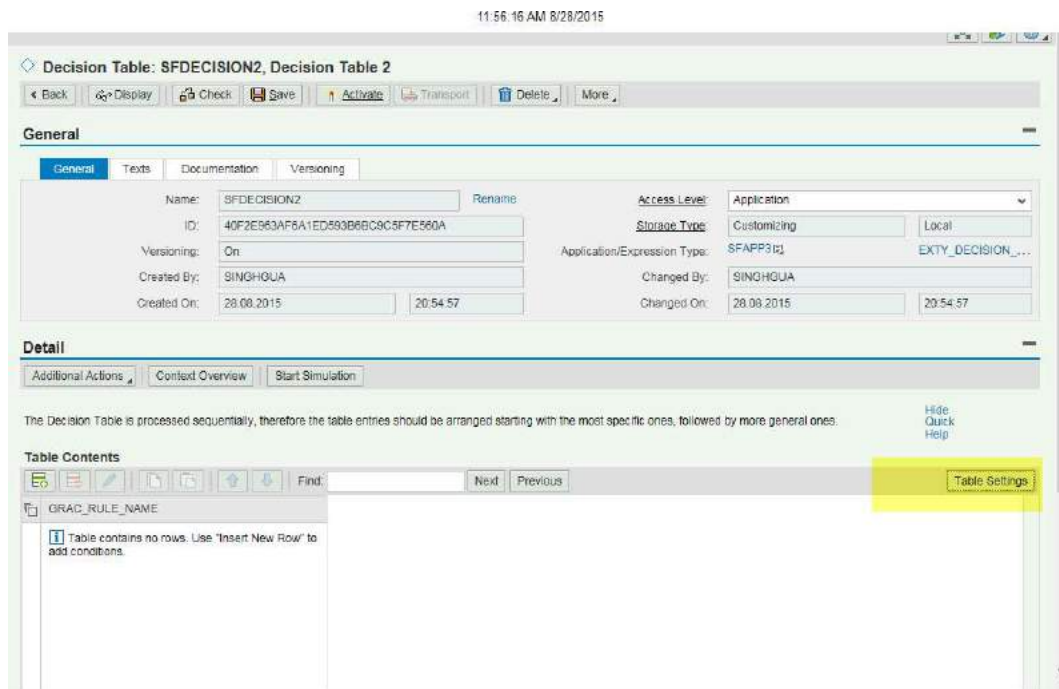
Object	Text	Type
<input checked="" type="checkbox"/> GRAC_RULE_NAME	Rule Name	Element
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

Expression Tables: Actions

Create Create And Navigate To Object Cancel

12. Click *Create and Navigate to Object*.

If you do not see the employee structure, add it by clicking *Table Settings*.



13. Click *From Context Data Objects*.

11:58:48 AM 8/28/2015

Table Settings
□ ×

Result Data Object

Settings: Return all matches found
 Return initial value if no match is found
 Return Exception for partial match

Result Data Object:

Table Check Settings

Overlap Check Settings:

Completeness Check Settings:

List of Columns

Condition Columns

Insert Column Remove Column Move Up Move Down

From Context Data Objects..	Text	Mandatory Input	Column Accessibility
From Expression..			

no condition columns have been created yet.

Result Columns

Insert Column from Data Object Insert Action Column Remove Column Move Up Move Down

Column Name	Text	Action Column	Mandatory Input	Column Accessibility
<input type="checkbox"/> GRAC_RULE_N...	GRAC_RULE_NAME	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Full Access (Chan... ▾)

14. You can select any attribute from the employee structure object on which you want to run your decision table. One sample scenario is DEPARTMENT as shown in the screenshot.

12:03:14 PM 8/28/2015

[Hide Search Fields](#)

Search Criteria

Element Type	is equal to	Any	+
Name	is equal to	*	+ -
Text	is equal to	*	+ -

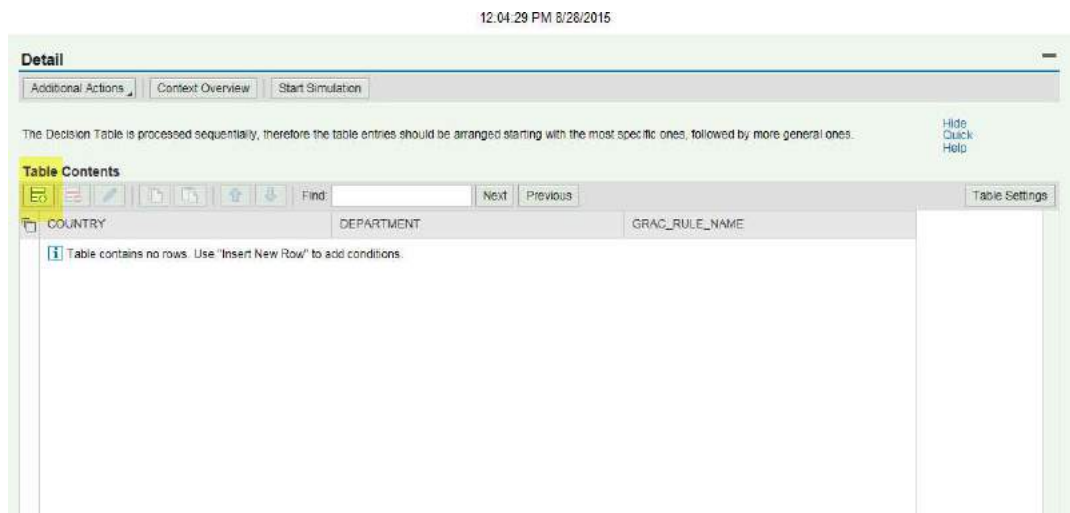
Maximum Number of Results:

Result list: 12 objects found

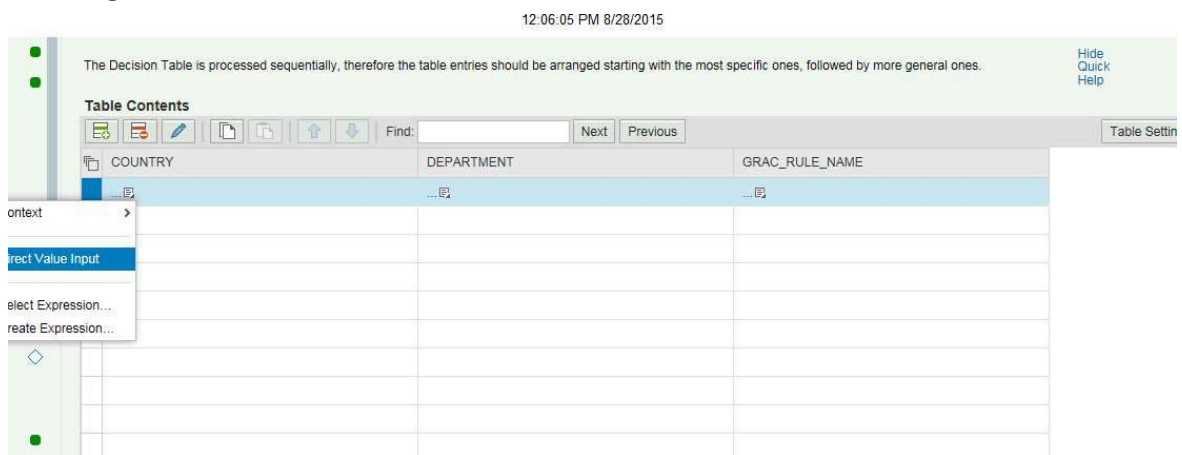
Object	Status	Type	Application
GRAC_S_EMPLOYEE	●	Structure	SFAPP3
ZRTEST_FLD_YESNO	●	Boolean	SFAPP3
COMPANY	●	Text	SFAPP3
COUNTRY	●	Text	SFAPP3
DEPARTMENT	●	Text	SFAPP3
EMPOSITION	●	Text	SFAPP3
JOBTITLE	●	Text	SFAPP3
LOCATION	●	Text	SFAPP3
ZEMPTYTYPE	●	Text	SFAPP3
ZREGION	●	Text	SFAPP3

15. Click *OK*.

16. Click Table Contents.



17. The screen displays a condition row. Right-click to assign a value to a condition. You can assign a direct value as shown below.



12:10:36 PM 8/28/2015

The Decision Table is processed sequentially, therefore the table entries should be arranged starting with the most specific ones, followed by more

Table Contents

DEPARTMENT	GRAC_RULE_NAME
...	...

DEPARTMENT
is equal to Finance Change
OK Clear Cell Cancel

18. Click *OK*.

19. Right click on `GRAC_RULE_NAME` to enter a specific value.

12:11:25 PM 8/28/2015

Additional Actions Context Overview Start Simulation

The Decision Table is processed sequentially, therefore the table entries should be arranged starting with the most specific ones, followe

Table Contents

DEPARTMENT	GRAC_RULE_NAME
FINANCE	...

Direct Value Input
Select Context Parameter...
Default Objects
Select Expression...
Create Expression...

12:13:34 PM 8/28/2015

The screenshot shows a search results window titled "Search: GRAC_RULE_NAME". Below the title bar, it displays "Results List: 26 results found for GRAC_RULE_NAME". There are two buttons: "Personal Value List" and "Show Search Criteria". A table lists the results:

Rule Name
AC PAYABLE3
ACCOUNT RULE

20. Either you can type the name of the rule to be mapped as a Result for this condition in the text box, or you can press the F4 key.

12:14:35 PM 8/28/2015

The screenshot shows the "Detail" view of a decision table. It includes buttons for "Additional Actions", "Context Overview", and "Start Simulation". A note states: "The Decision Table is processed sequentially, therefore the table entries should be arranged starting with the most specific ones, followed by more general".

Table Contents

DEPARTMENT: FINANCE | GRAC_RULE_NAME: ACCOUNT RULE

GRAC_RULE_NAME: ACCOUNT RULE

Buttons: OK, Clear Cell, Cancel

21. Select or type the rule that you want as a result object. The previous screen displays.
22. Click *OK*. Activate the function.

Decision Table: DT_SFFUNCT, Functi

Check object consistency and make object active for productive use

General

Detail

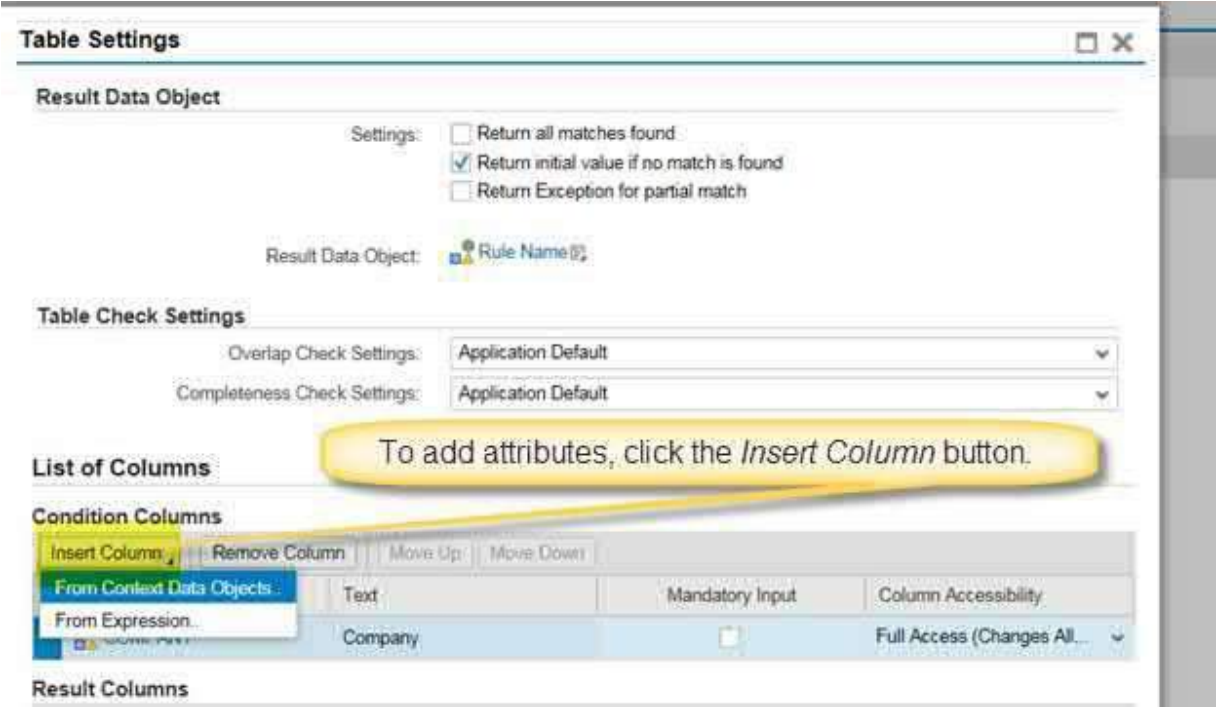
The Decision Table is processed sequentially, therefore the table entries should be arranged starting with the most specific ones, followed t

Table Contents

DEPARTMENT	GRAC_RULE_NAME
FINANCE	ACCOUNT RULE

23. The decision table is now configured for the following rule:
 For an employee with attribute value of *Finance* for Department, the rule ACCOUNT_RULE will be executed

24. Click *Table Settings*. The screenshot above shows that *Company* is one of the selected attributes for decision table. You can select more attributes by clicking on the *Insert Column* button.



25. You can select more attributes as shown in the sample below.

Search Criteria

Element Type	is equal to	Any	+
Name	is equal to	*	+ -
Text	is equal to	*	+ -

Maximum Number of Results:

Result list: 13 objects found

Object	Status	Type	Application
Employee Attributes	●	Structure	APP_SFRULE_TO_ROLE Desc
Business Process	●	Text	APP_SFRULE_TO_ROLE Desc
Company	●	Text	APP_SFRULE_TO_ROLE Desc
Cost Center	●	Text	APP_SFRULE_TO_ROLE Desc
Department	●	Text	APP_SFRULE_TO_ROLE Desc
Employee Type	●	Text	APP_SFRULE_TO_ROLE Desc
Functional Area	●	Text	APP_SFRULE_TO_ROLE Desc
Functional Area	●	Text	APP_SFRULE_TO_ROLE Desc
Job	●	Text	APP_SFRULE_TO_ROLE Desc
Location	●	Text	APP_SFRULE_TO_ROLE Desc

Previous Next Show All Objects Where Used

Ok Cancel

26. Once attributes are selected, you can specify values for them as shown in the example below.

Decision Table: SFDESCTABLE, Decision Table Active version available

[Back](#) | [Display](#) | [Check](#) | [Save](#) | [Activate](#) | [Delete](#) | [More](#)

General □

Detail -

[Additional Actions](#) | [Context Overview](#) | [Start Simulation](#)

Table Contents

[New](#) | [Edit](#) | [Delete](#) | [Refresh](#) | [Find](#) | [Next](#) | [Previous](#) [Table Settings](#)

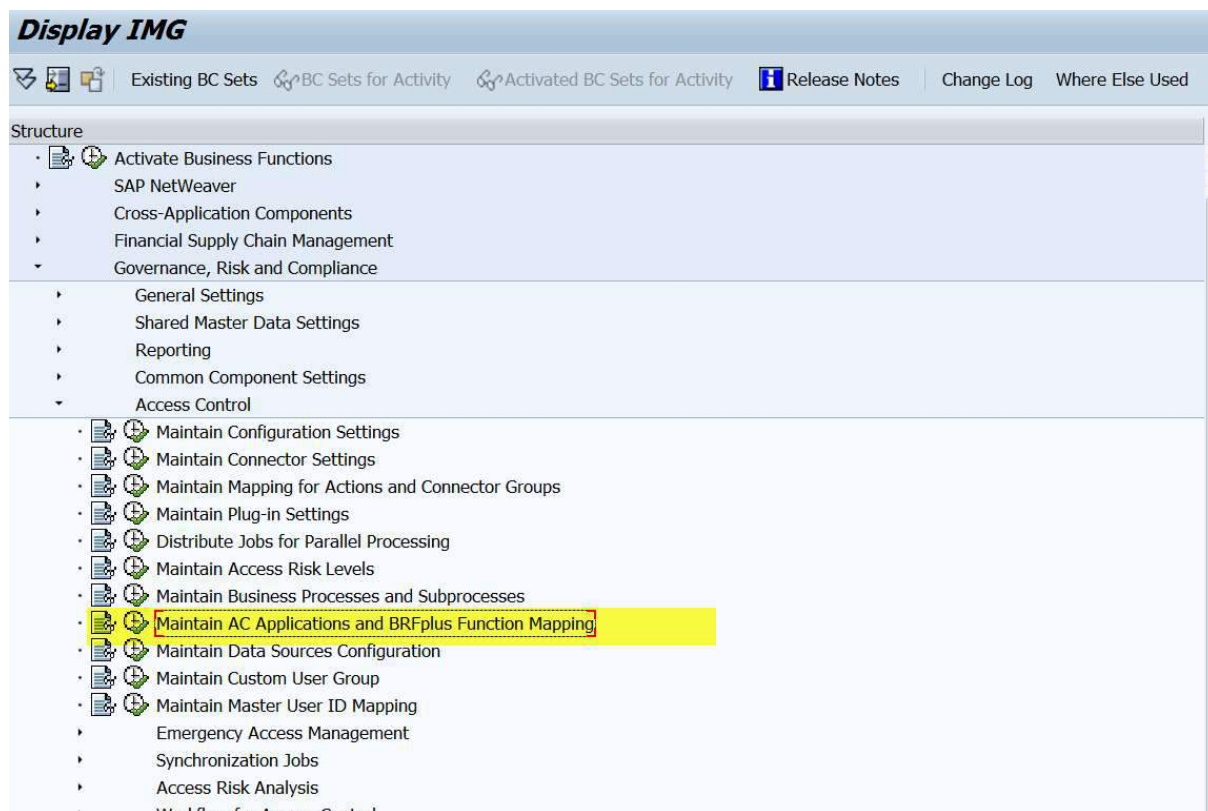
Company	Location	Business Process	Rule Name
SAP AG[0]	PALO ALTO[0]	ES00 (Basic)[0]	ANK_R1[0]
ACE_DEU[0]	GERMANY[0]	FI00 (Finance)[0]	ANK_R2[0]

4.12 Mapping BRF+ to SAP Access Control Application IDs

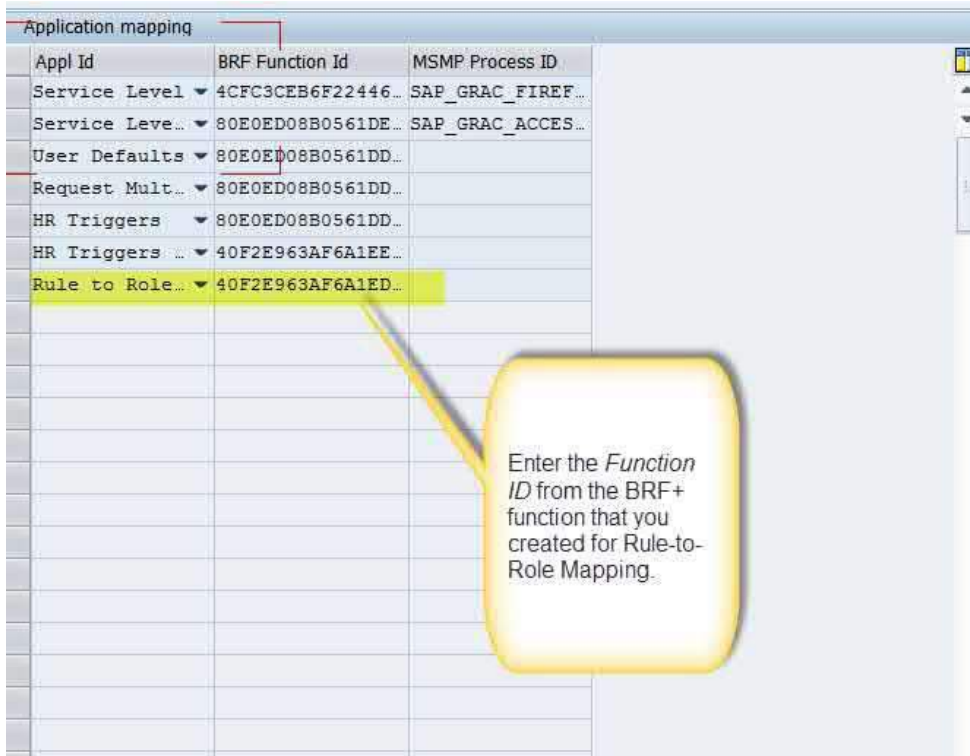
Once you have defined the BRF+ application that determines which roles to assign to employees based on the employee's attributes, you must map the relevant function ID to an SAP Access Control *Application ID*.

Procedure

1. In the SAP Reference IMG, choose Governance Risk, and Compliance → User provisioning → Maintain Access Control Applications and BRF+ Function Mapping



2. Enter the *Function ID* (you noted the ID in the previous section) for the BRF+ Rule-to-Role Mapping.



3. *Save* your entry.

4.13 Locating URLs for SAP Cloud Integration

Follow the steps below to find the URLs that you need to set up the SAP Cloud Integration channel adaptors.

Procedure

1. Go to SOA Management by executing transaction *SOAMANAGER*.
2. Click Web Service Configuration.
3. In the Search Criteria fields, enter the Web service name, for example, GRAC_SFEC_HR_TRIGGER, and click *Search*.
4. On the Search Result screen, click the relevant web service.

Design Time Object Search Configuration Search

Search criteria

Object Type is All

Object Name is GRAC_SFEC_HR_TRIC

Maximum Number of Results: 100

Search Clear values Reset search criteria

Search Result

Internal Name	Type	Name
GRAC_SFEC_HR_TRIGGER	Service Definition	GRAC_SFEC_HR_TRIGGER

5. On the Configurations screen, select the relevant service, and click the eyeglass icon to *Display Bindings*.

Details of Service Definition: GRAC_SFEC_HR_TRIGGER

Overview Configurations Classifications Details

Define Services and Bindings

Create Service Activate Deactivate Delete Republish Display as List

Service/Binding	Actions	State	Description
FA		Active	Provider for Service Definition 'GRAC...
binding			
GRAC_SFEC_HR_TRIGGER		Active	grac_sfec_hr_trigger
GRAC_SFEC_HR_TRIGGER			

6. On the **Transport Settings** tab, copy the **Calculated Access URL**. You will use it later to configure SAP Cloud Integration.

Configuration: Service Definition 'GRAC_SFEC_HR_TRIGGER', Service 'GRAC_SFEC_HR_TRIGGER', Binding 'GRAC_SFEC_H

Save Edit

Provider Security **Transport Settings** Message Attachments Identifiable Business Context Operation Settings A

Transport Binding

Alternative Access URL:	
Calculated Access URL:	/sap/bc/srt/rfc/s 'grac_sfec_hr_trigger'
Calculated Protocol:	HTTP
Make Local Call:	No Call in Local System
State Management Timeout:	0

i Note

These URLs are only accessible internally. To access the URLs externally, copy the first part from the SOAMANAGER browser window, for example, <https://xxx.sap.corp:44322/>. In the WSDL and endpoint URLs displayed in the *Details of Provider Configuration* screen, replace the first part of the URLs with the external part you copied before

5 Configuring SAP Cloud Integration Process

SAP provides prepackaged, generic integration content called integration flows for the integration of SAP Access Control with SAP SuccessFactors Employee Central.

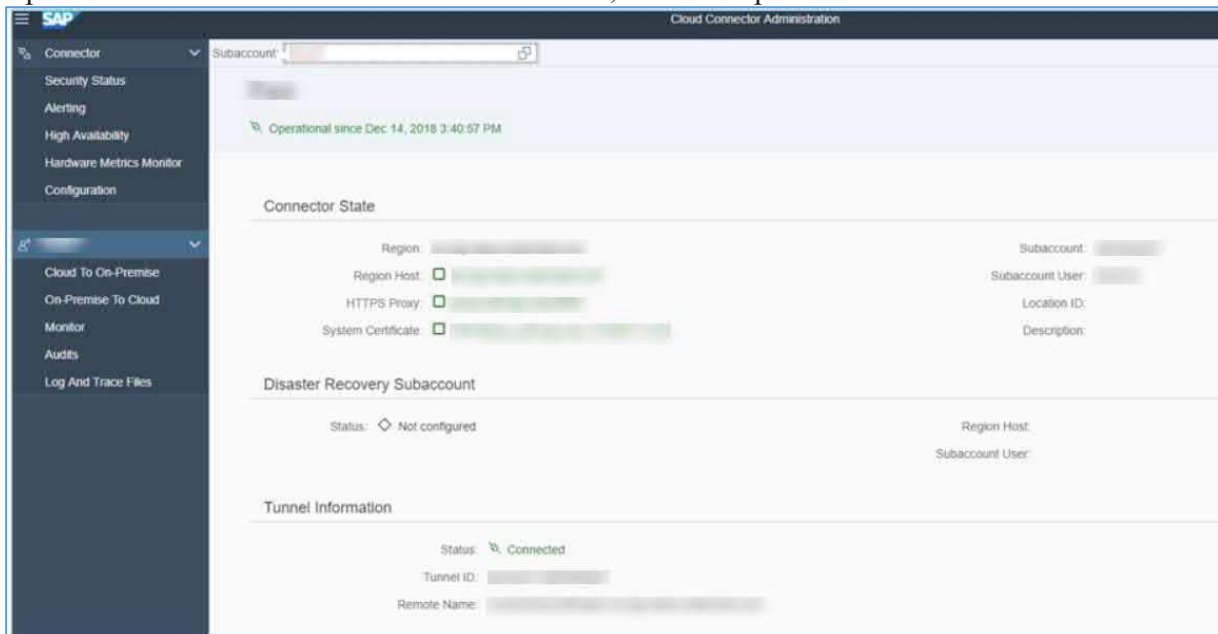
Prerequisites

You have received the SAP Cloud Integration provisioning email and the administrator has created the necessary users in SAP Cloud Integration.

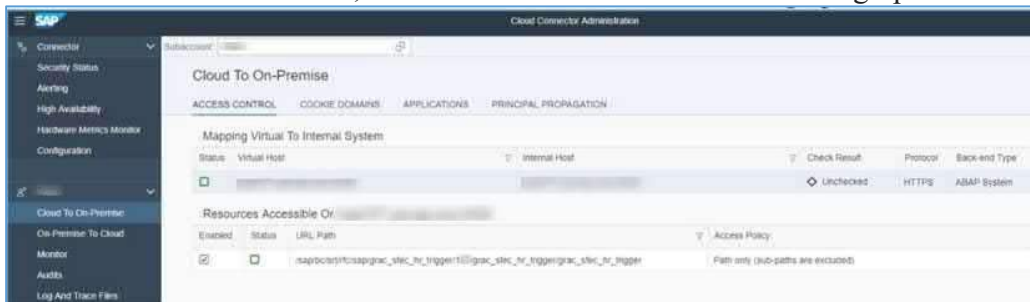
5.1 Configure SAP Cloud Connector Settings

To enable communication between your on-premise access control system and SFEC, you must configure the SAP Cloud Connector on the access control system.

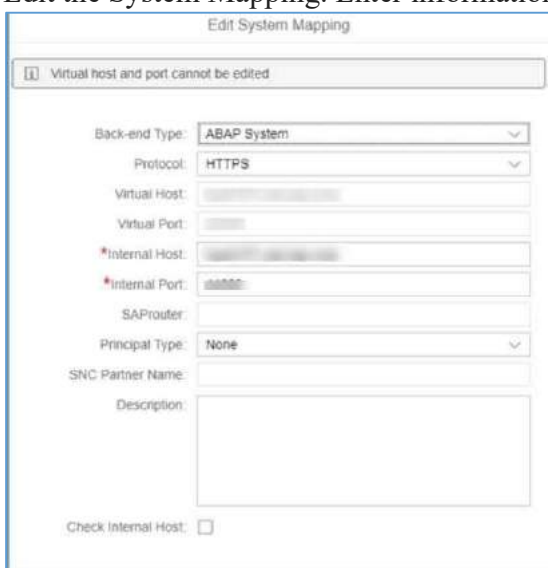
1. Open the SAP Cloud Connector as administrator, and then open subaccount for SFEC.



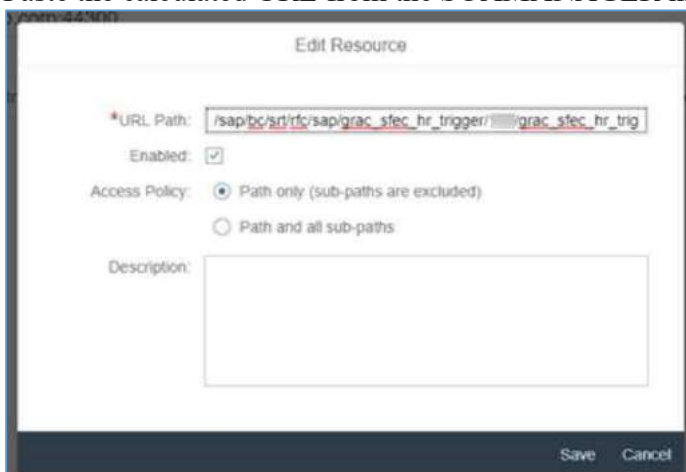
2. Click *Cloud To On-Premise*, and add the URL Path as shown in the graphic below.



3. Edit the System Mapping. Enter information for the GRC system.



4. Paste the calculated URL from the SOAMANAGER in the URL Path field.



5.2 Configure User Credentials for SFEC and GRC System

After you have configured the SAP Cloud Connector (in previous step), you need to create user credentials for the on-premise GRC system and SFEC in the SAP Cloud Integration.

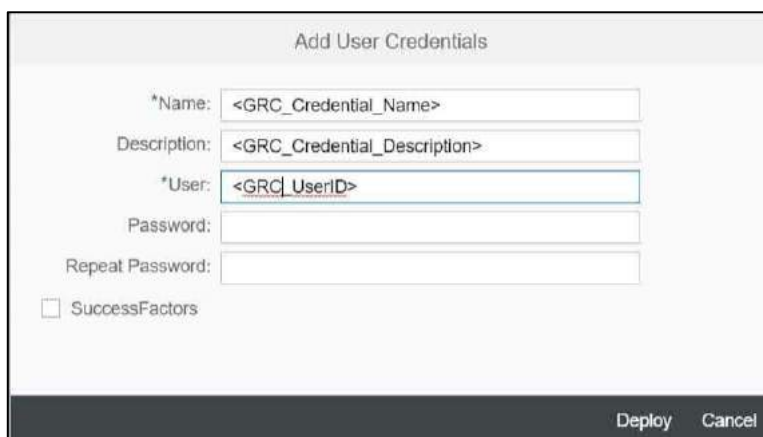
5.2.1 Configure GRC User Credentials

Prerequisites

The communication user is created in SAP Access Control.

Procedure

1. Access the SAP Cloud Integration screen by opening the URL from the provisioning email. It should be in the format: *https://<SAP Cloud Integration CI>*.
2. In the **Monitor** tab, navigate to **Manage Security Material**, and click **Security Material**.
3. Click **Add** → **User Credential** in the top right corner.
4. Enter a meaningful *Name* – this will be referenced in iFlows – a *Description*, and the *User* and *Password*. Do **not** check the *SuccessFactors* check box.



Note **i**

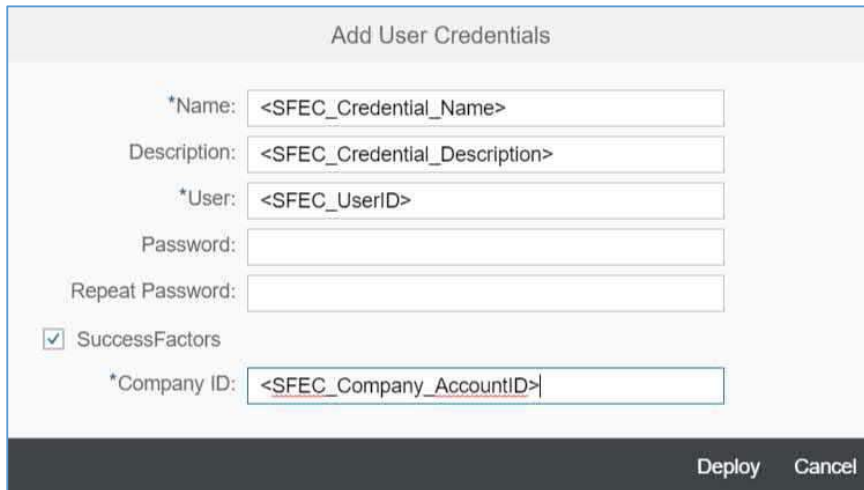
The User Name and Password must be taken from the *communication user* created in SAP Access Control.

5. Click **Deploy**.

5.2.2 Configure SFEC User Credentials

Procedure

1. Access the SAP Cloud Integration screen by opening the URL from the provisioning email. It should be in the format: *https://<SAP Cloud Integration CI>*.
2. In the **Monitor** tab, navigate to **Manage Security Material**, and click **Security Material**.
3. Click **Add** → *User Credential* in the top right corner.



4. Enter a meaningful *Name* – this will be referenced in iFlows – a *Description*, and the *User* and *Password*. Be sure to check the *SuccessFactors* check box and provide the *Company ID*.
5. Click **Deploy**.

Sample of completed configuration (one for SFEC and one for GRC):



Name	Type
system.jks	Keystore
SFLOGON	Credentials
GRCLOGON	Credentials

5.3 Configure and Deploy iFlows

To configure and deploy the SAP Access Control integration, you must copy the delivered integration package to your workspace and modify it.

Prerequisites

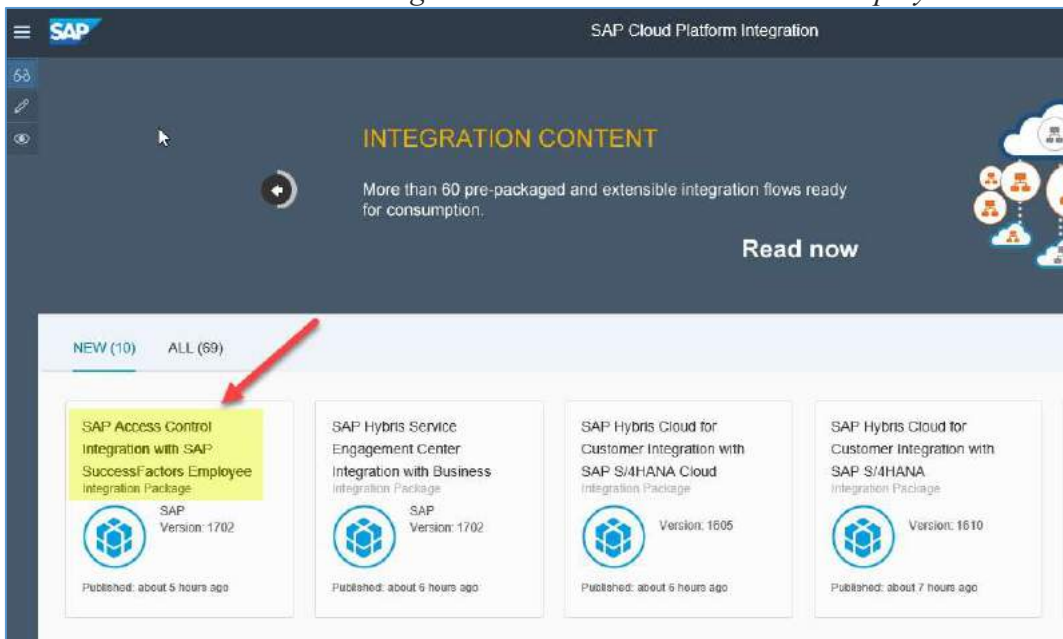
1. To be able to import and deploy iFlows, you need the *AuthGroup.IntegrationDeveloper* role assigned in your tenant.
2. For certificate-based authentication between SAP Access Control and SAP Cloud Integration, you need the client certificate from SAP Access Control. For more information, see the section *How to get the SAP Cloud Integration Client Certificate*.

Process

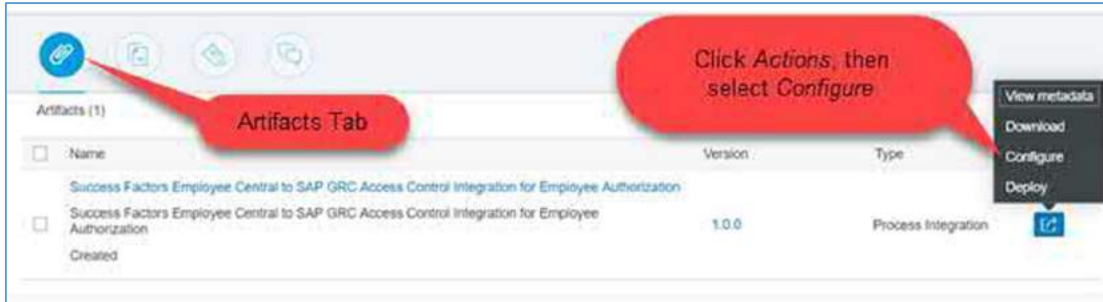
1. On SAP Cloud Integration, choose the *Discover* icon.



2. Choose *SAP Access Control Integration with SAP SuccessFactors Employee Central*.



3. In the **Discover** tab, hover over the integration flow (*SuccessFactors Employee Central to SAP GRC Access Control Integration for Employee Authorization*) to display the tooltip, and click *Copy to Workspace*.
4. In the *Artifacts* tab, select the desired iFlow package, click the *Actions* icon, and select *Configure*.



5. Create a receiver for SFEC:
 - a. On the *Receiver* tab, select the SAP SuccessFactors receiver from the dropdown.
 - b. Enter the address and credential name for the SAP SuccessFactors system.

Configure "Success Factors Employee Central to SAP GRC Access Control Integrat

Timer Receiver More

Receiver: SuccessFactorsCompoundEmployeeEndpoint

Adapter Type: SuccessFactors

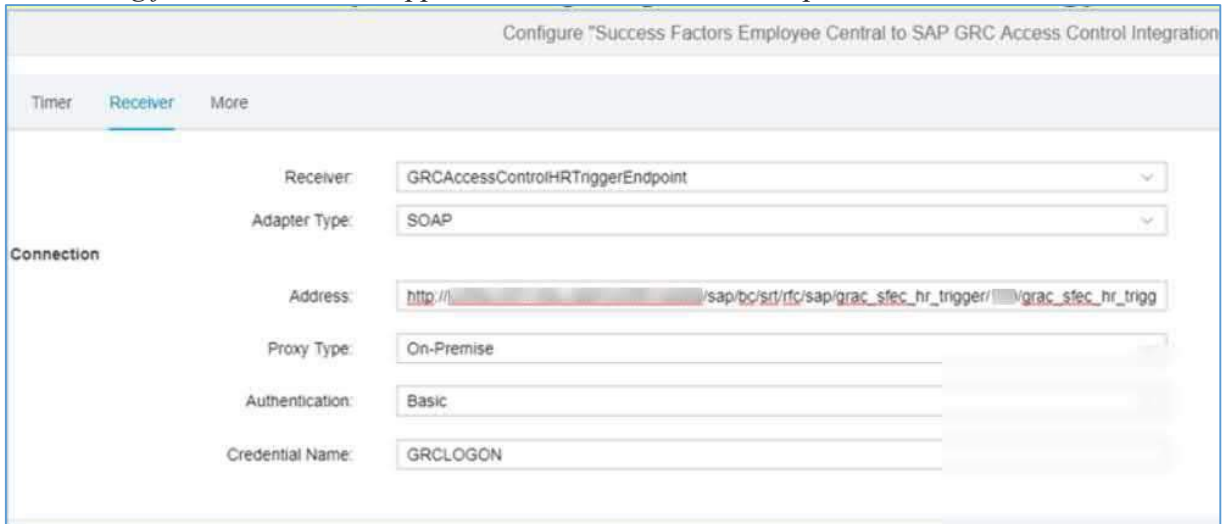
Processing

Address: https:// . successfactors.com

Credential Name: SFLOGON

- c. Allow the authentication type to default to *Basic Authentication*.
- d. Click *Save* and then click *Deploy*.

6. Create a Receiver for SAP Access Control:
 - a. On the *Receiver tab*, select the SAP Access Control receiver from the dropdown.
 - b. Provide the address and credential name for the SAP Access Control receiver.
The URL is built based on the *web-service calculated URL* you created in *Create a Binding for Web Services*. Append it with the hostname and port.



Configure "Success Factors Employee Central to SAP GRC Access Control Integration"

Timer Receiver More

Receiver: GRCAccessControlHRTriggerEndpoint

Adapter Type: SOAP

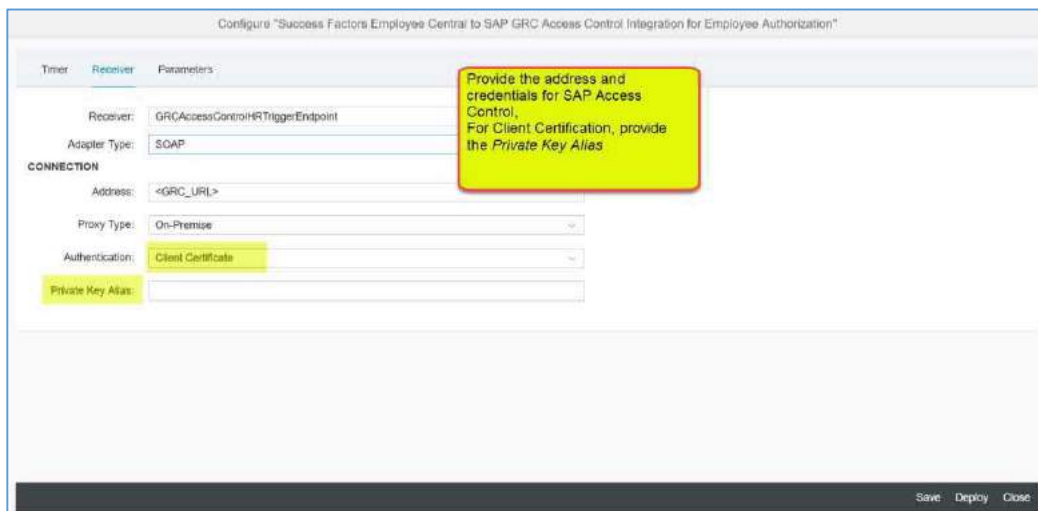
Address: http://.../sap/.../grac_sfec_hr_trigg

Proxy Type: On-Premise

Authentication: Basic

Credential Name: GRCLOGON

- c. Choose authentication type as *Basic* or *Client Certificate*.
 - If it is *Basic* authentication, provide the credential name.
 - If it is *Client Certification*, provide the *Private Key Alias*.
 For more information, see the section *How to get the SAP Cloud Integration Client Certificate*.



Configure "Success Factors Employee Central to SAP GRC Access Control Integration for Employee Authorization"

Timer Receiver Parameters

Receiver: GRCAccessControlHRTriggerEndpoint

Adapter Type: SOAP

CONNECTION

Address: <GRC_URL>

Proxy Type: On-Premise

Authentication: Client Certificate

Private Key Alias:

Provide the address and credentials for SAP Access Control. For Client Certification, provide the Private Key Alias

Save Deploy Close

7. Configure the execution parameters for the initial data load and for subsequent recurring integration runs.

Initial Data Load Configuration

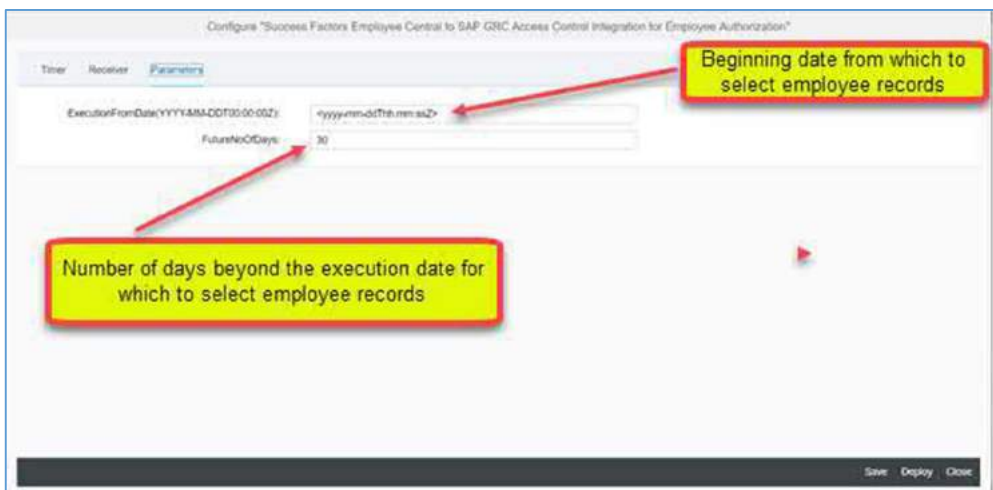
1. Choose the *Parameters* tab.
2. For the initial load, the first time you run the integration, provide the *ExecutionFromDate*. The system selects Employee Central records that were created or modified from this date forward.
3. *FutureNoOfDays*: The parameter controls how far into the future new hires can be processed. Enter the number of days beyond the today's date to consider for validity of employee records.



The *FutureNoOfDays* is 20.

New Hire 1 has a start date of today (7/30/2016)
 New Hire 2 has a start date of August 10 (8/10/2016)
 New Hire 3 has a start date of September 15 (9/15/2016)

SAP Cloud Integration will process new hires that fall within the range of today's date + 20 days. Employees with start dates on or before August 19 (July 30 +20 days) will be processed. Employees with start dates after August 19 will not be processed. In our example, New Hires 1 and 2 will be processed. New Hire 3 will not be processed.



4. Choose the *Timer* tab to schedule the initial load job.
5. Give the *Timer* (job) a descriptive name such as “InitialSFdataload”
6. Check *Run Once* for the initial data load.

7. Click *Save*.

When you are ready to execute the initial load, click *Deploy*.



Recurring Integration Configuration

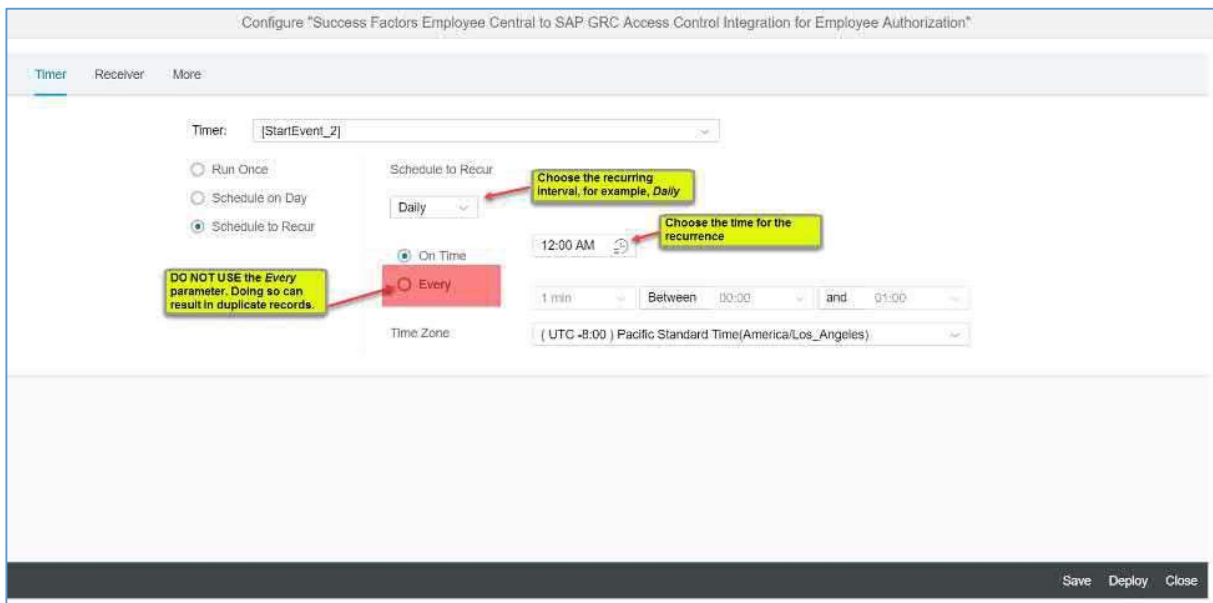
To set up a recurring job:

1. Choose the *Parameters* tab.
2. Leave the *ExecutionFromDate* empty.
3. *FutureNoOfDays*: Enter the number of days beyond the current run date for which you want to include records
4. Click *Save*.
5. Choose the *Timer* tab to schedule the recurring job, and select a timer from the dropdown menu.
6. Click **Schedule to Recur**.
7. Select the recurring interval, for example, *Daily* or *weekly*.
8. Select the *On Time* radio button to fill in the time for your recurring data transfer.

Warning

Do not select *Every* radio button! A recurring job should not be scheduled to run more than once in the same day. Doing so can result in duplicate records.

9. Click *Save*.
When you are ready to execute the job series, click *Deploy*.



5.3.1 Configure and Deploy iFlow - SuccessFactors Employee Central to SAP GRC Access Control Integration for Employee Authorization_OData

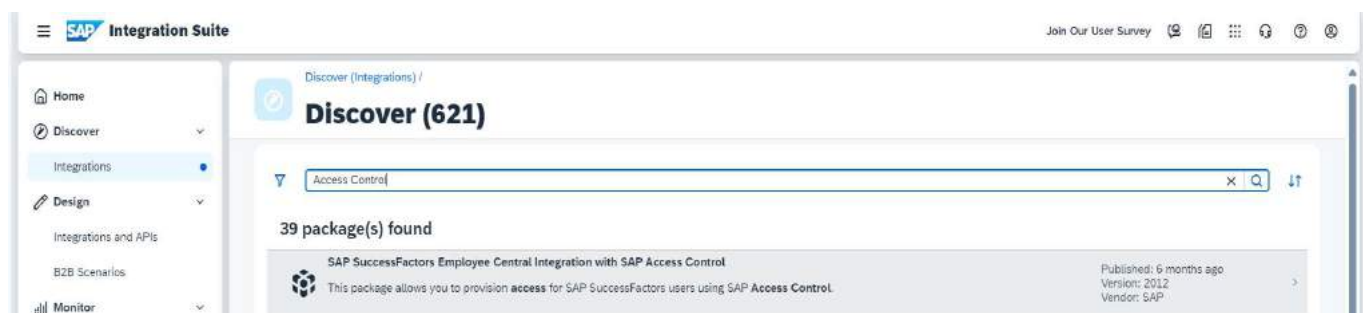
To configure and deploy the SAP Access Control integration, you must copy the delivered integration package to your workspace and modify it.

Prerequisites

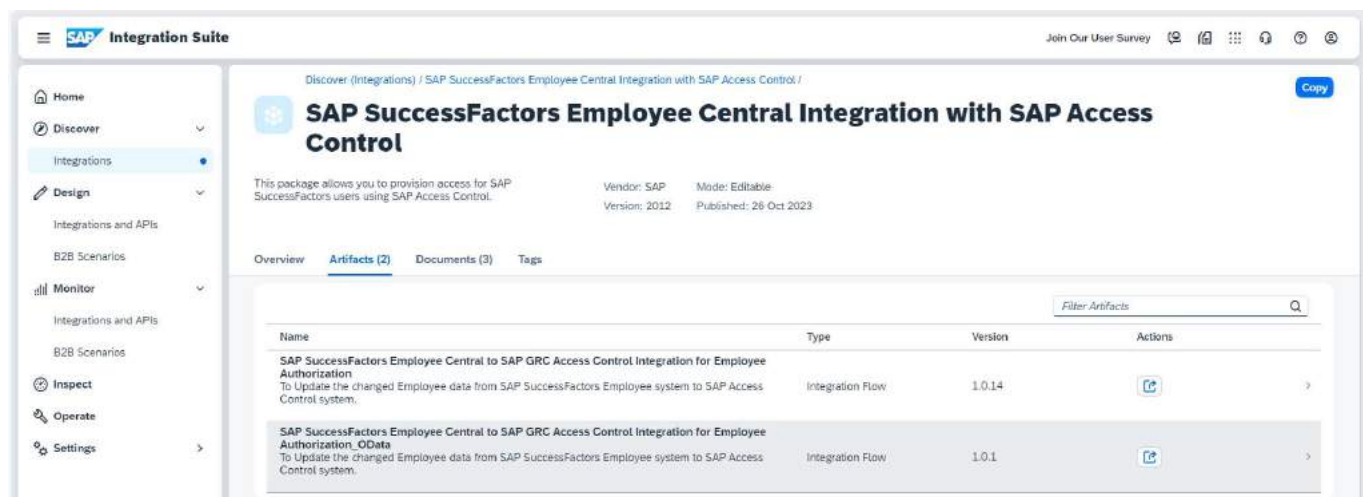
1. *SuccessFactors Employee Central to SAP GRC Access Control Integration for Employee Authorization_OData* iFlow is valid for **GRC 12.0 SP23 and above**.
2. Requirement: Huge data (>5000 records) is fetched from SFEC on daily basis.

Process

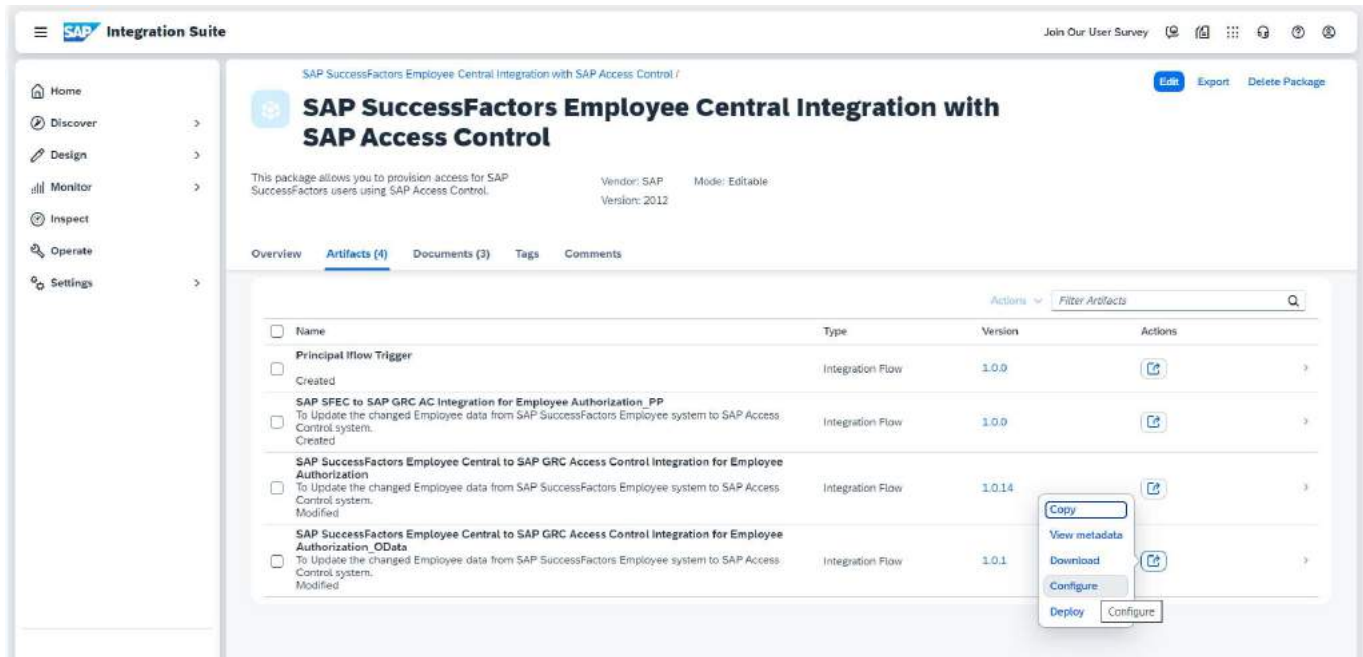
1. On SAP Cloud Integration, choose the *Discover* icon. Choose *SAP Access Control Integration with SAP SuccessFactors Employee Central*



2. In the **Discover** tab, select the integration flow (*SuccessFactors Employee Central to SAP GRC Access Control Integration for Employee Authorization_OData*) and click *Copy to Workspace*.

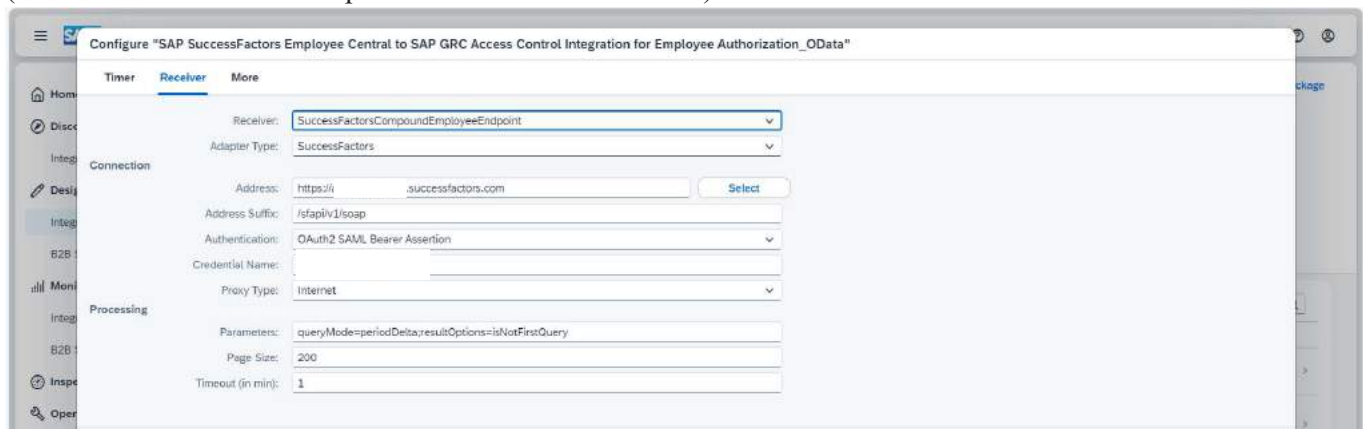


3. In the *Artifacts* tab, select the iFlow package, click the *Actions* icon, and select *Configure*.



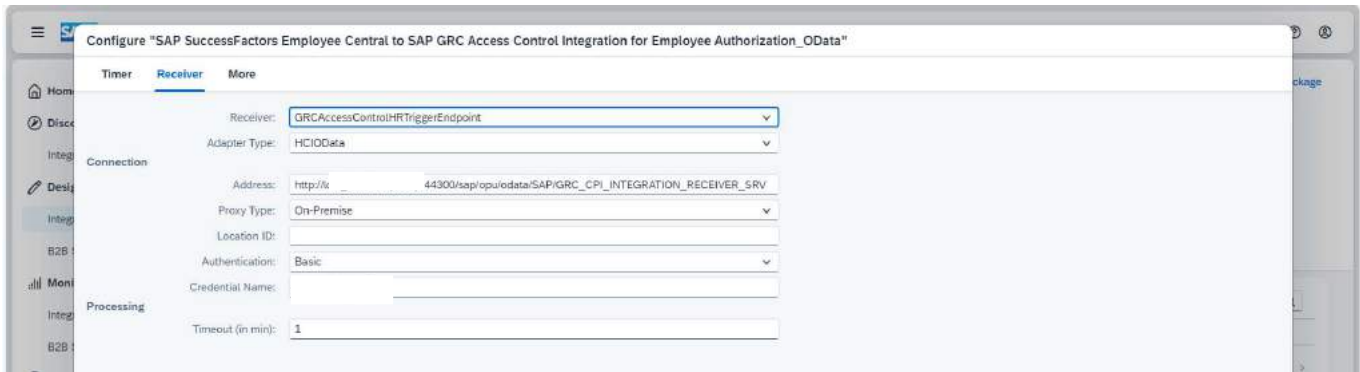
4. Create a receiver for SFEC:

- On the *Receiver* tab, select the SAP SuccessFactors receiver from the dropdown.
 - Enter the address and credential name for the SAP SuccessFactors system.
 - Allow the authentication type to *Basic Authentication/ OAuth Authentication*.
- (For OAuth Authentication please check section - 5.3.1.1)



5. Create a Receiver for SAP Access Control:

- On the *Receiver* tab, select the SAP Access Control receiver from the dropdown.
- Provide address as the <host>:<port>/sap/opu/odata/SAP/GRC_CPI_INTEGRATION_RECEIVER_SRV.
- Provide Proxy-Type as On-Premise and Location ID as location maintained in cloud connector
- Provide Authentication as Basic Authentication.
- Click on Save.



6. Configure the execution parameters for the initial data load and for subsequent recurring integration runs.

Initial Data Load Configuration

1. Choose the *Parameters* tab.
2. For the initial load, the first time you run the integration, provide the *ExecutionFromDate*. The system selects Employee Central records that were created or modified from this date forward.
3. *FutureNoOfDays*: The parameter controls how far into the future new hires can be processed. Enter the number of days beyond the today's date to consider for validity of employee records.



Example

The FutureNoOfDays is 20.

New Hire 1 has a start date of today (7/30/2016)

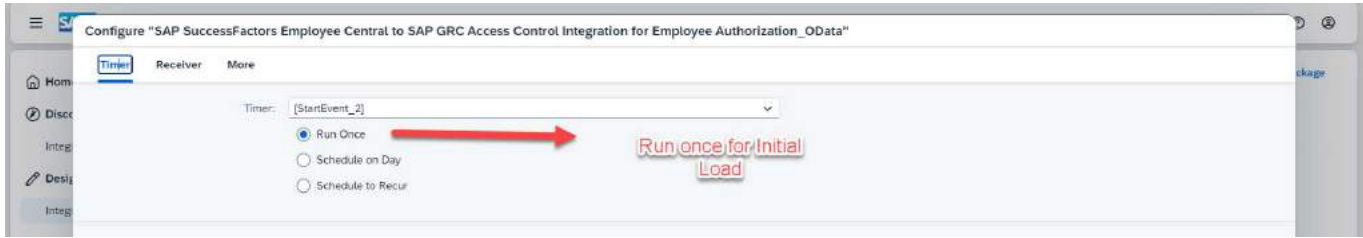
New Hire 2 has a start date of August 10 (8/10/2016)

New Hire 3 has a start date of September 15 (9/15/2016)

SAP Cloud Integration will process new hires that fall within the range of today's date + 20 days. Employees with start dates on or before August 19 (July 30 +20 days) will be processed. Employees with start dates after August 19 will not be processed. In our example, New Hires 1 and 2 will be processed. New Hire 3 will not be processed.

4. Choose the *Timer* tab to schedule the initial load job.
5. Give the *Timer* (job) a descriptive name such as "InitialSFdataload"
6. Check *Run Once* for the initial data load.
7. Click *Save*.

When you are ready to execute the initial load, click *Deploy*.



Recurring Integration Configuration

To set up a recurring job:

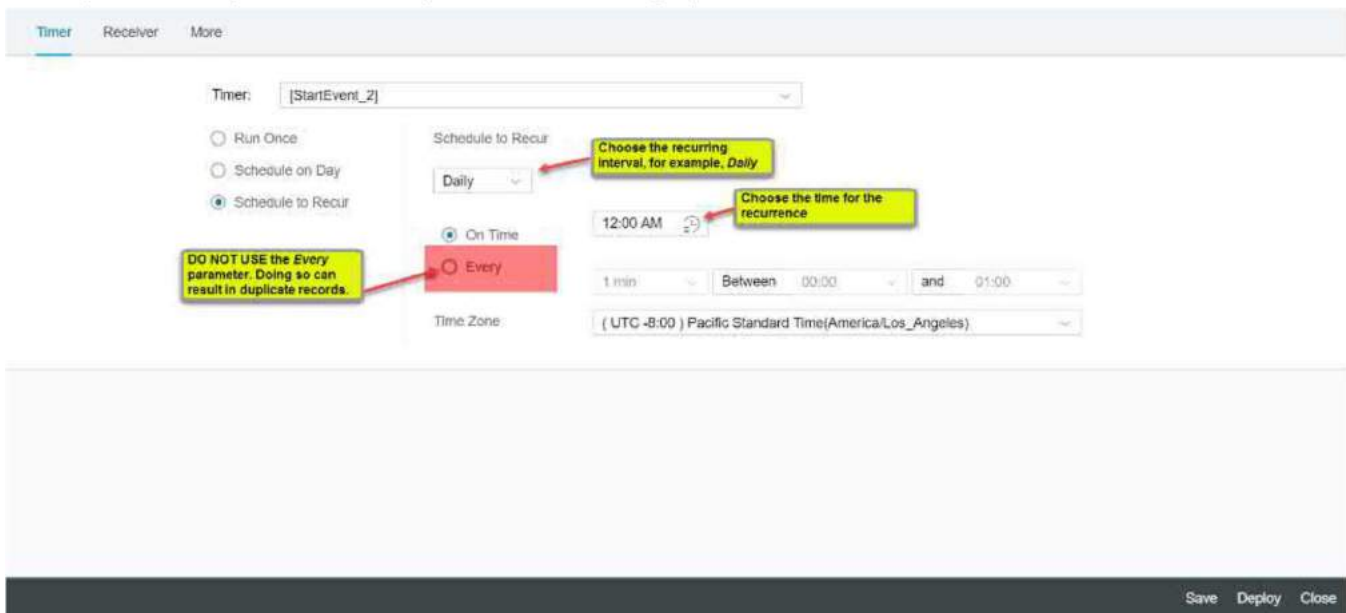
1. Choose the *Parameters* tab.
2. Leave the *ExecutionFromDate* empty.
3. *FutureNoOfDays*: Enter the number of days beyond the current run date for which you want to include records
4. Click *Save*.
5. Choose the *Timer* tab to schedule the recurring job, and select a timer from the dropdown menu.
6. Click **Schedule to Recur**.
7. Select the recurring interval, for example, *Daily* or *weekly*.
8. Select the *On Time* radio button to fill in the time for your recurring data transfer.

Warning

Do not select *Every* radio button! A recurring job should not be scheduled to run more than once in the same day. Doing so can result in duplicate records.

9. Click *Save*.

When you are ready to execute the job series, click *Deploy*.

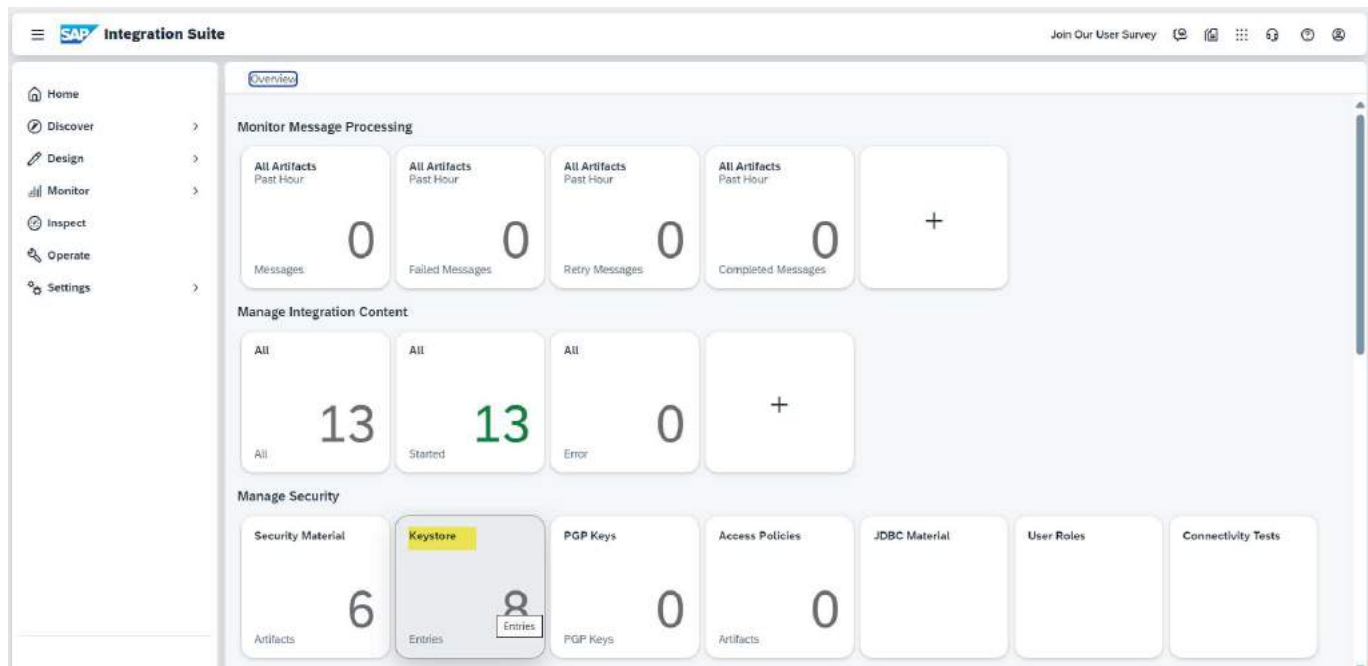


5.3.1.1 How to get the SFEC OAuth2 SAML Bearer Assertion

Follow below steps in CPI and SFEC instance to register the client application and get the OAuth2 SAML Bearer Assertion:

Step 1: Creating a Key Pair in SAP Cloud Integration

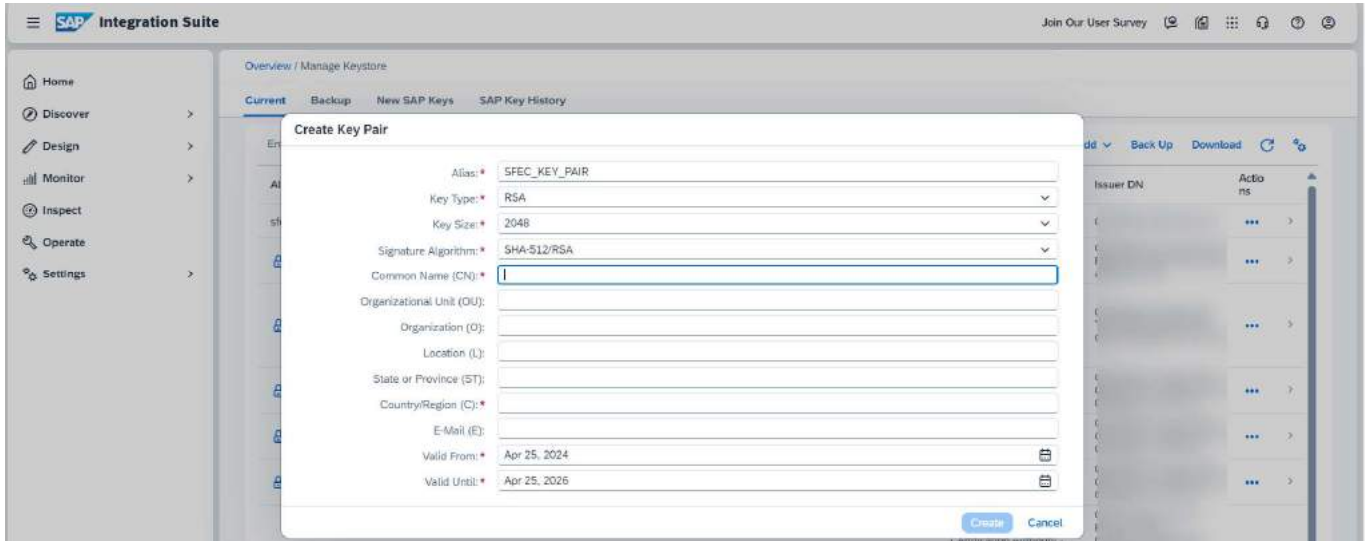
Create a new key pair creation is considered, if you have a valid key pair, you can re-use it by uploading the same. In SAP Cloud Integration Web UI Monitoring section, click on Keystore tile.



Click on the Create -> Key Pair

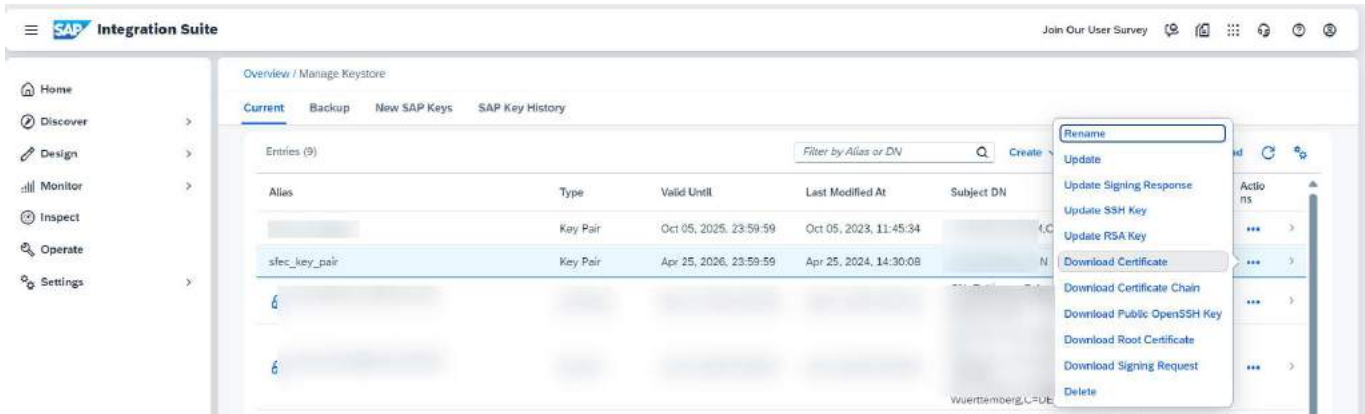


Provide the relevant details. The value for **Common Name (CN)** should be the user name exists in your SAP SuccessFactors instance who has the access/authority to invoke the SuccessFactors API through OAuth2 token.



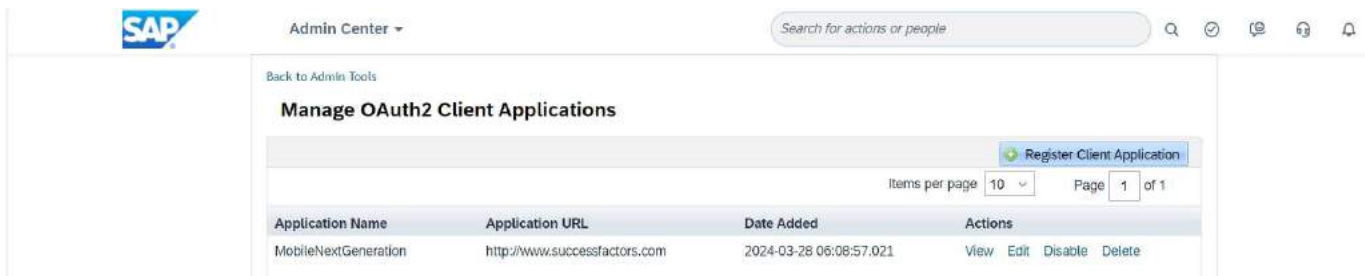
Click on Create button once finished providing details. Copy (or remember) the Alias name for further use.

After creation, download the certificate part of it. The public key of this file will be used while registering the OAuth2 client in SAP SuccessFactors system.

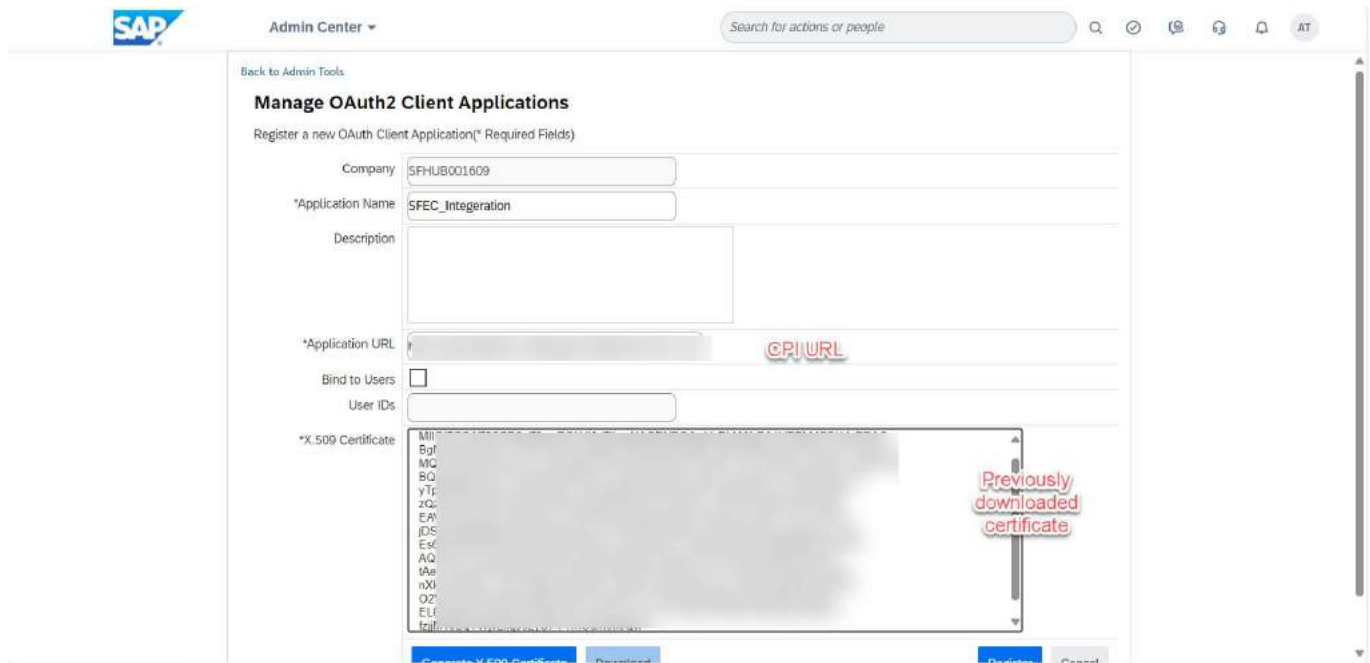


Step 2: Registering an OAuth2 client in SAP SuccessFactors System

Login to your SAP SuccessFactors system as administrator and then create a new OAuth2 Client in ‘Manage OAuth2 Client Applications’ section.

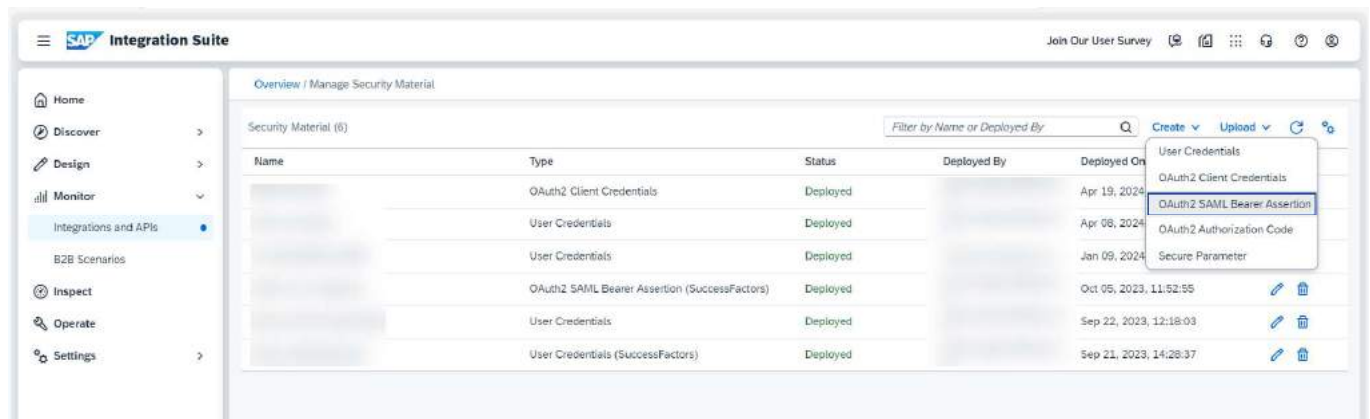


In creating OAuth2 Client Application, provide relevant details, copy the certificate part (the content between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----) and add/paste that into X.509 Certificate place. Click on Register, and get hold of API Key (which will be treated as Client Key when deploying OAuth2 SAML Bearer credentials in SAP Cloud Integration)



Click on Register button.

Click on View button in Manage OAuth2 client application. Copy the API Key value, which will be treated as Client Key while deploying OAuth2 SAML Bearer credentials in SAP Cloud Integration. In the Monitoring Section of SAP Cloud Integration, click on the 'Security Material' UI tile, and then click on Create -> OAuth2 SAML Bearer Assertion.



Provide the relevant details:

Name: your unique name for this key/credentials

Grant Type: OAuth2SAMLBearerAssertion

Audience: www.successfactors.com

Client Key: use the copied value of the **API Key** we saw in steps earlier

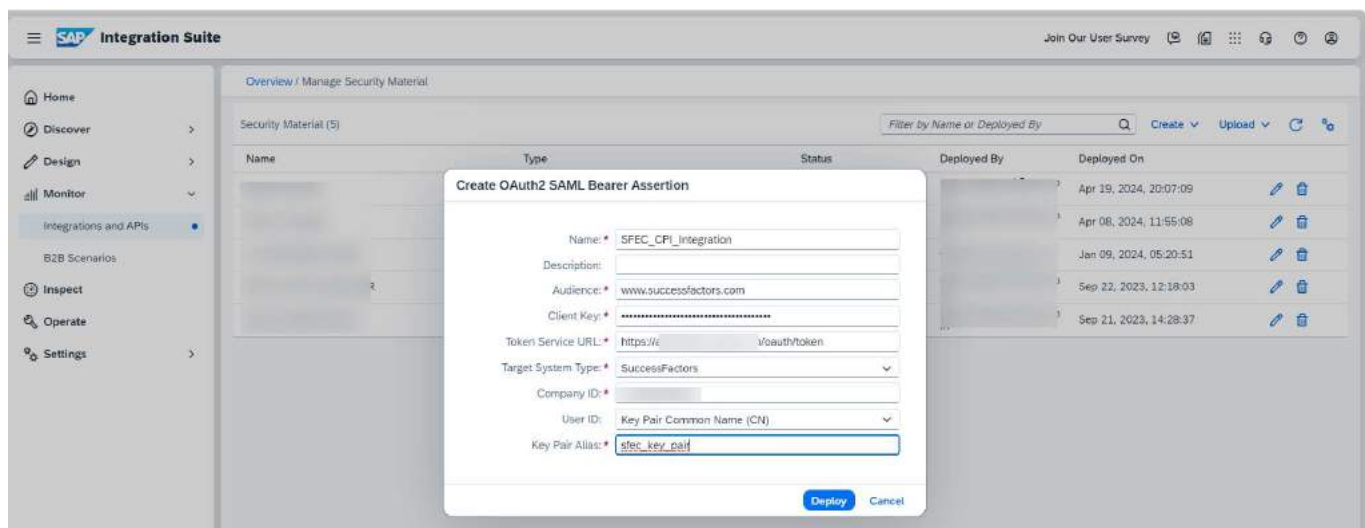
Token Service URL: API URL + **oauth/token**, sample = https://apisalesdemo4.successfactors.com/**oauth/token**

Target System Type: SuccessFactors

Company ID: your SF company ID

User ID: Key Pair Common Name (CN)

Key Pair Alias: your unique name created in earlier instruction (found in Keystore)

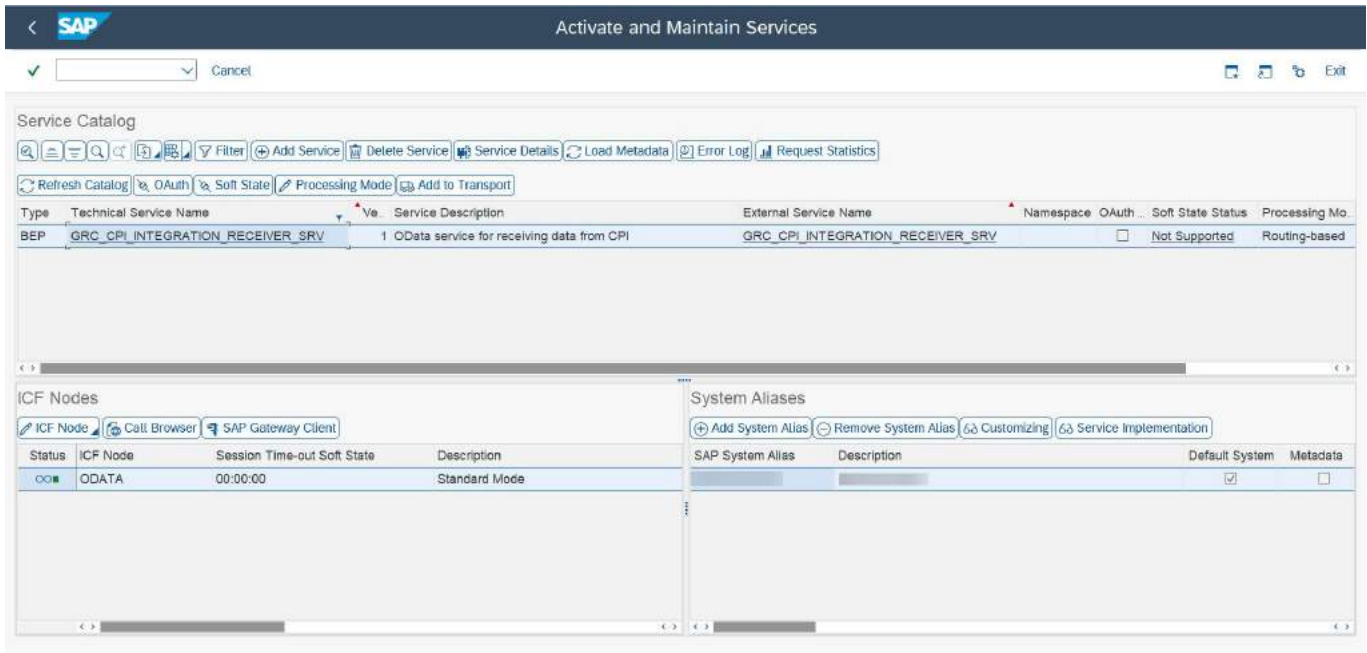


Deploy!

5.3.1.2 How to Register OData Service in GRC system

In GRC system, please follow below steps to register new OData service for CPI Iflow "*SuccessFactors Employee Central to SAP GRC Access Control Integration for Employee Authorization_OData*"

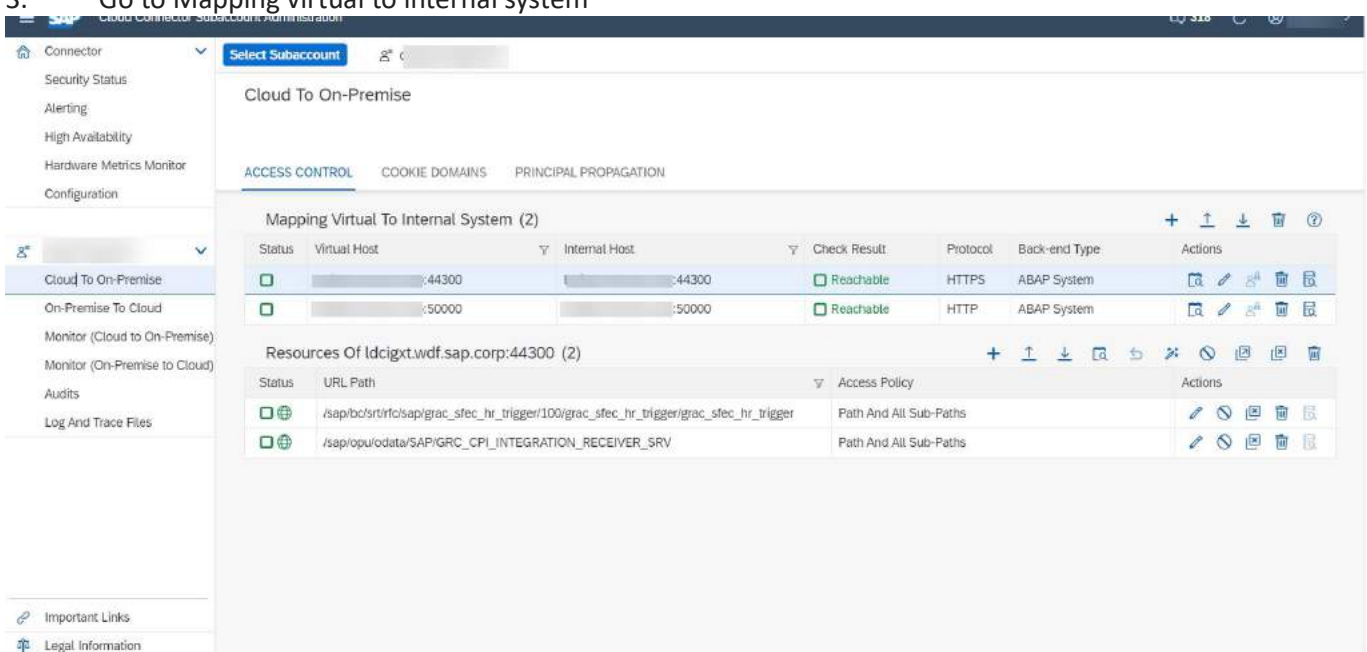
1. Go to /IWFND/MAINT_SERVICE transaction.
2. Add Service "GRC_CPI_INTEGRATION_RECEIVER_SRV" in Gateway client
3. Add system alias



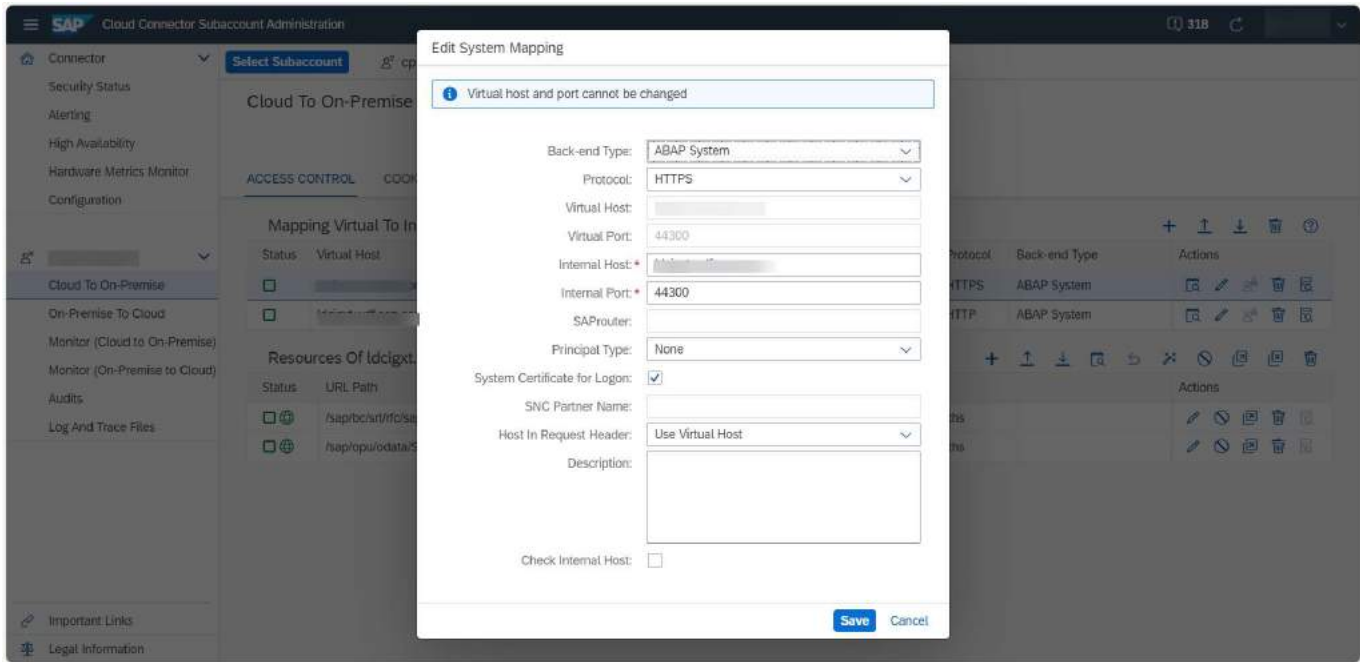
5.3.1.3 How to configure Cloud Connector

For Iflow *SuccessFactors Employee Central to SAP GRC Access Control Integration for Employee Authorization_OData*, please follow below steps to configure cloud connector:

1. Go to Cloud Connector
2. Select the subaccount - cloud to on-premise
3. Go to Mapping virtual to internal system

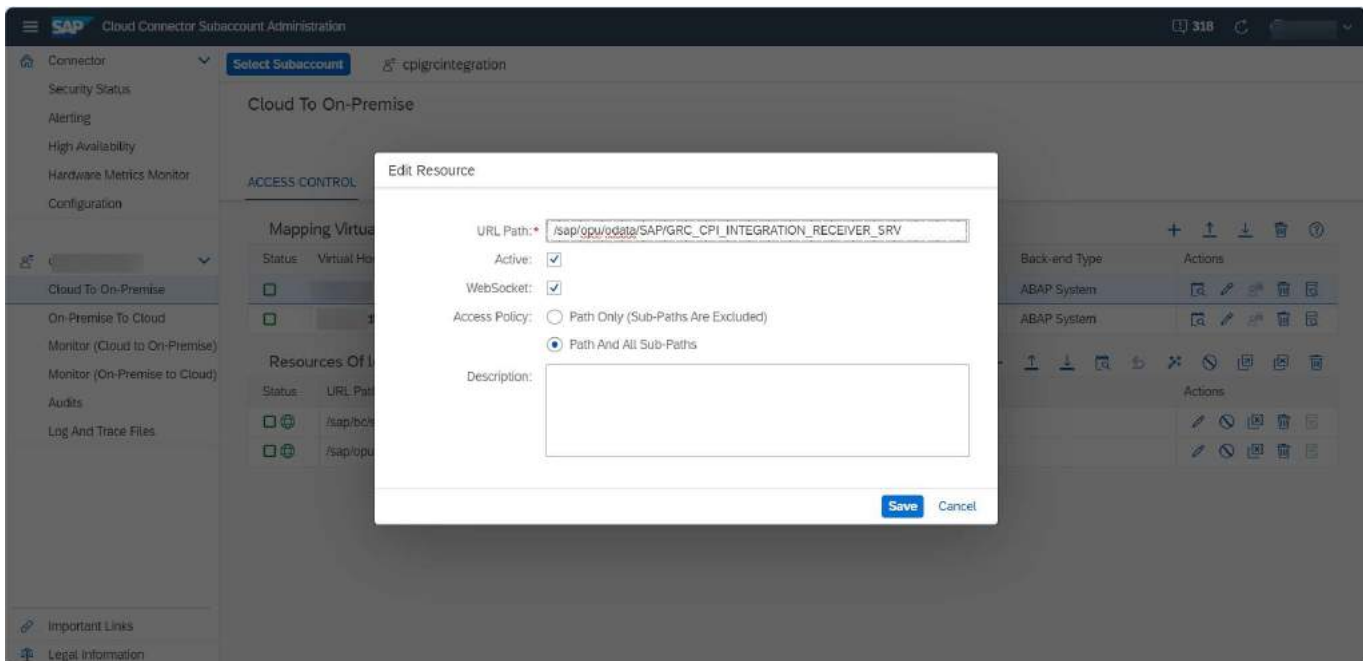


4. Create a new Virtual host with following details:



5. Navigate to GRC system and add resources . Please mention following details:

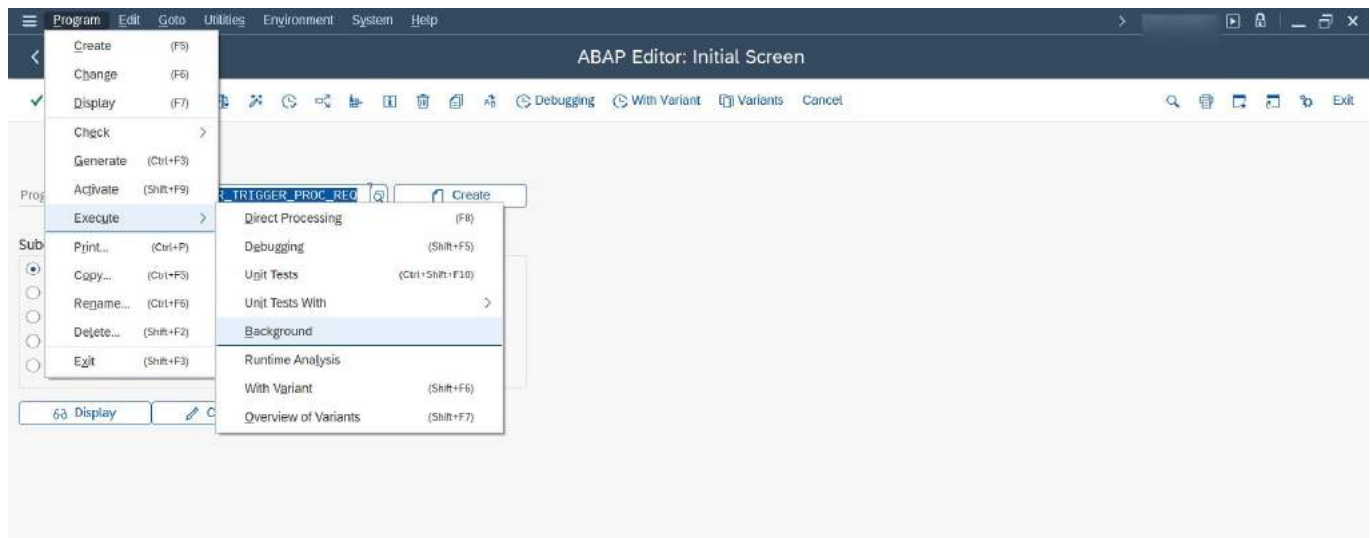
- URL Path : /sap/opu/odata
- Active checked
- Path and all sub path checked



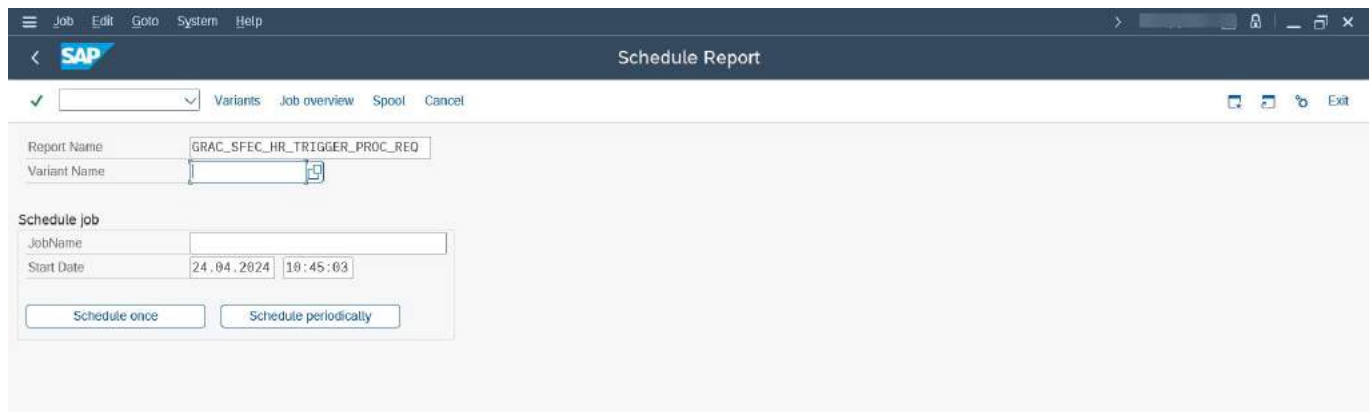
5.3.1.4 How to schedule new background job

For Iflow *SuccessFactors Employee Central to SAP GRC Access Control Integration for Employee Authorization_OData*, the HR Trigger access requests are not created automatically after scheduling CPI job. Schedule a background job after CPI job recurrence timing.

1. After successfully running the Iflow, please schedule a new background job for program 'GRAC_SFEC_HR_TRIGGER_PROC_REQ' in your GRC system.



2. Do not enter any value in notification parameter for variant.
3. Enter the variant and job name and schedule periodically.



3. The new background job will AUTOMATICALLY create all the SFEC HR Trigger request whose status in GRACSFECTRUSER is OPEN.

5.3.2 Configure and Deploy iFlow - SAP SFEC to SAP GRC AC Integration for Employee Authorization_PP

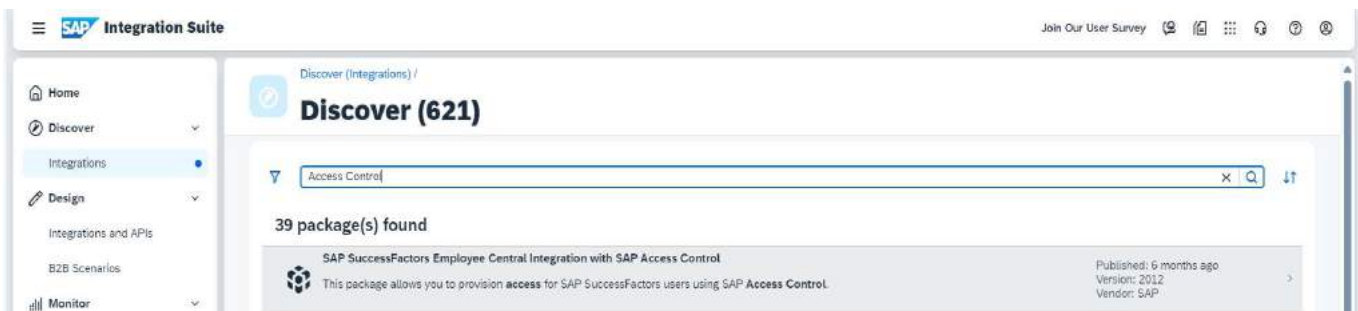
To configure and deploy the SAP Access Control integration, you must copy the delivered integration package to your workspace and modify it.

Prerequisites

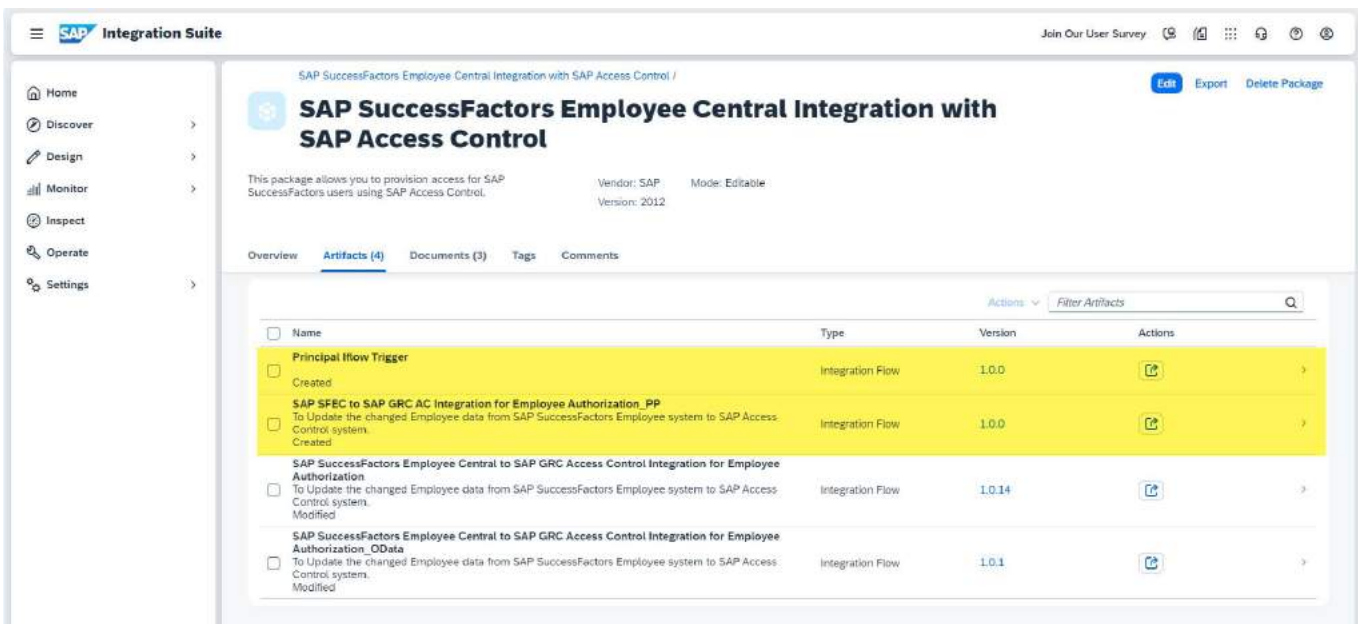
1. *SAP SFEC to SAP GRC AC Integration for Employee Authorization_PP* iFlow is introduced to support principal propagation and remove Basic Authentication from GRC receiver adaptor.

Process

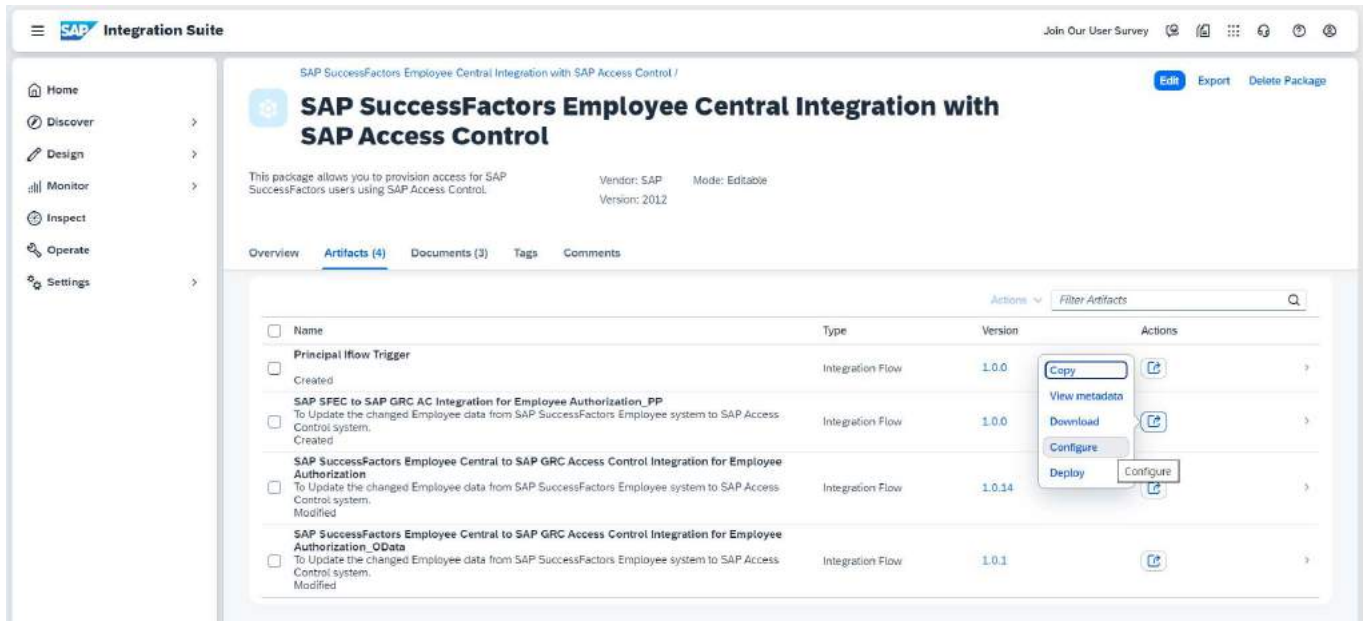
1. On SAP Cloud Integration, choose the *Discover* icon. Choose *SAP Access Control Integration with SAP SuccessFactors Employee Central*



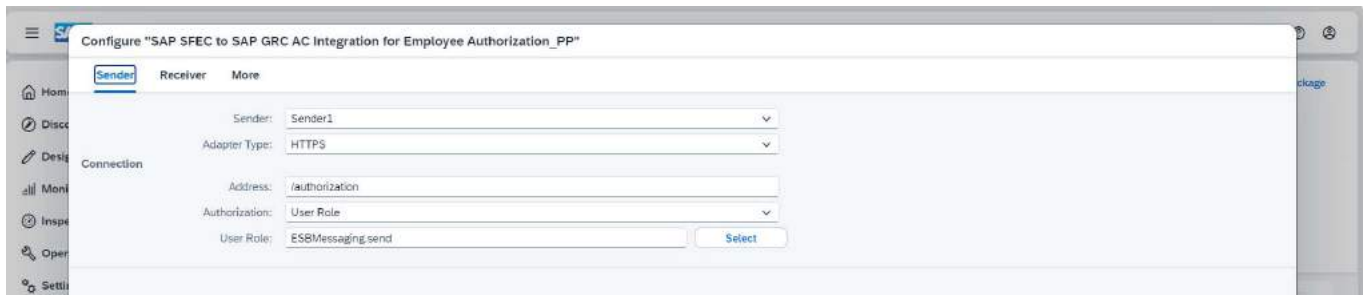
2. In the **Discover** tab, select the integration flow (*SAP SFEC to SAP GRC AC Integration for Employee Authorization_PP*) and click *Copy to Workspace*.



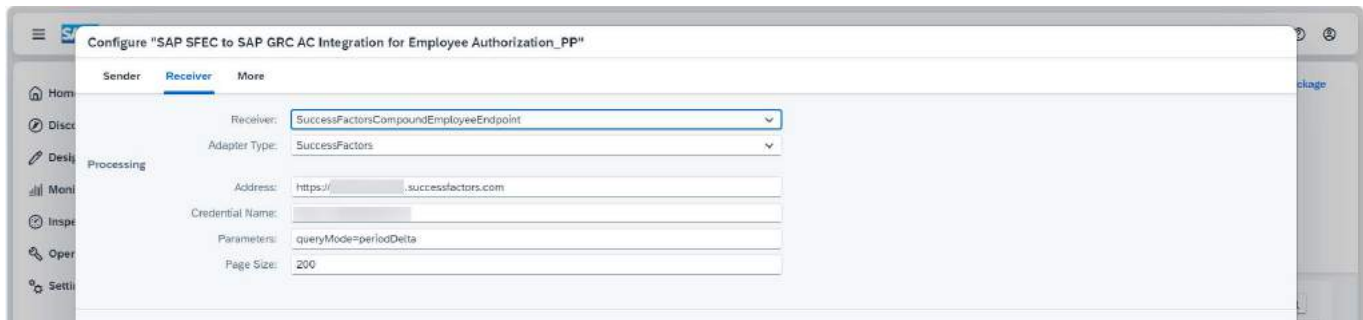
3. In the *Artifacts* tab, select the iFlow package, click the *Actions* icon, and select *Configure*.



4. Create a sender for Principal Propagation:
 - a. On the *Sender* tab, select the Sender1
 - b. Enter the *Adapter Type* as HTTPS.
 - c. Enter *Address* as "/authorization".
 - d. Enter *Authorization* as "User Role"
 - e. Enter User Role as "ESBMessaging.send"

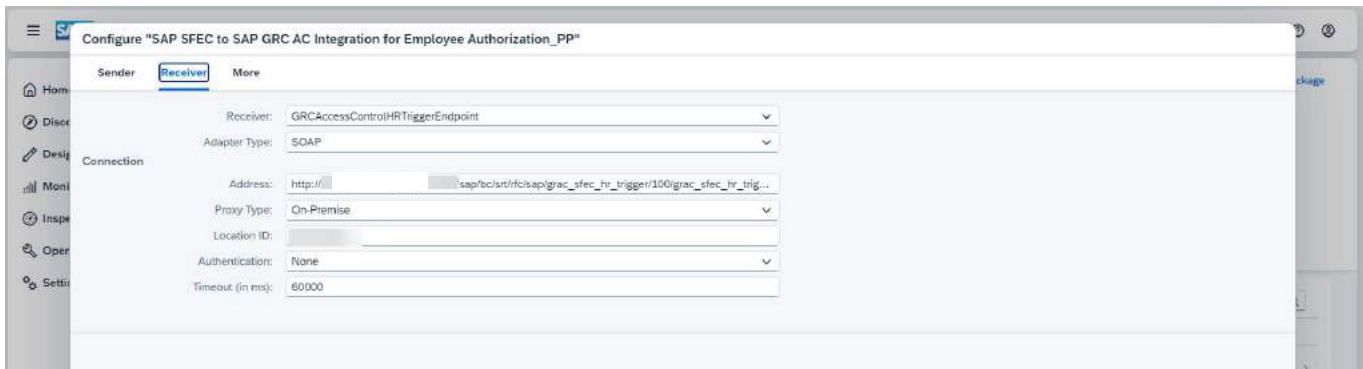


5. Create a receiver for SFEC:
 - a. On the *Receiver* tab, select the SAP SuccessFactors receiver from the dropdown.
 - b. Enter the address and credential name for the SAP SuccessFactors system.
 - c. Allow the authentication type to *Basic Authentication/ OAuth Authentication*.
(For OAuth Authentication please check section - 5.3.1.1)



6. Create a Receiver for SAP Access Control:

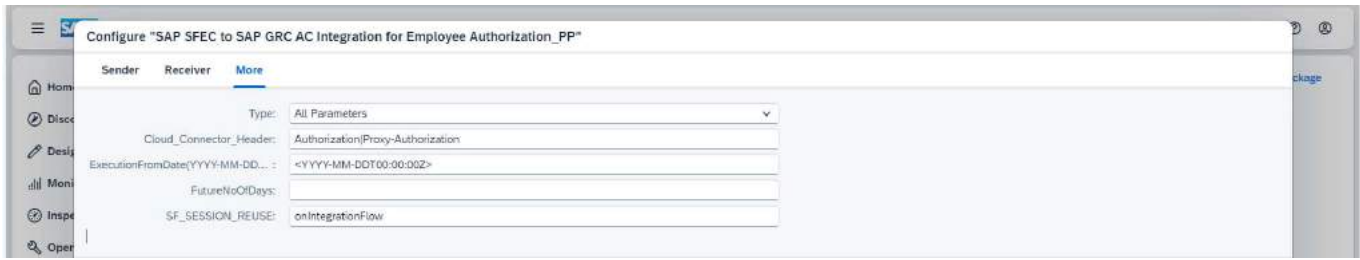
- a. On the *Receiver tab*, select the SAP Access Control receiver from the dropdown.
- b. Provide the address and credential name for the SAP Access Control receiver. The URL is built based on the *web-service calculated URL* you created in *Create a Binding for Web Services*. Append it with the hostname and port.
- c. Provide Proxy-Type as On-Premise and Location ID as location maintained in cloud connector
- d. Provide Authentication as None.
- e. Click on Save.



7. Configure the execution parameters for the initial data load and for subsequent recurring integration runs.

Initial Data Load Configuration

1. Choose the *Parameters* tab.
2. *Cloud Connector Header* should be maintained as
 - a. *Authorization|Proxy-Authorization (in case Principal Iflow Trigger has authentication as OAuth2 Client Credentials)*
 - b. *Blank (in case Principal Iflow Trigger has authentication as Basic Authentictaion)*
3. For the initial load, the first time you run the integration, provide the *ExecutionFromDate*. The system selects Employee Central records that were created or modified from this date forward.
4. *FutureNoOfDays*: The parameter controls how far into the future new hires can be processed. Enter the number of days beyond the today's date to consider for validity of employee records.



Example

The FutureNoOfDays is 20.

New Hire 1 has a start date of today (7/30/2016)

New Hire 2 has a start date of August 10 (8/10/2016)

New Hire 3 has a start date of September 15 (9/15/2016)

SAP Cloud Integration will process new hires that fall within the range of today's date + 20 days. Employees with start dates on or before August 19 (July 30 +20 days) will be processed. Employees with start dates after August 19 will not be processed. In our example, New Hires 1 and 2 will be processed. New Hire 3 will not be processed.

4. Choose the *Timer* tab to schedule the initial load job.
5. Give the *Timer* (job) a descriptive name such as "InitialSFdataload"
6. Check *Run Once* for the initial data load.
7. Click *Save*.

When you are ready to execute the initial load, click *Deploy*.



Recurring Integration Configuration

To set up a recurring job:

1. Choose the *Parameters* tab.
2. Leave the *ExecutionFromDate* empty.
3. *FutureNoOfDays*: Enter the number of days beyond the current run date for which you want to include records
4. Click *Save*.
5. Choose the *Timer* tab to schedule the recurring job, and select a timer from the dropdown menu.
6. Click **Schedule to Recur**.
7. Select the recurring interval, for example, *Daily* or *weekly*.
8. Select the *On Time* radio button to fill in the time for your recurring data transfer.

Warning

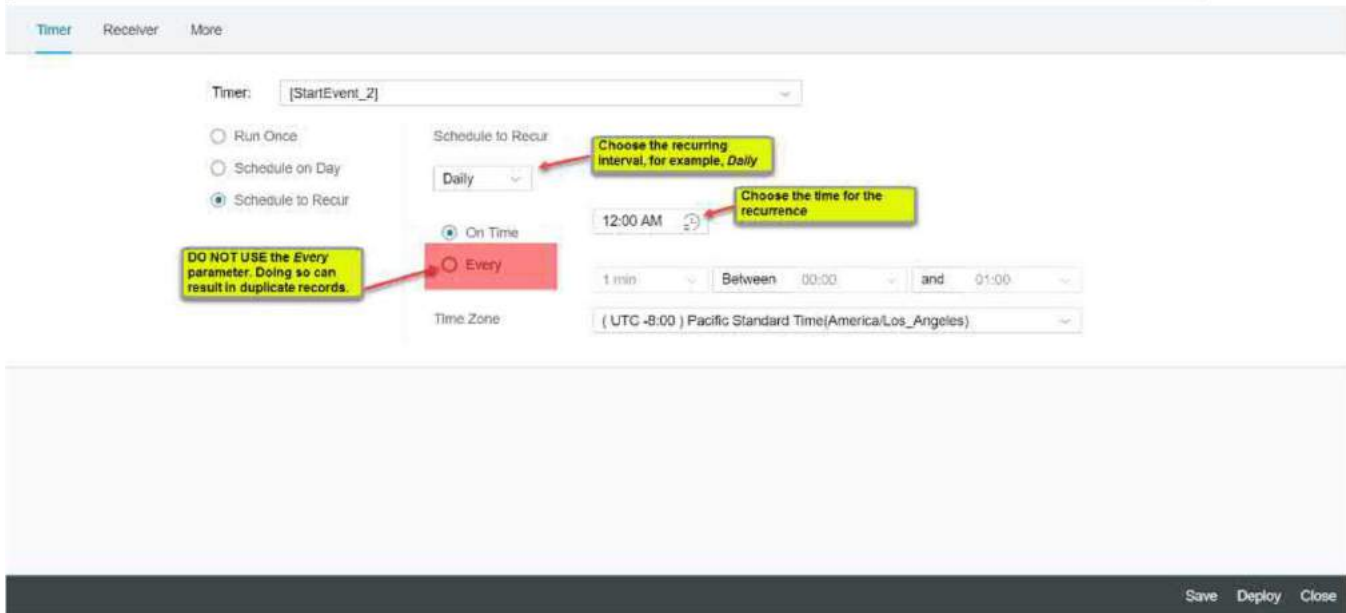
Do not select Every radio button! A recurring job should not be scheduled to run more than once in the same day. Doing so can result in duplicate records.

9. Click *Save*.

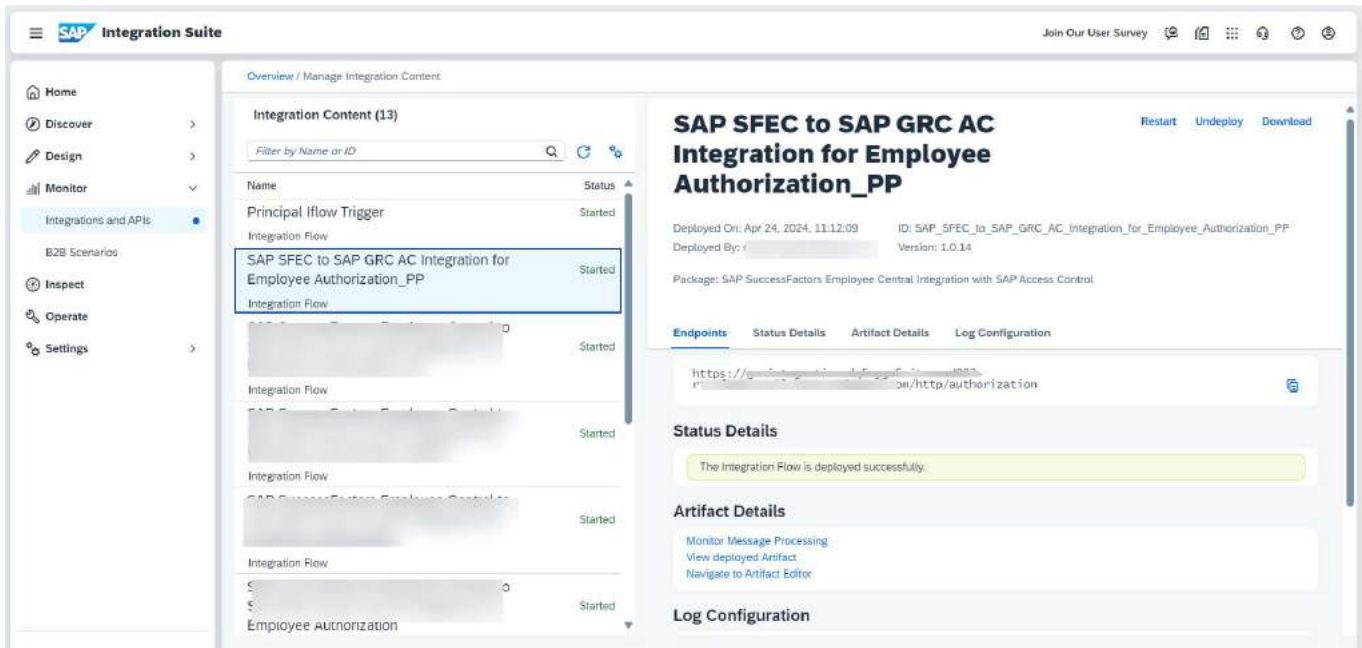
When you are ready to execute the job series, click *Deploy*.

SAP SuccessFactors Employee Central to SAP Access Control Integration using SAP Cloud Integration

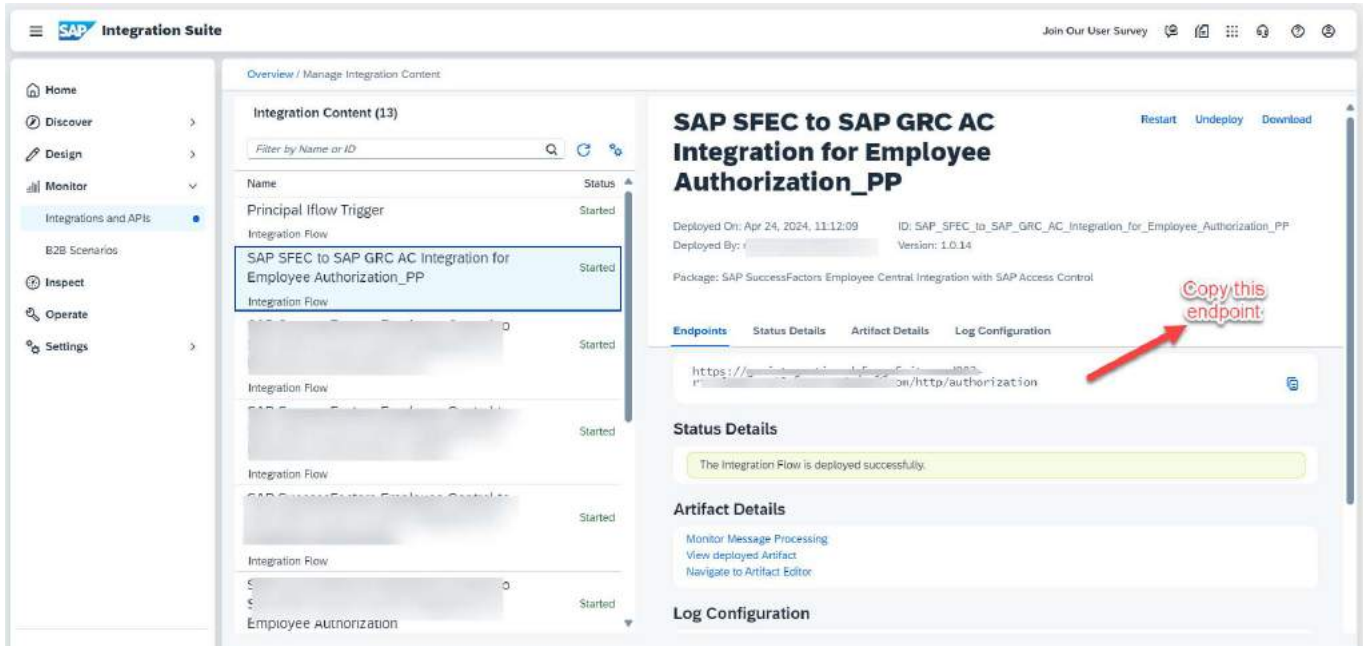
C U S T O M E R



10. Once deployed, navigate to Monitor tab then to Overview and Manage Integration Content



11. Go to Endpoints tab and copy the endpoint.



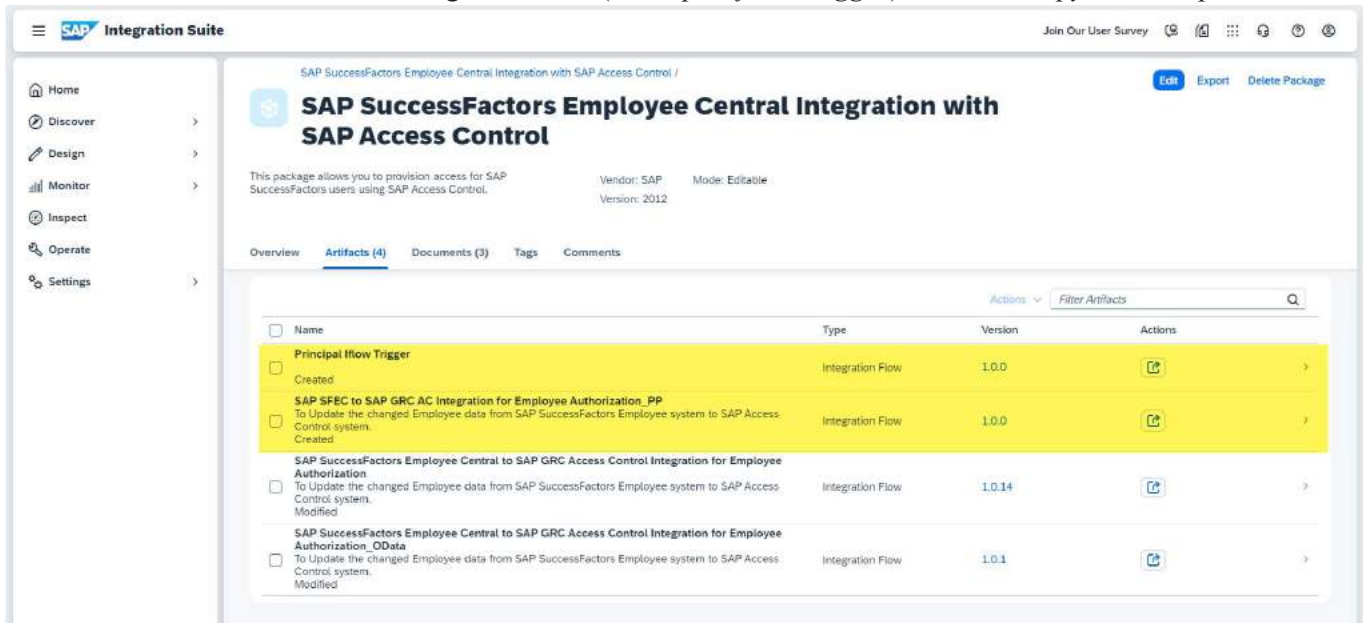
5.3.2.1 Configuring Principal Iflow Trigger

Prerequisites

1. SAP SFEC to SAP GRC AC Integration for Employee Authorization_PP Iflow is deployed.

Process

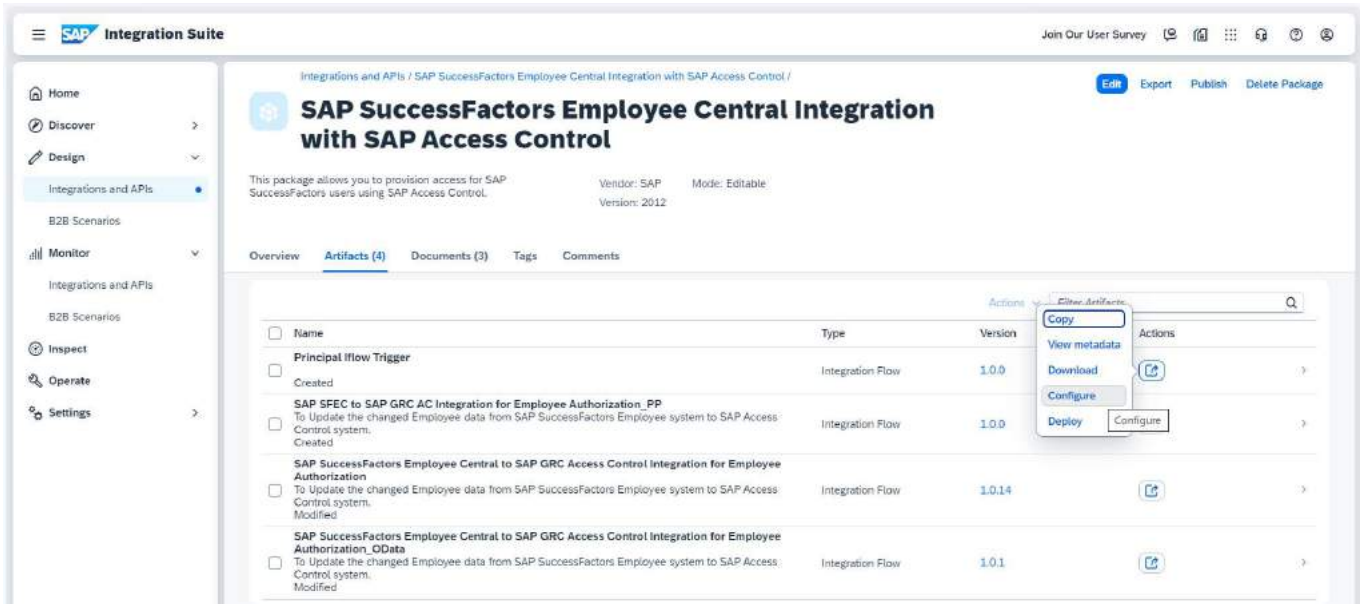
1. On SAP Cloud Integration, choose the *Discover* icon. Choose *SAP Access Control Integration with SAP SuccessFactors Employee Central*
2. In the **Discover** tab, select the integration flow (*Principal Iflow Trigger*) and click *Copy to Workspace*.



SAP SuccessFactors Employee Central to SAP Access Control Integration using SAP Cloud Integration

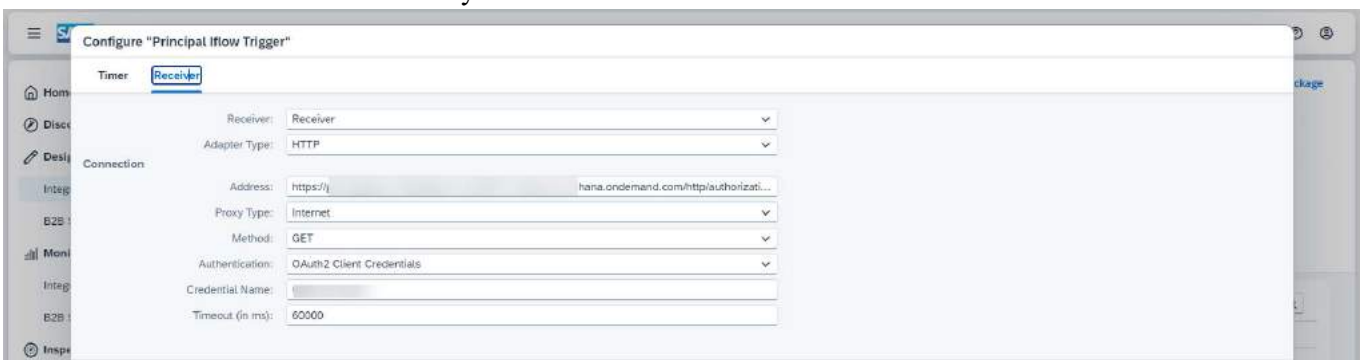
C U S T O M E R

3. In the *Artifacts* tab, select the iFlow package, click the *Actions* icon, and select *Configure*.



4. Create a sender for Principal Propagation:

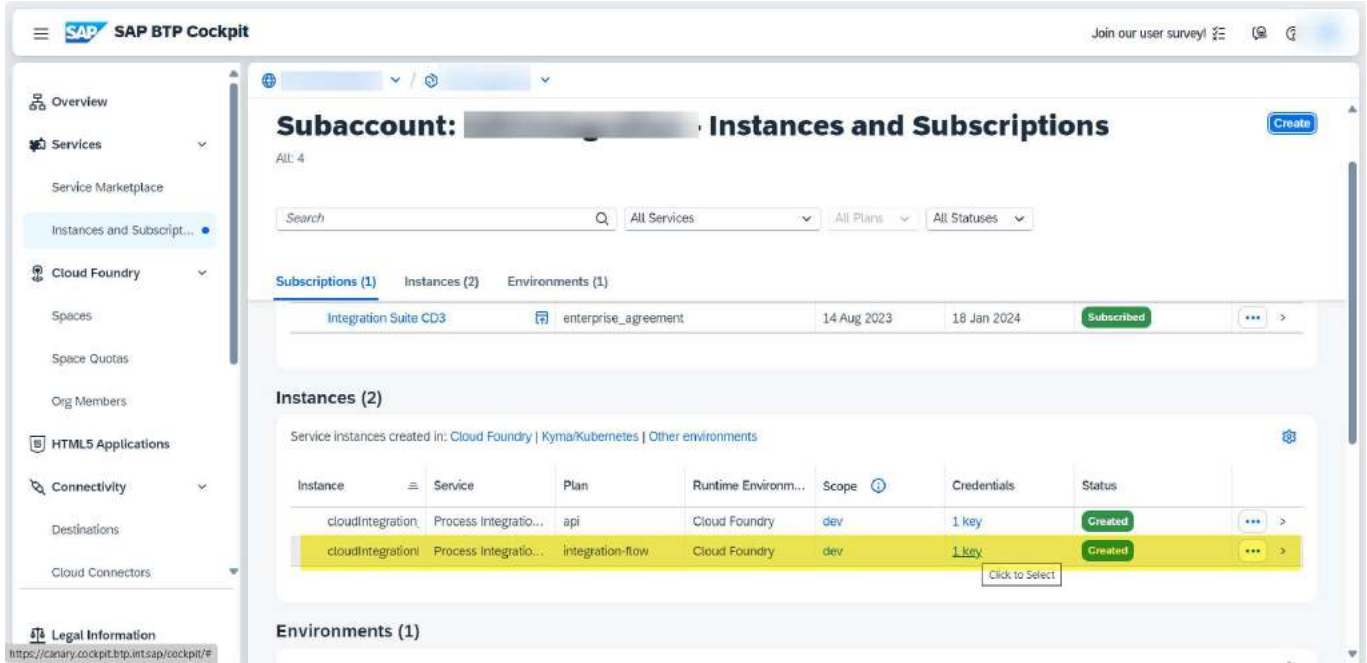
- On the *Receiver* tab, select the Receiver
- Enter the *Adapter Type* as HTTP.
- Enter *Address* as endpoint of deployed iflow *SAP SFEC to SAP GRC AC Integration for Employee Authorization_PP*.
- Enter *Proxy Type* as Internet.
- Enter *Method* as GET.
- Enter *Authorization* as:
 - Basic Authentication (use valid IDP user credentials to trigger *SAP SFEC to SAP GRC AC Integration for Employee Authorization_PP* iflow)
 - OAuth2 Client Credentials (configure based on section 5.3.2.1)
- Enter *Credential Name* from security material.



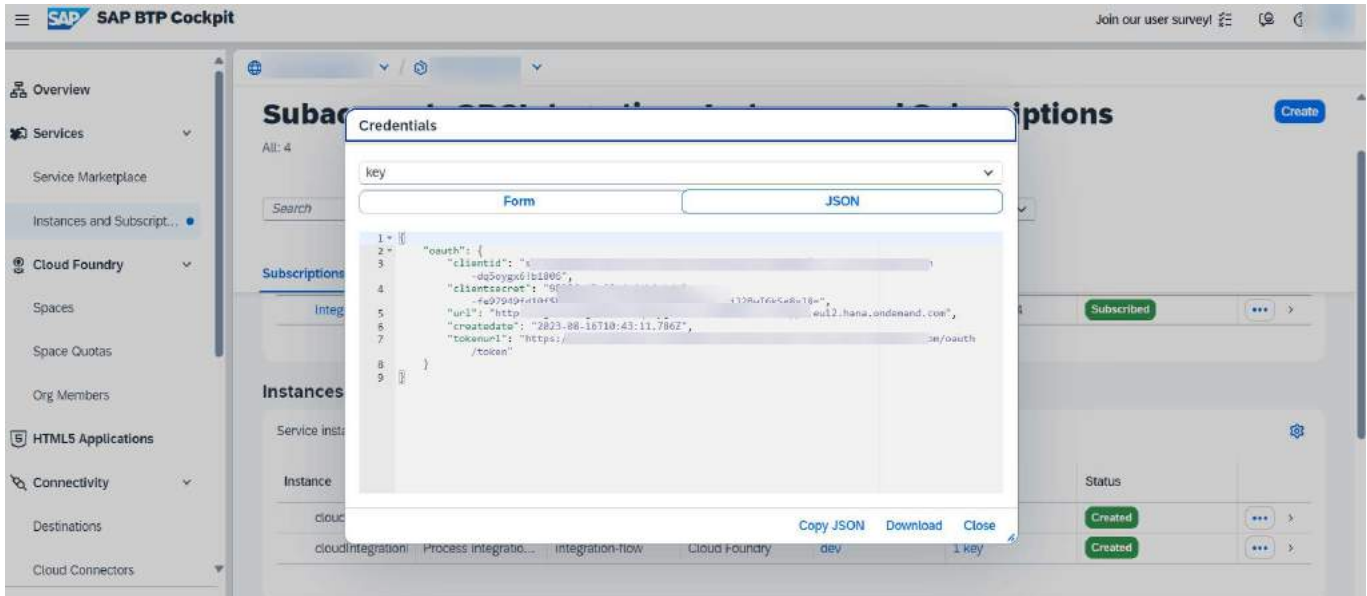
5.3.2.2 Configuring OAuth2 Client Credentials in CPI Security Material

Navigate to SAP BTP Subaccount and get the instance details from below:

1. Go to BTP Subaccount
2. Navigate to Instances & Subscription



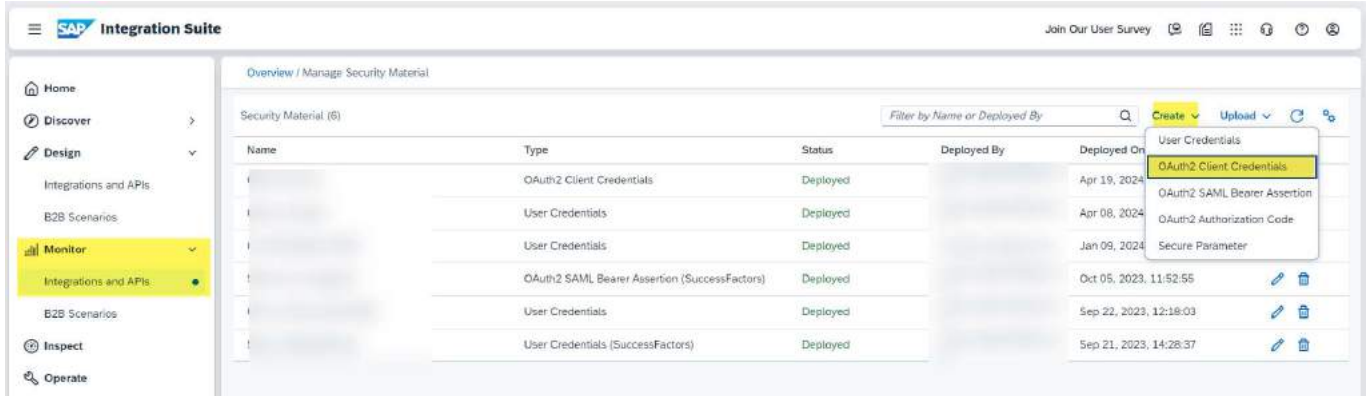
3. Click on Credential Key of the Instance with Plan as Integration Flow.
4. Copy all the fields



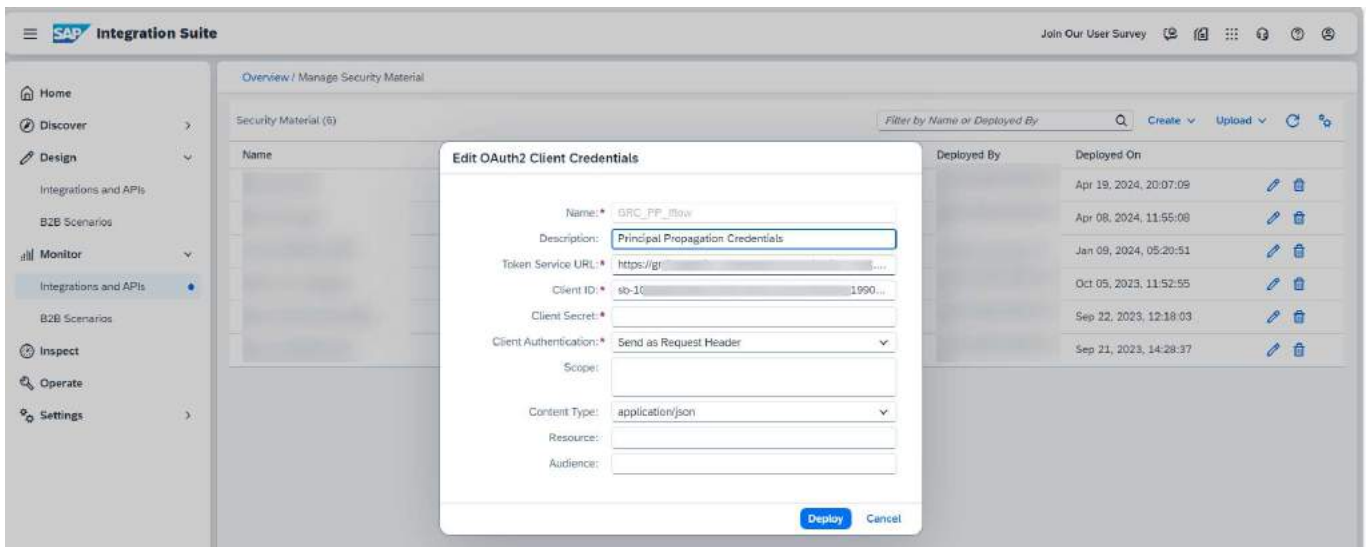
SAP SuccessFactors Employee Central to SAP Access Control Integration using SAP Cloud Integration

C U S T O M E R

- Navigate to CPI -> Monitor -> Security Materials
 Create a new OAuth2 Client Credential for Principal Propagation Iflow
1. Go to CPI -> Security material
 2. Create OAuth2 Client Credentials



3. Enter the following values:
 Enter Name - <Credential_Name>
 Token URL - <BTPInstance_Token_URL>
 Client ID - <BTPInstance_Client_ID>
 Client Secret - <BTPInstance_Client_Secret>
 Client Authentication - Send as Request Header
 Content Type - application/json

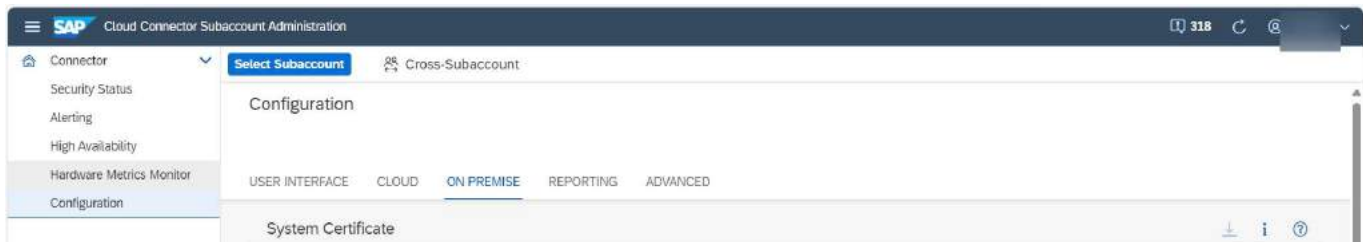


5.3.2.3 Configuring Cloud Connector and Backend on-Premises GRC system

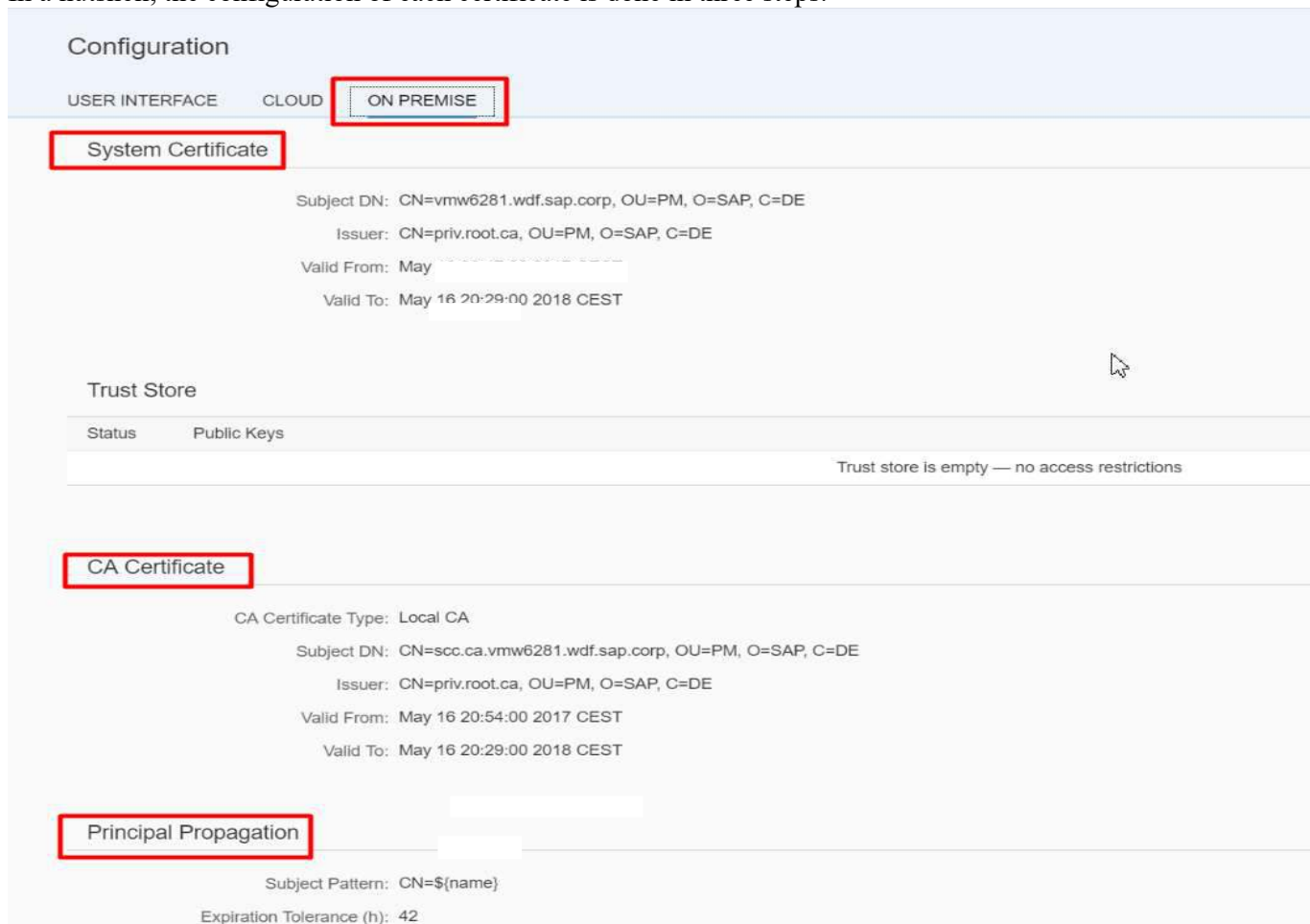
Configure cloud connector as mentioned in Section 5.1

Configuring the certificates on the SAP Cloud Connector

The configuration in the cloud connector relevant to Principal Propagation relies on three different configuration elements: System Certificate, CA Certificate and principal propagation.



In a nutshell, the configuration of each certificate is done in three steps.



Steps to follow to configure on-Premise certificates:

1. Generate a certificate signing request.
2. Use the PKI to sign the certificate.
3. Upload the signed certificate in the appropriate place of the Cloud Connector.

UI Certificate

In the context of the SAP Cloud Connector (SCC), create the UI Certificate. This certificate should match the full qualified domain name of the server hosting SCC. (CN, OU, O, C)

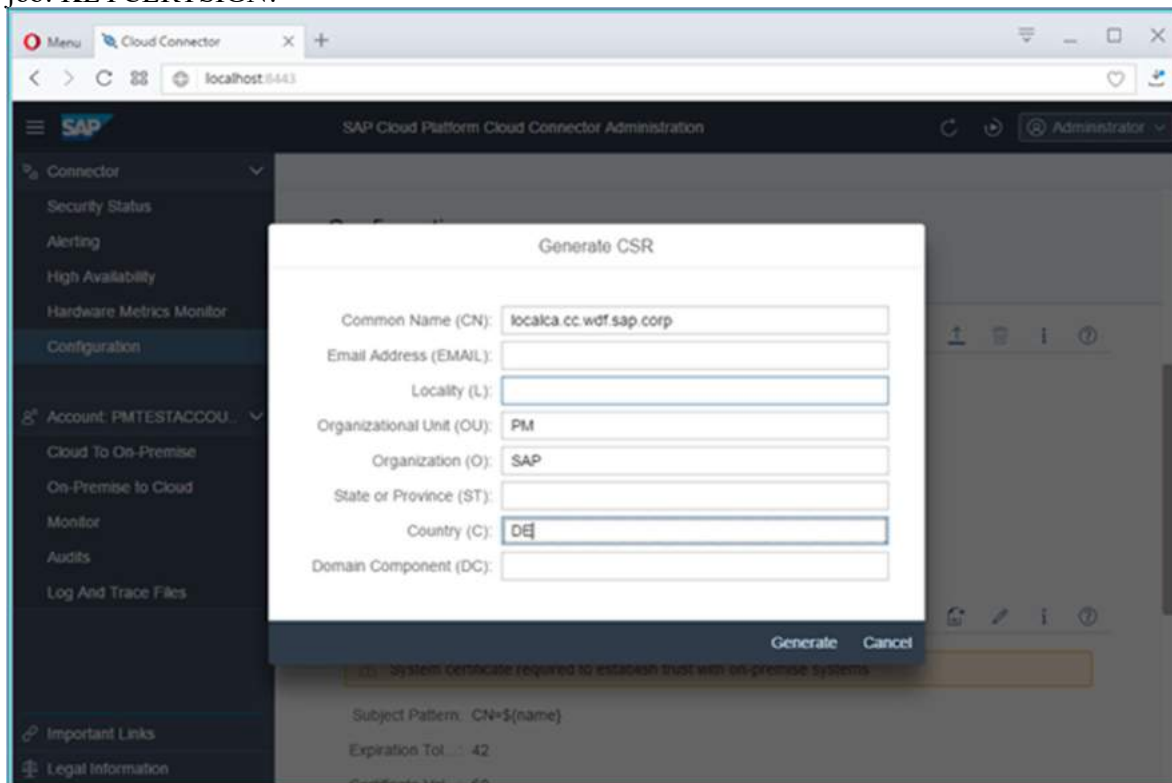
Once the certificate is generated signed by CSR / self-signed. Then upload the signed CSR which is now called certificate and stored in a DER format.

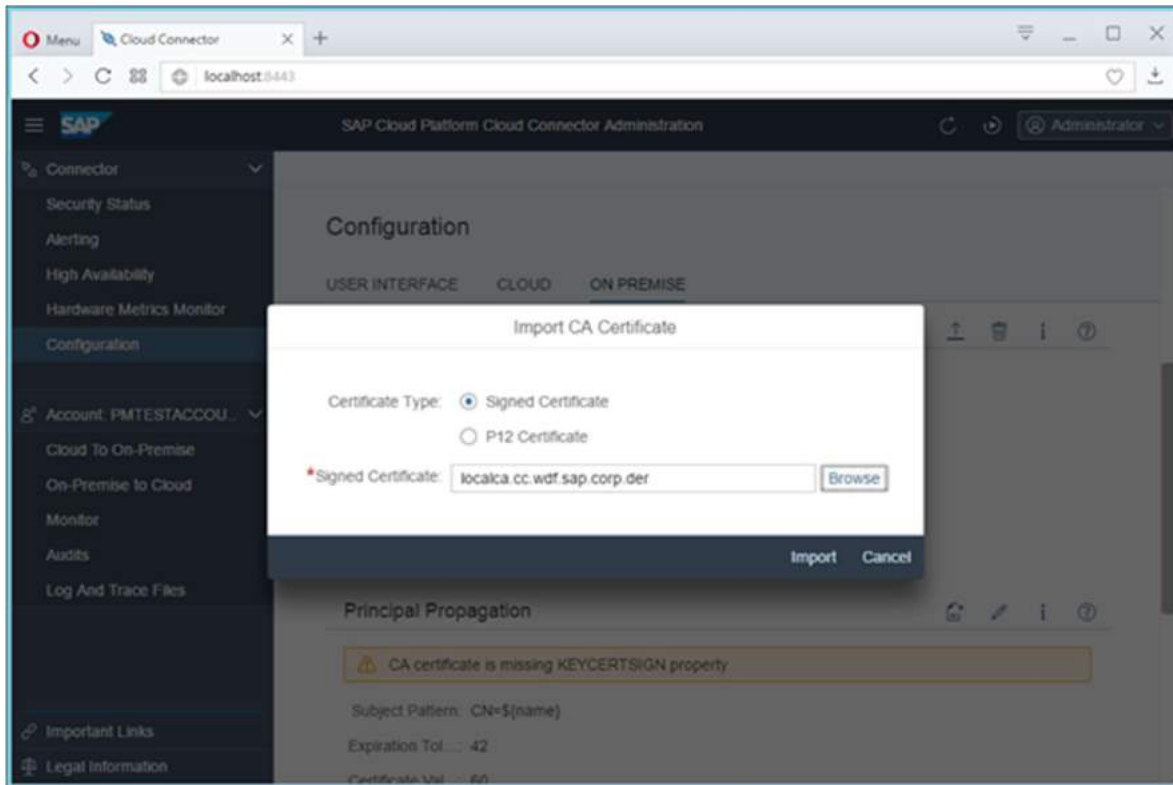
System certificate

Once the UI Certificate configured, the system certificate can reuse it.

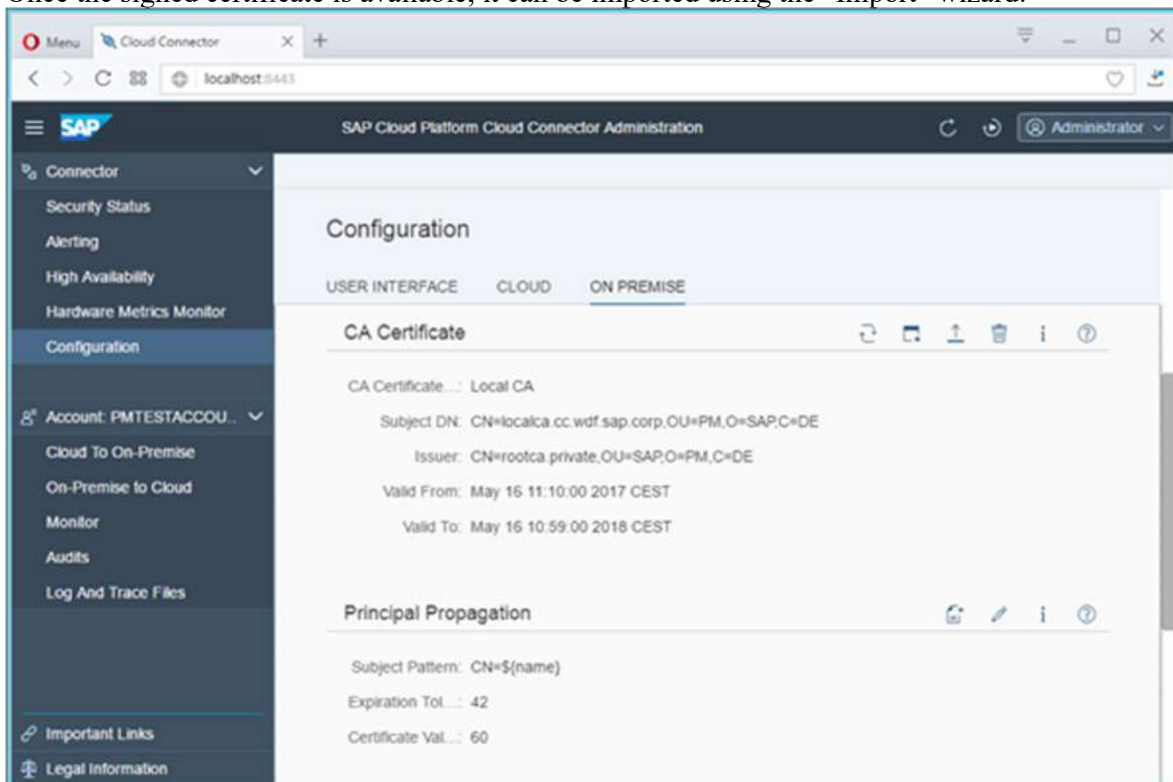
CA certificate

This certificate will be used to sign the short-lived certificate that will be passed to the backend to authenticate the logged in user. The important detail is that this specific certificate needs a very specific property to be able to do its job: KEYCERTSIGN!





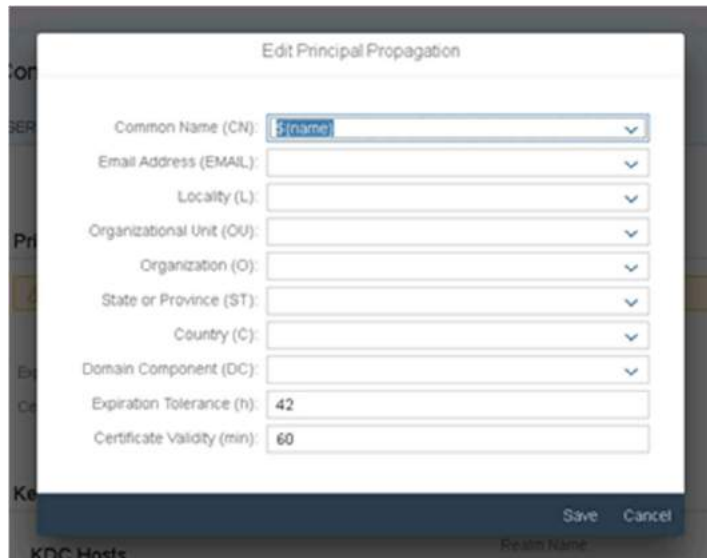
Once the signed certificate is available, it can be imported using the “Import” wizard.



Principal Propagation

Under Principal Propagation generate a sample certificate (the first icon in the row). One of the roles of the SCC in the context of Principal propagation is to generate short-lived certificates based on some identity information retrieved from the logged in user.

We will use the generated sample certificate later in our configuration to build our rule in the CERTRULE transaction.

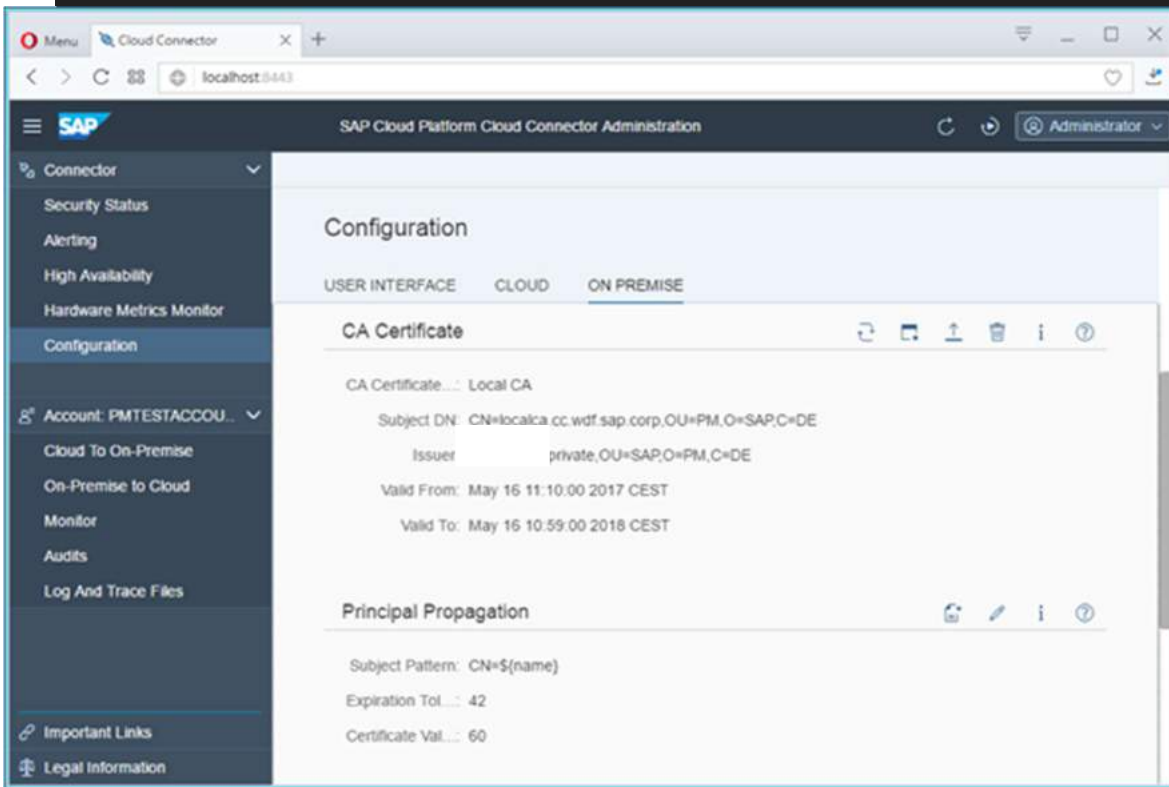


The screenshot shows a dialog box titled "Edit Principal Propagation". It contains the following fields:

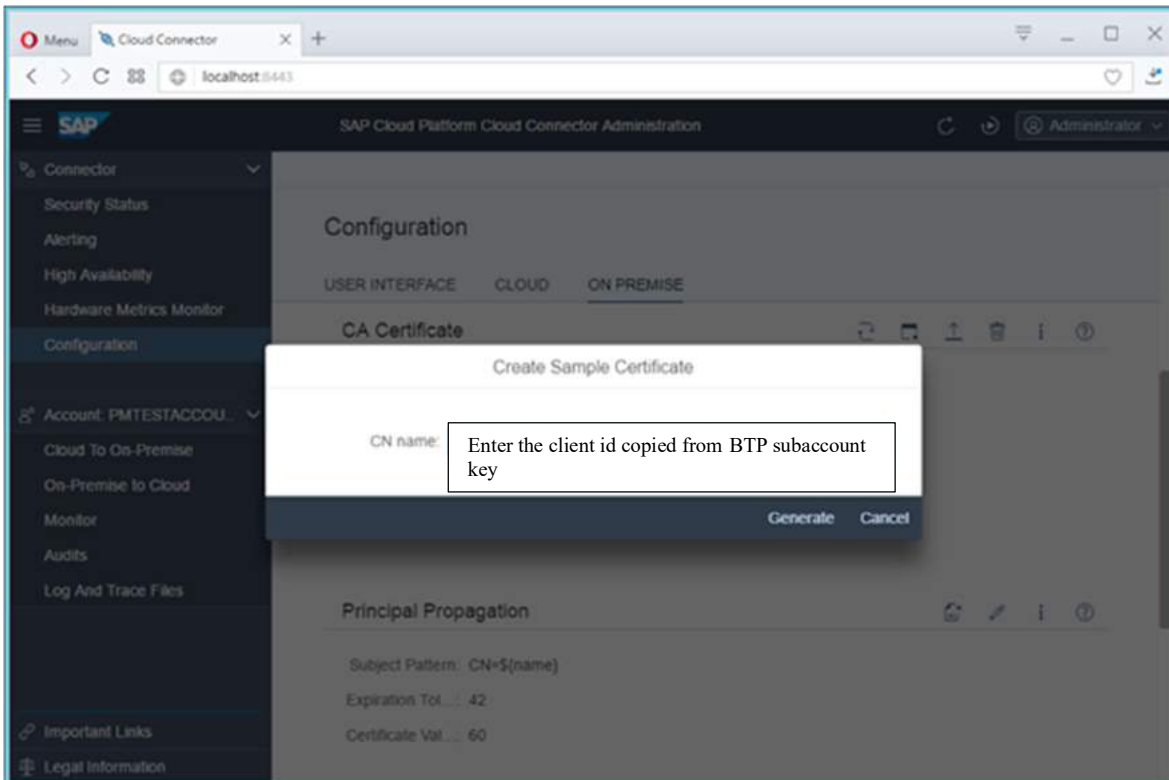
- Common Name (CN):
- Email Address (EMAIL):
- Locality (L):
- Organizational Unit (OU):
- Organization (O):
- State or Province (ST):
- Country (C):
- Domain Component (DC):
- Expiration Tolerance (h):
- Certificate Validity (min):

At the bottom right, there are "Save" and "Cancel" buttons.

This screen describes the pieces of information that will be used to build the short-lived certificates. In the screenshot above the name is the only info that is passed.



Press Save to store the information and you should see the finished Principal Propagation configuration as shown above.



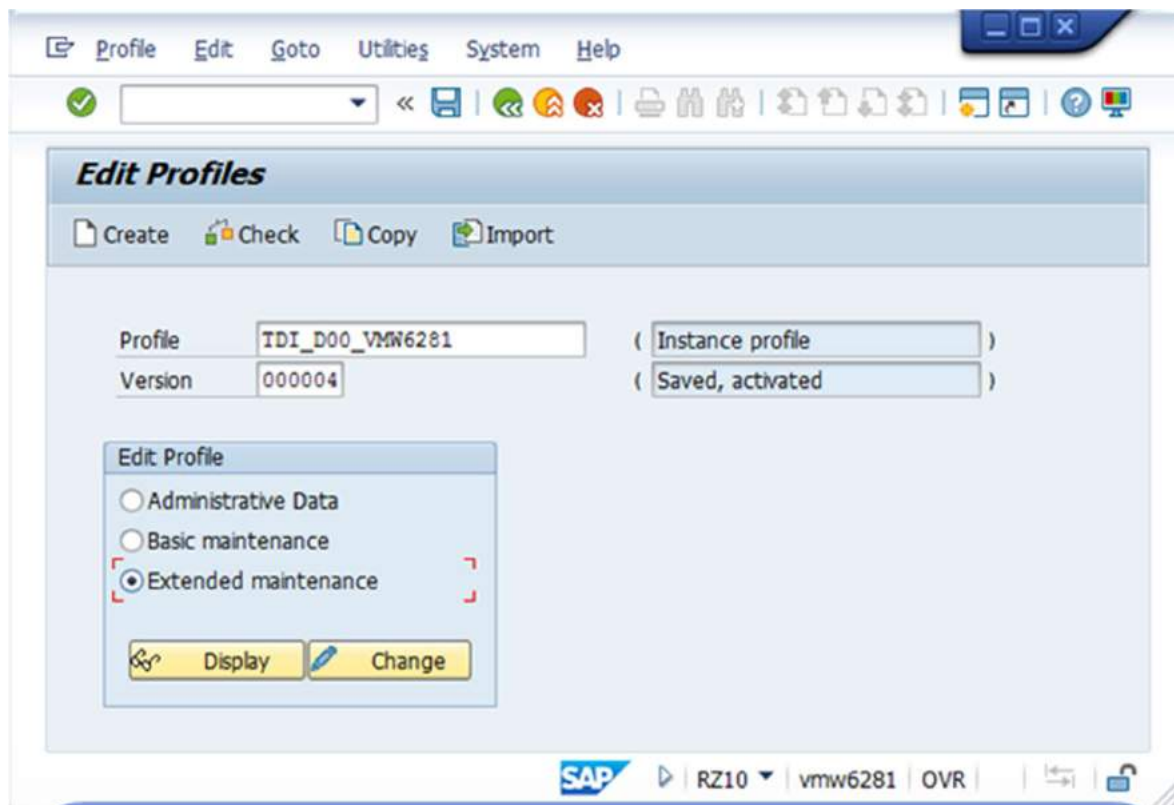
Now create dummy certificate that will be used as a reference for all the certificates that will be issued by the SCC.

5.3.2.4 Configure the SAP Gateway

On the SAP backend, only few transactions will be required: RZ10, STRUST, CERTRULE (or EXTID_DN), SICF and SMICM.

Enabling Certificate Based Login

In order to have the Gateway request a certificate rather than prompt for a username and a password, certain profile parameters need to be maintained. This configuration is done using the transaction RZ10.



Choose the instance profile (could also be the DEFAULT profile) and mark the Extended maintenance radio button and then press the Change button.

Profile Parameter Goto System Help

Maintain Profile 'TDI_D00_VMW6281' Version '000004'

Copy Parameter Parameter Parameter

16.05.2017 Active parameters 11:29:10

Parameter Name	Parameter value
SAPSYSTEMNAME	TDI
SAPGLOBALHOST	vmw6281
SAPSYSTEM	00
INSTANCE_NAME	D00
DIR_CT_RUN	\$(DIR_EXE_ROOT)\\$(OS_UNICODE)\NTAMD64
DIR_EXECUTABLE	\$(DIR_INSTANCE)\exe
DIR_PROFILE	\\vmw6281\sapmnt\TDI\SYS\profile
_PF	\$(DIR_PROFILE)\TDI_D00_vmw6281
SETENV_00	PATH=\$(DIR_EXECUTABLE);%PATH%
Start_Program_00	immediate \$(DIR_CT_RUN)\\$(DIR_SEP)sapce\$(FI_EXE) pf=\$(DIR_PROFILE)\\$(DIR
_CPARGO	list=\$(DIR_CT_RUN)\sapcrypto.lst
Start_Program_03	immediate \$(DIR_CT_RUN)\sapce\$(FI_EXE) pf=\$(PF) \$(CPARGO)
Start_Program_04	immediate \$(DIR_CT_RUN)\\$(DIR_SEP)strdba.cmd TDI
rdisp/wp_no_dia	10
rdisp/wp_no_btc	3
rdisp/wp_no_vb	1
rdisp/wp_no_vb2	1
rdisp/wp_no_spo	1

Pressing the new parameter button will allow you to insert a new parameter into the profile by presenting the screen below.

Parameter Edit Goto System Help

Maintain Profile 'TDI_D00_VMW6281' Version '000004'

Copy Line Line PARAM+ PARAM-

Parameter name: Status: Seq. no.:

Parameter val.:

Unsubstituted standard value:

Substituted standard value:

Comment:

Maintain the 4 profile parameters listed below.

login/certificate_mapping_rulebased	This parameter allows the GW to map, based on a rules defined in CERTRULE, the identity contained in an identity certificate received during the authentication with an internal user. If set to 0, this mapping need to be maintained manually through EXTID_DN.
icm/HTTPS/verify_client	This parameter instructs the GW to request a certificate from clients trying to access any resource in the GW. It is a key parameter to configure certificate base authentication on the GW.
icm/HTTPS/trust_client_with_issuer	Value corresponding to the Issuer of the SAP Cloud Connector System Certificate This parameter contributes to the establishment of a trust between the SAP Cloud Connector and the SAP Gateway System.
icm/HTTPS/trust_client_with_subject	Value corresponding to the subject of the SAP Cloud Connector System Certificate This parameter contributes to the establishment of a trust between the SAP Cloud Connector and the SAP Gateway System.

Make sure you press the Copy button for each parameter you create. The result is a profile that looks like the screenshot below.

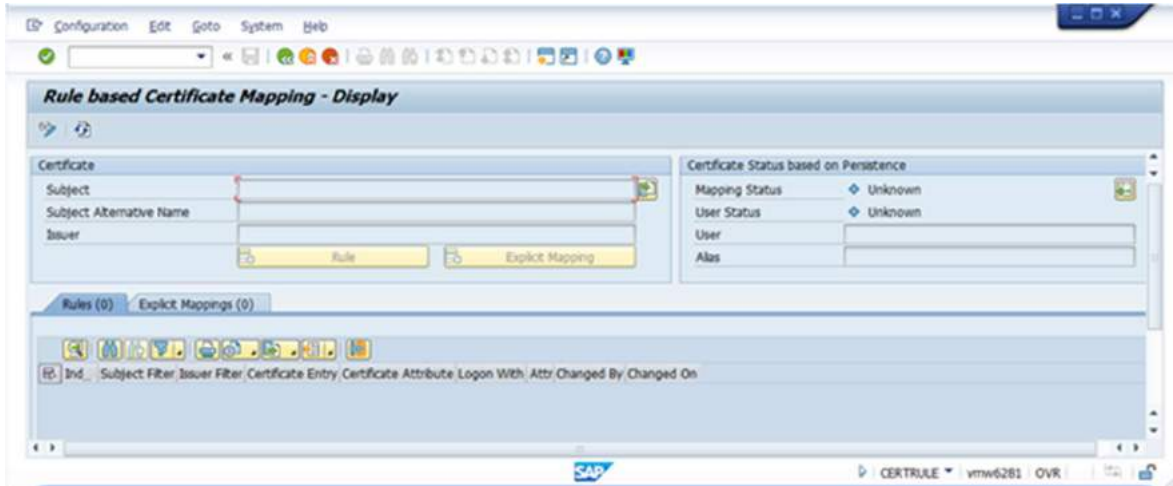
The screenshot shows the 'Maintain Profile' interface for 'TDI_D00_VMW6281' Version '000012'. The interface includes a toolbar with 'Copy', 'Parameter', and other icons. Below the toolbar, a table lists active parameters. The 'icm/HTTPS/trust_client_with_subject' parameter is highlighted in yellow, with its value 'CN=* OU=PM, O=SAP, C=DE' visible. Other parameters listed include SPSYSTEMNAME (TDI), SAPGLOBALHOST, SAPSYSTEM (00), INSTANCE_NAME (D00), DIR_CT_RUN, DIR_EXECUTABLE, DIR_PROFILE, and _PF.

Parameter Name	Parameter value
login/certificate_mapping_rulebased	
icm/HTTPS/verify_client	
icm/HTTPS/trust_client_with_subject	CN=* OU=PM, O=SAP, C=DE
icm/HTTPS/trust_client_with_issuer	
SAPSYSTEMNAME	TDI
SAPGLOBALHOST	
SAPSYSTEM	00
INSTANCE_NAME	D00
DIR_CT_RUN	\$(DIR_EXE_ROOT)\\$(OS_UNICODE)\NTAMD64
DIR_EXECUTABLE	\$(DIR_INSTANCE)\exe
DIR_PROFILE	\\vmw6281\sapmnt\TDI\SYS\profile
_PF	\$(DIR_PROFILE)\TDI_D00_vmw6281

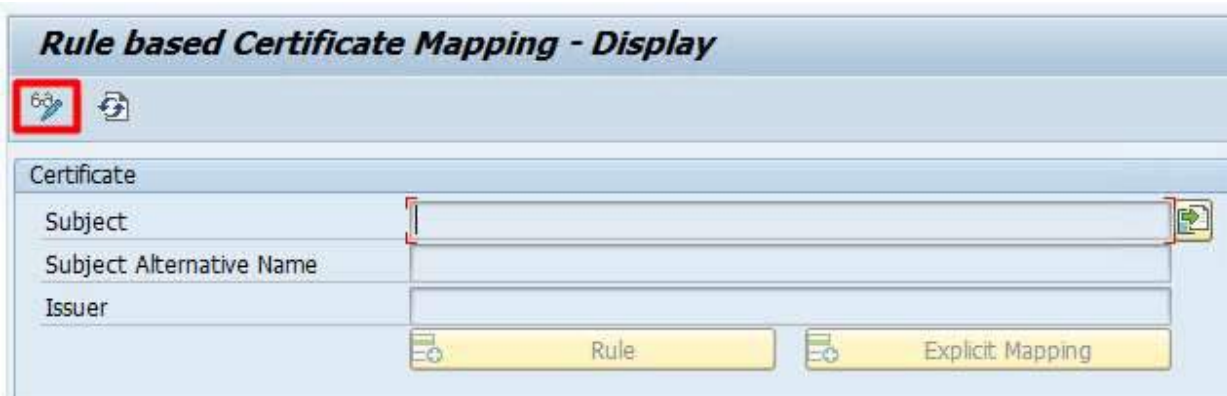
NOTE : What if a trust had to be configured with more than one system? The issuer and subject parameter we have just mentioned can only reference a single system.
In the SAP note 2052899, SAP introduce a new parameter that can be included in the profile multiple times and that replaces the actual two parameters: icm/trusted_reverse_proxy_0.

Now that the system requests a certificate as its primary login mechanism, we need to complement this configuration by configuring a rule that helps identify the individual user being authenticated.

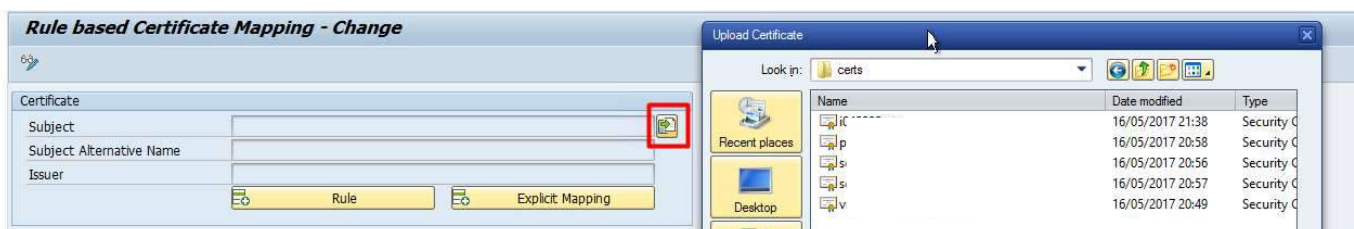
This is achieved using the transaction CERTRULE.



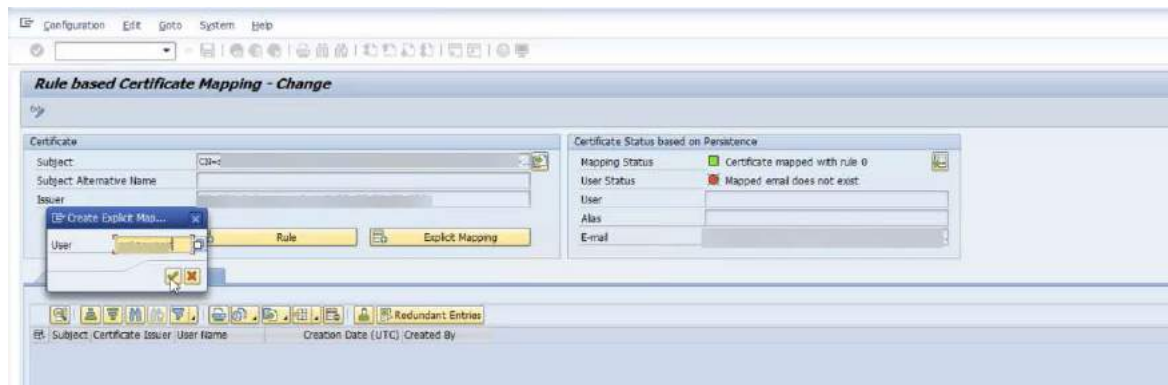
If the buttons are transparent as shown above, you will have to enter change mode by pressing the “glasses&pencil” icon.



Press the “Import Certificate” button to choose your template certificate. Here is where we will use the sample certificate generated in the Cloud Connector’s Principal propagation tab.



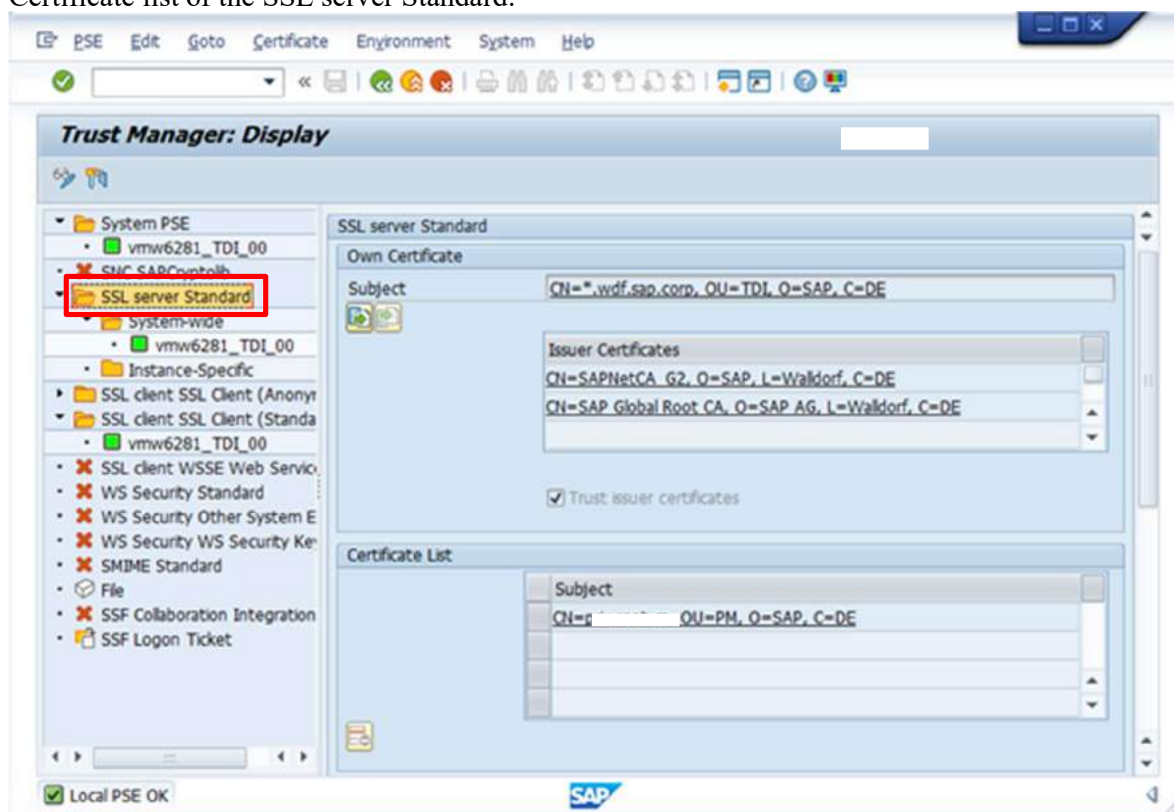
Once you have chosen the certificate to import, press the Explicit Mapping button to create an explicit mapping. Do not worry about the traffic lights in the right-hand pane. They will turn green when you save the rule, if the user exists.



Create a Dialog type user in SU01 - <USER>. Click on Explicit Mapping - and enter user as <USER>. Press the Save icon on the top ribbon to save the rule. Notice that the traffic lights are now green.

Configuring the backend for Principal Propagation

In transaction STRUST, the issuer of the certificate we used in the previous section needs to be added to the Certificate list of the SSL server Standard.

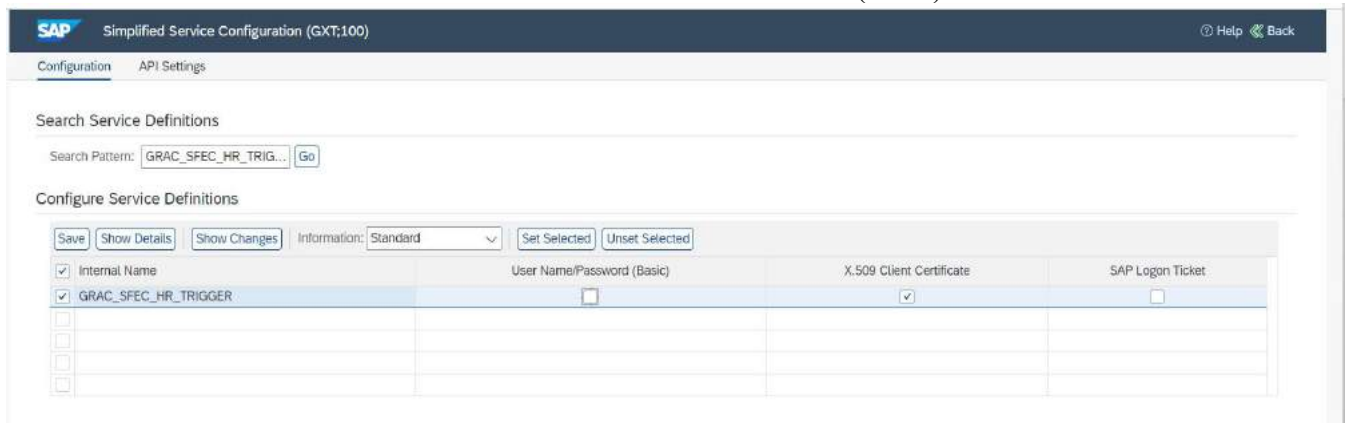


Configuration of SOAMANAGER

This configuration is required only in case of OAuth 2.0 Client Credentials authentication in *Principal Iflow Trigger*.

Navigate to transaction SOAMANAGER, then to Simplified Service Configuration.
Search for object GRAC_SFEC_HR_TRIGGER.

Select the X.509 Client Certificate and uncheck User Name/ Password (Basic)



The screenshot shows the SAP Simplified Service Configuration (GXT:100) interface. The search pattern is GRAC_SFEC_HR_TRIGGER. The configuration table is as follows:

Internal Name	User Name/Password (Basic)	X.509 Client Certificate	SAP Logon Ticket
<input checked="" type="checkbox"/> GRAC_SFEC_HR_TRIGGER	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

5.4 How to get the SAP Cloud Integration Client Certificate

In the SAP Cloud Integration provisioning email, follow the link under *Certificate Information*. In the resulting screen, choose *X509 Certificate* with option *Binary CER*. Download it to your local machine.

5.5 View and Extend the Deployed iFlows using SAP Eclipse (Optional)

This step is optional and only required if you want to extend the standard iFlows. For example, if you want to add content and field mapping beyond what is delivered.

Prerequisites

1. Install the SAP Cloud Integration Eclipse environment. For more information, see <https://tools.hana.ondemand.com/#hc>.
2. Maintain the SAP Cloud Integration Operation server details at *Windows* → *Preferences* → *SAP Cloud Integration* → *Operation server* (see provisioning email for details).
3. Configure and deploy prepackaged content using SAP Cloud Integration web UI. For more information, see the section *Configure and Deploy iFlows using SAP Cloud Integration Web UI*.

5.5.1 Download the iFlow Projects on Your Desktop

1. Go to Integration Designer perspective.
2. In the *Project Explorer*, on the Eclipse toolbar, navigate to *File* → *Import*.
3. In the Import wizard, select the option Integration Content Archive und in the former SAP HANA Cloud Integration and click Next.
4. In the next screen under *Import*, select *Tenant Management Node* in the *Form location* dropdown and select your tenant in the *Tenant ID* dropdown box.
5. From the Integration content section, select the iFlow that you want to download and click *Finish*.
6. The project is imported and displayed under the Project Explorer

5.5.2 View the configured certificates and externalized parameters

1. In the Project Explorer, expand the tree view and double click to open the iFlow found under *scr.main.resources.scenarioflows.integrationflows*.
2. In the Integration Designer, select the iFlow.
3. Within the iFlow, select the sender system under the *Properties* tab.
4. If you wish to update the authentication of the iFlow to *Basic Authentication*, select the mode of authentication as *Basic Authentication*.
5. For certificate based authentication, view the details un the *Properties* tab.
6. To view the configuration of the iFlow, click on the *Externalized Parameters* tab, under the *Value* field, and view the configured <host>:<port> information of the receiver system.

5.5.3 Extend the project in Eclipse and Deploy

1. To extend the iFlow project, you can make modifications to any of the three folders:
 - a. *Scr.main.resources.mapping*
 - b. *Scr.main.resources.scenarioflows.integrationflow*
 - c. *Scr.main.resources.wsdl*
2. Deploy the modified iFlow project by using the right click option at the iFlow project level and selecting *Deploy Integration Content*.
3. Enter the *Tenant ID* and click *OK*.

6 Monitor Phase: Monitor Messages Across Systems

Messages are exchanged between the SAP Access Control, SAP Cloud Integration, and SAP SuccessFactors systems, during data load and go-live phases. These messages need to be monitored to:

- Identify incorrect data in messages
- Identify the component where the message has failed
- Check connectivity issues between the components

6.1 Initial Load

Initial load triggers an initial transfer of all employee records from Employee Central to SAP Access Control. You specify a start date to select the employee records to be processed.

6.2 Delta Load

Delta load applies to customers who are using SAP Access Control in a production environment and are newly integrating with SAP SuccessFactors. When you execute the data transfer process, the system records the timestamp of the run. The system uses this timestamp to select the employee changes for the next integration run. Only changes that are newer than the recorded timestamp are included in the next integration run.

6.3 Field Mapping in SAP Cloud Integration

The tables below list the field mapping between the OData API structure from Employee Central and the Web service structure from SAP Access Control.

This table shows the delivered field mapping used by SAP Cloud Integration.

Note

If you add custom fields, you must also modify the SAP Cloud Integration process. For more information, see SAP SuccessFactors Employee Central Configuration.

Employee Details

OData API Structure Node	OData API Structure Attribute	Web Service Node	Web Service Attribute
person	person_id_external	UserChangeDetails.item	Userid
person.personal_information	first_name	UserChangeDetails.item	Fname
person.personal_information	last_name	UserChangeDetails.item	Lname
person.email_information	email_address	UserChangeDetails.item	Email
person.phone_information	phone_number	UserChangeDetails.item	Telnumber
person.employment_information	end_date	UserChangeDetails.item	ValidTo
person.employment_information.job_information	Company	UserChangeDetails.item	Company
person.employment_information.job_information	Department	UserChangeDetails.item	Department

person.employment_informati on.job_information	job_code	UserChangeDetails.item	Empjob
person.employment_informati on.job_information	manager_id	UserChangeDetails.item	Manager
person.employment_informati on.job_information	Position	UserChangeDetails.item	Empposition
person.employment_informati on.job_information	cost_center	UserChangeDetails.item	Costcenter
person.employment_informati on.job_information	start_date	UserChangeDetails.item	ValidFrom
person	person_id_ext ernal	UserChangeDetails.item. UserChange.item	USERID
person.employment_informati on	end_date	UserChangeDetails.item. UserChange.item	VALID_TO
person.employment_informati on.job_information	action	UserChangeDetails.item. UserChange.item	
person.employment_informati on.job_information	business_unit	UserChangeDetails.item. UserChange.item	BUSINESS_AREA
person.employment_informati on.job_information	company	UserChangeDetails.item. UserChange.item	COMPANY
person.employment_informati on.job_information	company_terri tory_code	UserChangeDetails.item. UserChange.item	COMPANY_TERRI TORY_CODE
person.employment_informati on.job_information	department	UserChangeDetails.item. UserChange.item	DEPARTMENT
person.employment_informati on.job_information	division	UserChangeDetails.item. UserChange.item	PERSONNELAREA

person.employment_informati on.job_information	emplStatus	UserChangeDetails.item. UserChange.item	EMPLSTATUS
person.employment_informati on.job_information	event	UserChangeDetails.item. UserChange.item	EVENT
person.employment_informati on.job_information	job_code	UserChangeDetails.item. UserChange.item	EMPJOB
person.employment_informati on.job_information	manager_id	UserChangeDetails.item. UserChange.item	Manager
person.employment_informati on.job_information	position	UserChangeDetails.item. UserChange.item	EMPPOSITION
person.employment_informati on.job_information	start_date	UserChangeDetails.item. UserChange.item	VALID_FROM

Employee Change Details

OData API Structure Node	OData API Structure Attribute	Web Service Node	Web Service Attribute
person	person_id_external	UserChangeDetails.item. UserChange.item	USERID
person.employment_information	end_date	UserChangeDetails.item. UserChange.item	VALID_TO
person.employment_information.job_information	action	UserChangeDetails.item. UserChange.item	
person.employment_information.job_information	business_unit	UserChangeDetails.item. UserChange.item	BUSINESS_AREA
person.employment_information.job_information	company	UserChangeDetails.item. UserChange.item	COMPANY
person.employment_information.job_information	company_territory_code	UserChangeDetails.item. UserChange.item	COMPANY_TERRITORY_CODE
person.employment_information.job_information	department	UserChangeDetails.item. UserChange.item	DEPARTMENT
person.employment_information.job_information	division	UserChangeDetails.item. UserChange.item	PERSONNELAREA
person.employment_information.job_information	emplStatus	UserChangeDetails.item. UserChange.item	EMPLSTATUS
person.employment_information.job_information	event	UserChangeDetails.item. UserChange.item	EVENT
person.employment_information.job_information	job_code	UserChangeDetails.item. UserChange.item	EMPJOB

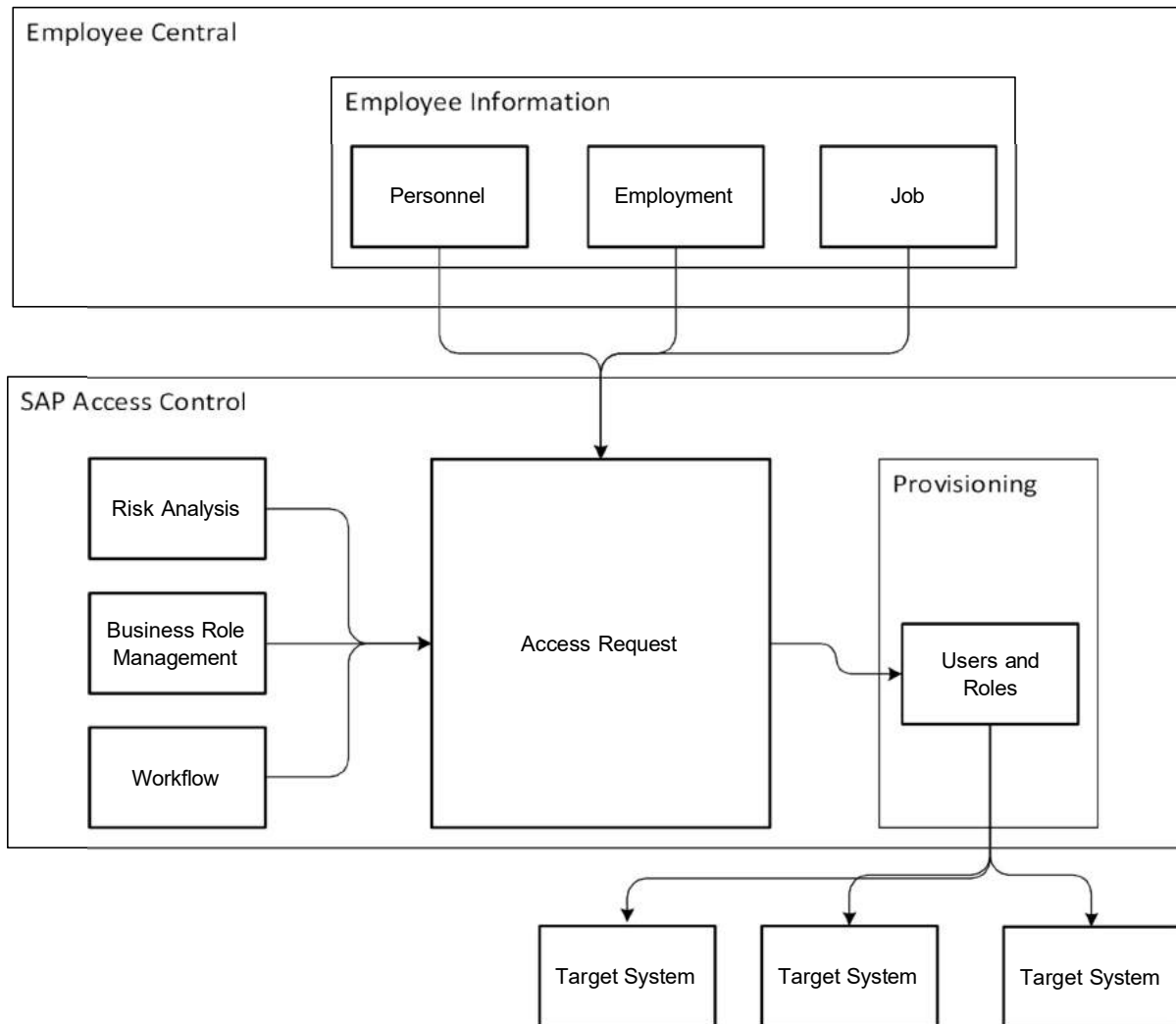
person.employment_information.job_information	manager_id	UserChangeDetails.item. UserChange.item	Manager
person.employment_information.job_information	position	UserChangeDetails.item. UserChange.item	EMPPPOSITION
person.employment_information.job_information	start_date	UserChangeDetails.item. UserChange.item	VALID_FROM

Custom Fields

OData API Structure Node	OData API Structure Attribute	Web Service Node	Web Service Attribute
Structure Node	Attribute	UserChangeDetails.item.CustomFields.item	SAP ACCESS CONTROL Custom Field Name

7. Data Integration Concepts

SAP SuccessFactors Employee Central is your master system. Changes to employee data in Employee Central are transferred to SAP Access Control using SAP Cloud Integration. This integration process is illustrated below:



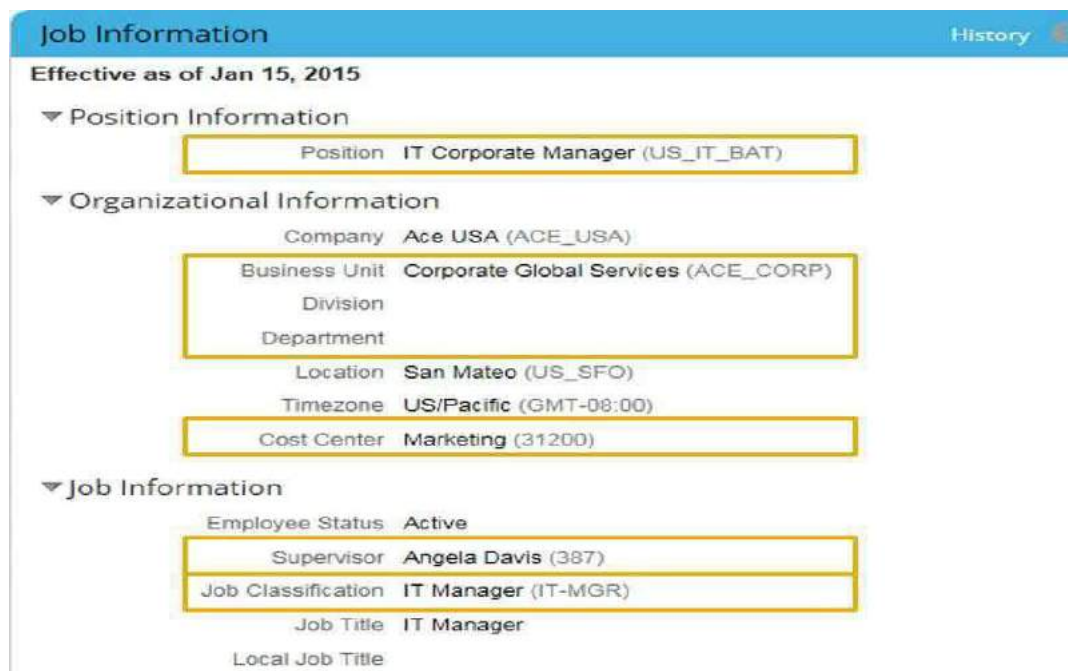
i Note

An integration package is delivered for SAP Cloud Integration that contains the iFlow covering the entire integration scenario. After you deploy and configure the iFlow, the scenario is ready to run.

7.1 Transferring Employee Change Data

SAP Cloud Integration triggers employee data transfer from Employee Central using the scheduled SAP Cloud Integration process.

Below is an example of an employee's job information in Employee Central. This employee has a position, a business unit, a cost center, a manager, and a job classification assignment.



The screenshot displays the 'Job Information' page in SAP Employee Central, effective as of Jan 15, 2015. The page is organized into three main sections: Position Information, Organizational Information, and Job Information. Each section contains key data points highlighted with yellow boxes.

Section	Field	Value
Position Information	Position	IT Corporate Manager (US_IT_BAT)
Organizational Information	Company	Ace USA (ACE_USA)
	Business Unit	Corporate Global Services (ACE_CORP)
	Division	
	Department	
	Location	San Mateo (US_SFO)
	Timezone	US/Pacific (GMT-08:00)
Job Information	Cost Center	Marketing (31200)
	Employee Status	Active
	Supervisor	Angela Davis (387)
	Job Classification	IT Manager (IT-MGR)
	Job Title	IT Manager
	Local Job Title	

7.2 Staging Tables

Once SAP Access Control receives the employee change data, it is stored in staging tables. If needed, you can use these staging tables for troubleshooting the integration process. The following are the staging tables:

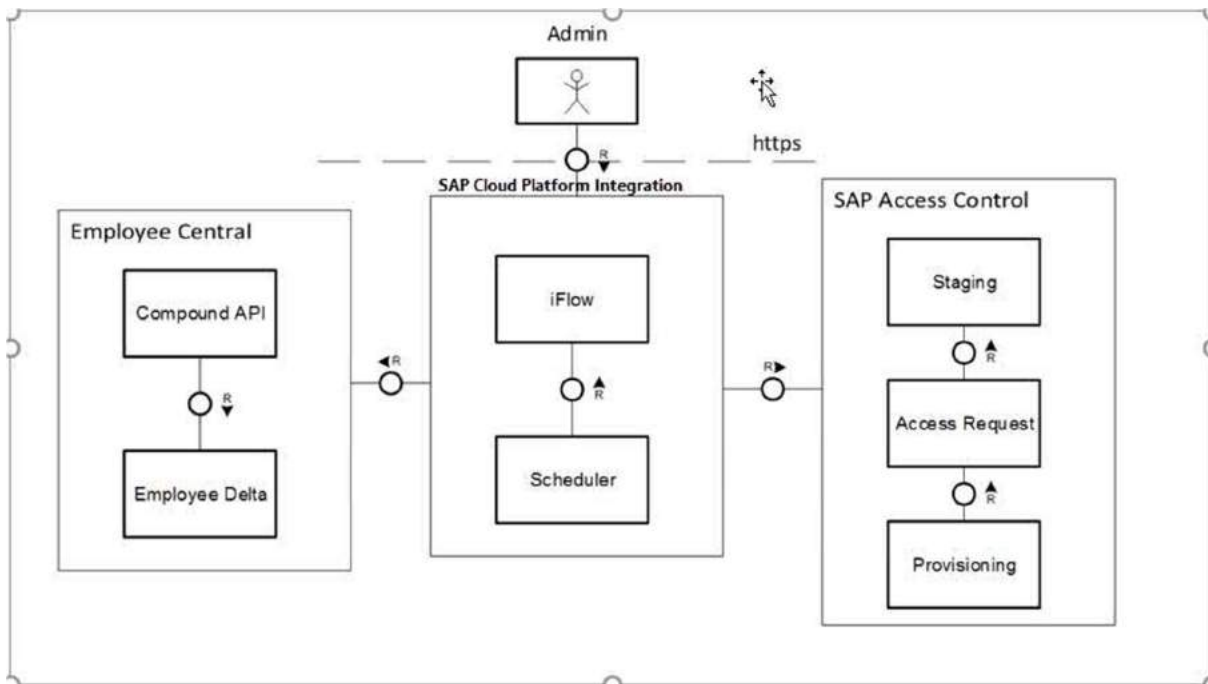
Staging Table Name	Description
GRACSFECTRUSER	Employee Details
GRACSFECUSRCHNG	Employee Change Information
GRACSFECUSERCF	Employee Custom Fields

Table GRACSFECTRUSER contains a processing status for each record. The possible statuses are listed in the table below.

Processing Status	Meaning
OPEN	Record is not yet processed
PROCESSED	Request successfully created
FAILED	Request was not created due to errors

7.3 OData Services and SOAP Messages

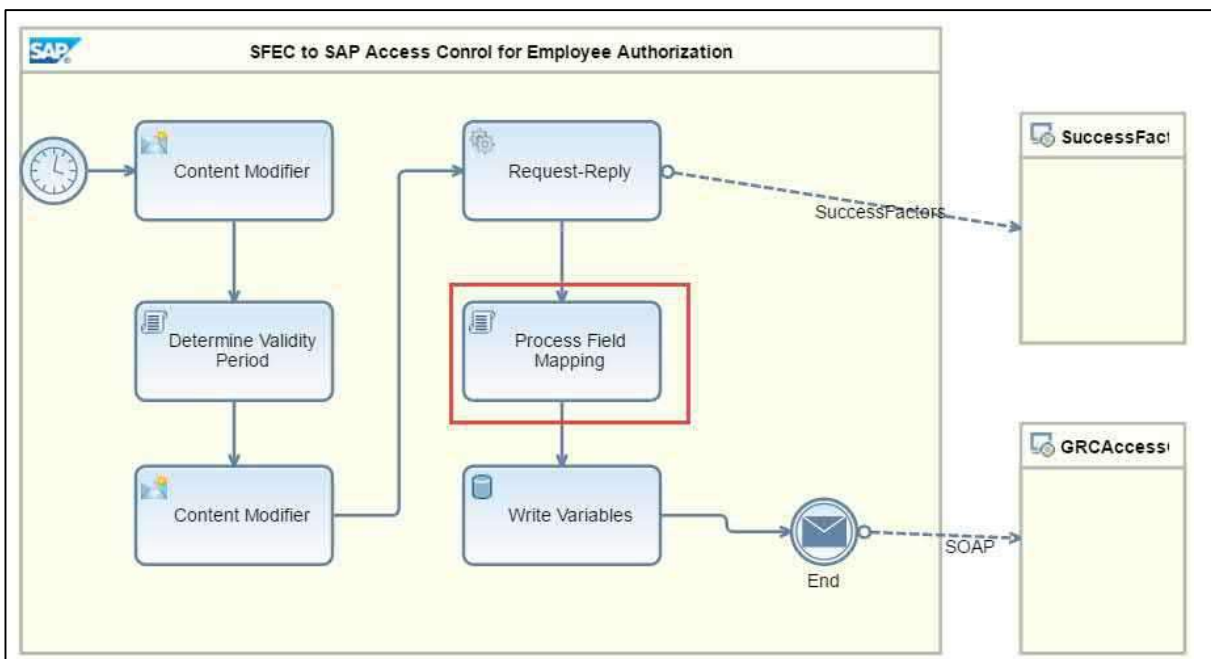
The transfer process is always triggered from SAP Cloud Integration, either manually by an administrator, or automatically by a scheduled, periodic process. SAP Cloud Integration calls an OData service that extracts data according to filter values. The employee data is then transferred to SAP Access Control as a SOAP message. Once data arrives in SAP Access Control, Access Control takes actions based on BRF+ rules. An access request is created with the correct authorizations.



The following OData services and SOAP messages are used in the data transfer process:

Source/Destination	OData/SOAP Service	SOAP Message
Employee Central	CompoundEmployee	11508 XML SFOData.EmployeeHRTrigger Element QUERY Response
SAP Access Control	GRAC_SFEC_HR_TRIGGER	1508 XML Web Services SOAP Client SAP AC Employee HR Trigger Request_In EXECUTE Request

7.4 Extending the Data Transfer Process



If you want to extend the data transfer process, you can create a custom (or country-specific) field in Employee Central. In SAP Access control, you create corresponding custom fields and map the fields to the corresponding Employee Central field.

8 Monitoring the Integration Process

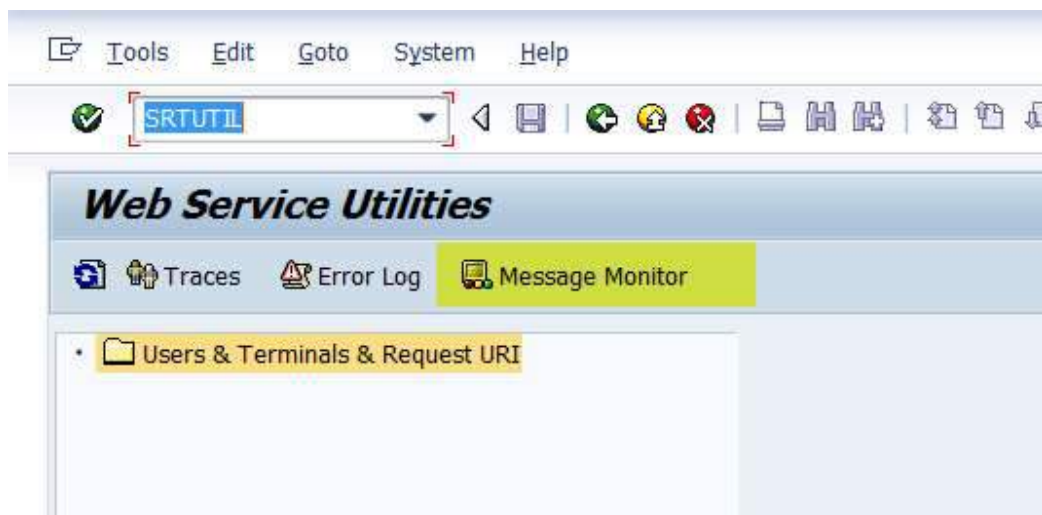
This section describes the tools that are available for monitoring the transfer of employee data from SAP SuccessFactors Employee Central to SAP Access Control. The table below shows an overview of the monitoring tools that are described in more detail in the following sections.

Integration Monitoring Tools

System	Monitoring tool	Where can I find it?	What is it used for?
SAP Access Control	Web Service Utilities offers an <i>Error Log</i> and a <i>Message Monitor</i> tool.	Transaction <i>SRTUTIL</i> (Web Service Utilities) or <i>SXMB_MONI</i> (Integration Engine: monitoring)	Monitor incoming SOAP messages
SAP Access Control	Application Log	Transaction <i>SLG1</i>	Monitor creation of inbound messages and storage of replication requests in the staging area
Employee Central	SFAPI Audit Log	<i>Administration Tools</i> → <i>Company Processes & Cycles</i> <i>Company Settings</i> → <i>SFAPI</i> → <i>Audit Log</i>	Monitor Compound Employee API calls for employee assignment data
SAP Cloud Integration	Process Reporting	<i>Operations view</i> → <i>Monitor Message Processing</i> → <i>Integration Flow tile</i> → <i>Select the artifact name</i> → <i>Check the status details and logs</i>	Monitor the message processing in SAP Cloud Integration CI Web UI.

8.1 SAP Web Service Utilities

To access the SAP Web Service Utilities, in the SAP system, go to transaction *SRTUTIL*.



➔ Recommendation

For more information about the tool, see *Web Service Logging and Tracing* in the ABAP Web Services documentation (search for *web service logging and tracing* in the SAP Help Portal at <http://help.sap.com/netweaver>).

i Note

Depending on your system configuration, transaction *SRTUTIL* might not be available. If the transaction is not available, use transaction *SXMB_MONI* - *Integration Engine: Monitoring*.

8.1.1 SAP Message Monitor

The *Message Monitor* shows you an overview of all received messages along with their content. You can select the message, for example, by specifying the execution time.

Use transaction *SRTUTIL* to access the Message Monitor. Click the *Message Monitor* icon to access the screen below.

The screenshot displays the SAP Message Monitor interface. At the top, the title bar reads "Web Service Utilities: Message Monitor". Below this, there are several sections:

- Result Output:** Contains radio buttons for "Summary" and "Detail" (selected), and a "Restore Default Selection" button.
- Message View:** Contains radio buttons for "Basic View" (selected) and "Technical View".
- Selection Methods:** Three tabs: "Standard Selection", "User-Defined Selection", and "Advanced Selection".
- Message ID and Sequence ID:** Two input fields, each with a search icon.
- Based on time range:** A section with two radio buttons: "Execution Time" (selected) and "Creation Time". It includes:
 - Timestamp from:** 13.04.2015 / 10:24:23
 - Timestamp to:** 13.04.2015 / 23:59:59
 - Max. Number of Messages:** A text input field containing "200".
 - Processing Status Group:** A dropdown menu.
 - Adapter Type:** A dropdown menu.
 - User Name:** A text input field.

8.2 SAP Application Log

The system creates an application log when the employee change data are processed and stored as access requests in the staging area, as well as when the entries in the staging area are processed.

Procedure

1. Go to transaction Analyze Application Log (SLG1)
2. Enter the object GRAC
3. Enter the sub object HRTRIGGERSFEC.
4. Click *Execute*.

Analyse Application Log

Object: GRAC (generic input)
Subobject: HRTRIGGERSFEC (generic input)
External ID: *

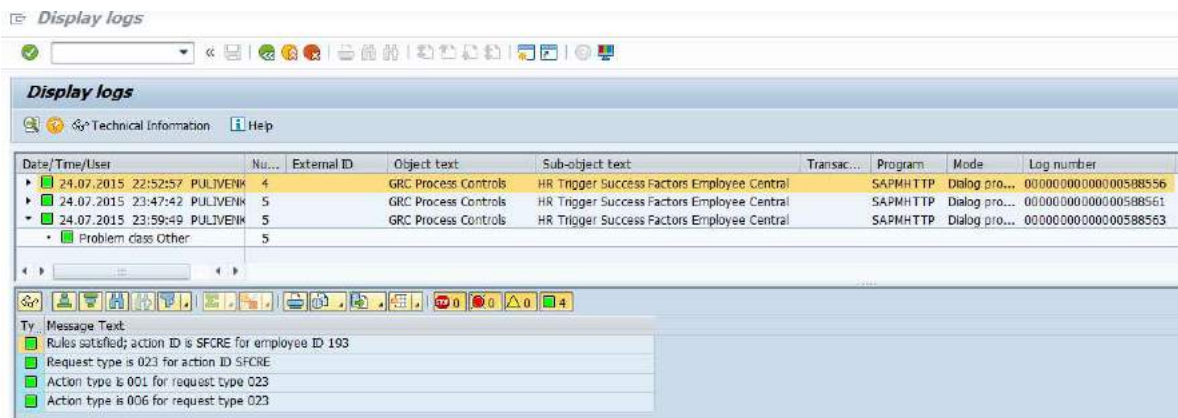
Time Restriction
From (Date/Time): 16.08.2015 00:00:00
To (Date/Time): 16.08.2015 23:59:59

Log Triggered By
User: *
Transaction code: *
Program: *

Log Class
 Only very important logs
 Only important logs
 Also less important logs
 All logs

Log Creation
 Any
 Dialog
 In batch mode
 Batch input

5. The application log displays.
 - a. Status indicator
 - b. Message texts apply to the row selected above. Click the row to display all related messages.
 - c. Each row represents one run of the interface



8.3 Employee Central SFAPI Audit Log

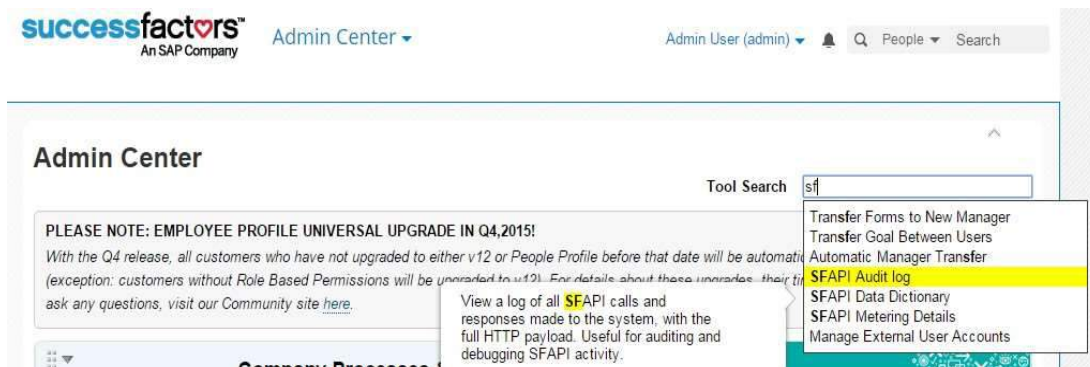
The audit log for the Compound Employee API from Employee Central contains Employee Central data.

Note

The SFAPI Audit Log is intended to help with support and debugging of API usage. You can use it, for example, to share information with SAP support to help resolve API related support issues. The tool allows you to download data from individual calls, which you can send to an SAP support representative.

Procedure

1. To access the SFAPI Audit Log, go to Employee Central and choose *Administration Tools*.
2. In the Tool Search, enter *SFAPI*.



3. The system displays the Audit Log.



4. The Audit Log shows the last 10,000 API calls to the system. For each call, you can view the details by selecting the button under the *SOAP* or *HTTP* columns in the log table.
5. You can use the *Session ID* from SAP Cloud Integration to find a specific API call in the SFAPI Audit Log

SFAPI Audit Log

Filter Options

Login ID

Session ID

Correlation ID

ID	Login ID	Status	SFAPI Call	Object	SOAP	HTTP	Call Time	Response (ms)	Session ID	Correlation ID
662759		Success	query	compoundemployee			2015-05-05 14:16:02.003	1906	A44D2AEEB03CA5E6F1FB89848D2812F1.DC13QACANDSFAP101	Z7e62790-70a3-402-ac54-1408bd423a22
662755		Success	login				2015-05-05 14:15:58.252	51	A44D2AEEB03CA5E6F1FB89848D2812F1.DC13QACANDSFAP101	6eb6e0c4-5ce1-4877-a29f-a80167643

Note

For more information about the SFAPI Audit Log, refer to the **HCM Suite SFAPI** programmer's guide at <http://help.sap.com/cloud4hr>, under **APIs**.

8.4 Process Reporting in SAP Cloud Integration

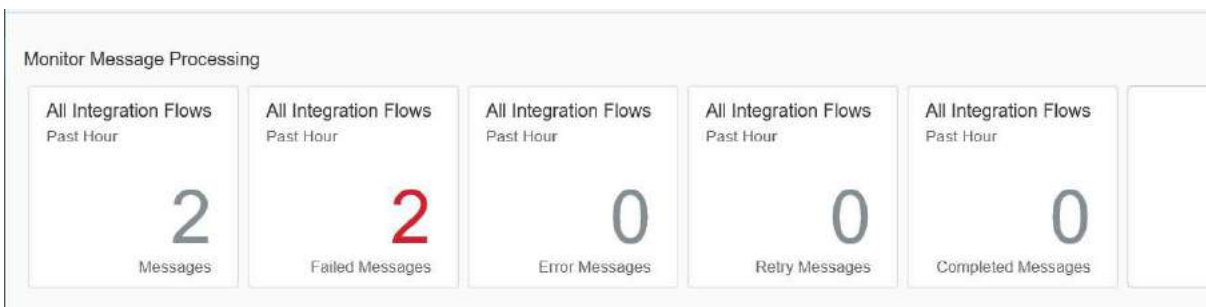
To monitor the process execution in SAP Cloud Integration, sign on to SAP Cloud Integration.

Procedure

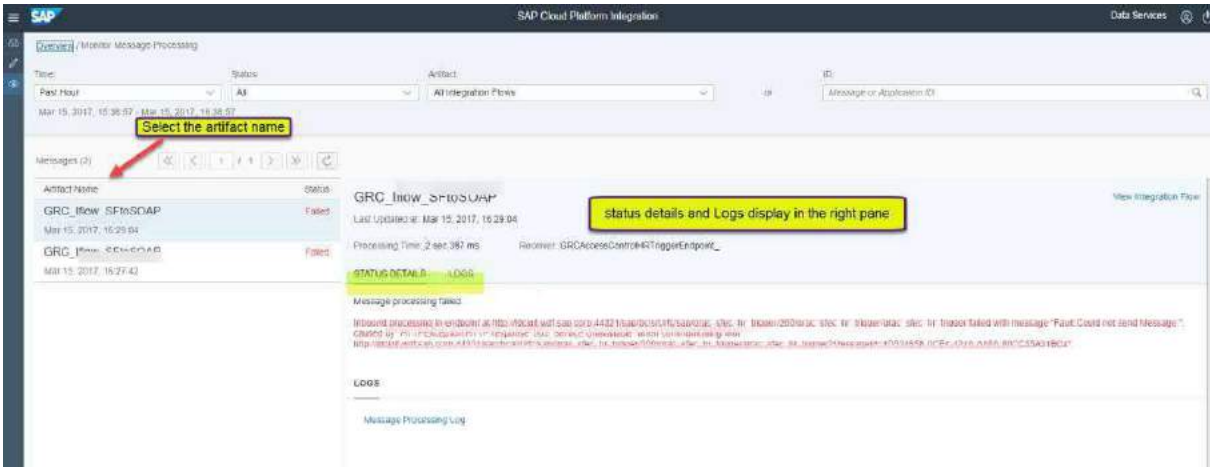
1. From the SAP Cloud Integration Web UI (<https://cd2grc1-tmn.hci.int.sap.hana.ondemand.com/itspaces/#/shell/discover>), choose the *Operations* view



2. Under Monitor Message Processing, choose the appropriate Integration Flow tile.



3. In the left navigation pane, select the artifact name.



4. In the right pane, the system displays the *Status Details* and *Logs* within the specified timeframe on the messages in which your processes are deployed.

8.4.3 Messages in SAP Web Service Utilities

You can use the *Timestamp* from SAP Cloud Integration to filter for a specific entry in the message monitor of the *Web Service Utilities* tool in the SAP system.

Procedure

1. In the SAP Access Control system, go to transaction *SRTUTIL*.
2. Click Message Monitor
3. Enter the *Timestamp* range.
4. Click Execute.

Web Service Utilities: Message Monitor

Result Output
 Summary Detail Restore Default Selection

Message View
 Basic View Technical View

Standard Selection | User-Defined Selection | Advanced Selection

Message ID

Sequence ID

Based on time range
 Execution Time Creation Time Max. Number of Messages

Timestamp from /

Timestamp to /

Processing Status Group

Adapter Type

User Name

Sender Information

Addressing
 IBC IBC Type IBC Name
 Party Party Name

Interface Name

Receiver Information

Addressing
 IBC IBC Type IBC Name
 Party Party Name

Interface Name

Enter the timestamp range that you want to display

5. On the result screen, click the outgoing connection.
6. Click *View Document* to see the details.

DOCUMENT CHANGE HISTORY

Release	Version	Date	Description
Q2 2021	2.0	June, 2021	Updated version

Important Disclaimers and Legal Information

Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of wilful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: <http://help.sap.com/disclaimer>).

© 2017 SAP SE or an SAP affiliate company. All rights reserved. No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx> for additional trademarks information and notices.