SAP SuccessFactors

PUBLIC
SAP Best Practices for SAP SuccessFactors
Document Version: 1H 2022 – 2022-05-18

Getting Started Guide: SAP Best Practices for SAP SuccessFactors EC Integration with SAP ERP HCM Payroll

THE BEST RUN SAP

Content

1 Purpose

This Getting Started guide describes all activities you need to carry out before you implement the solution package from system preparation to implementation of the business content and validation.

Further Info

This section is for the following target groups who already have a sound knowledge of the SAP Best Practices implementation, including tools and documentation.

- **Business consultants**: Evaluate business content/processes including troubleshooting, FAQ, and further information, for extended usage of the package.
- **Implementation consultants (application consultants)**: Implementation of business content and processes.

> **i** Note
>
> The Reimagined Home Page (Latest Home Page) will be pushed to all customer instances (that are not already migrated). For more details, check the Migration to Reimagined Home Page June 2022 - Innovation Alert post in the *SAP SuccessFactors Community*.
>
> Therefore all home page activities described in this solution are already based on the new UI experience.

> **i** Note
>
> All workbooks referenced in the configuration guides can be found on the SAP Help Portal.

2 Solution Overview

The SAP Best Practices content for migration and replication is intended to accelerate the migration of organizational and employee data from the on-premise SAP ERP HCM System to SAP SuccessFactors Employee Central and to enable replication of the data from SAP SuccessFactors Employee Central to SAP HCM on-premise Payroll in the core hybrid setup.

The salient features of the solution are the following:

- Based on Business Integration Builder solution.
- Based on SAP Cloud Platform Integration as the middleware for integration between SAP HCM and SuccessFactors Employee Central.
- Based on SAP Best Practices content for deploying SuccessFactors Employee Central.
- Accelerates deployment of the required configuration, including mappings and BADIs to integrate SAP ERP HCM and Best Practices SuccessFactors Employee Central.

3 System Setup and Preparation

Prior to implementing an SAP Best Practices package (SAP BP package), check the **Software and Delivery Requirements** document regarding required SAP notes to be installed in the on-premise finance/cloud payroll system.

4 Preparing for Implementation

4.1 SAP ERP HCM

4.1.1 Create Technical Communication User

A communication user must be created in the SAP ERP HCM system for technical communication between the ERP system and Cloud Platform Integration account as a system or communication user.

1. In your **SAP ERP HCM** system, access the transaction using one of the following navigation options:

Transaction Code	**SU01**
Menu Path	▶ *SAP Menu* ▶ *Tools* ▶ *Administration* ▶ *User Maintenance* ▶ *Users* ▶

2. On the *User Maintenance: Initial Screen*, enter a **<User Id>** for your technical user, for example, SF_COMM.
3. Choose *Create*.
4. On the **Logon Data** tab, choose the *entry B (System)*, as *User Type*.
5. On the **Roles** tab, assign the user roles described in the next section Authorization Roles [page 6] to the user.
6. *Save* your user.

4.1.2 Authorization Roles

The following roles specific to integration and migration need to be provided to the technical communication user created in the previous step. These roles also need to be provided to users who are testing and executing the migration and replication reports.

- SAP_HR_SFIOM_PROCESSING
- SAP_HR_SFIOM_WEBSERV
- SAP_HR_SFI_EMPL_DATA_REPL

In addition, the user customizing the technical settings would require access to the generic roles (if not already provided by the system administrator) to carry out customizations in the Configuration guides.

- SAP_BC_WEBSERVICE_SERVICE_USER
- SAP_BC_CUS_CUSTOMIZER
- SAP_ABAP_CHANNELS_ADMIN
- SAP_BC_CTS_ADMIN
- SAP_BC_WEBSERVICE_ADMIN_TEC

- B_ALE_ALL
- S_IDOC_ALL

4.1.3 Obtain Signed Client Certificate

Communication from ERP to CPI is based on Client Certificate Authentication.

The client certificate for the ERP system must be signed by one of the certifying authorities, which is trusted by the load balancer. Further information can be found on the Load Balancer Root Certificates Supported by SAP page.

The client certificate needs to be imported to the ERP system using the transaction STRUST (Trust Manager).

In addition, the certifying authority's root certificates and other certificates must also be imported to the Cloud Platform Instance, if not done already.

4.2 SAP SuccessFactors Employee Central

4.2.1 SAP SuccessFactors Provisioning Settings

You must have access to SAP SuccessFactors Employee Center provisioning to perform the configuration for the instance. As a customer, you do not have access to Provisioning. To complete tasks in Provisioning, contact your implementation Partner. If you are no longer working with an Implementation partner, contact SAP Support.

In the SAP SuccessFactors instance, the following provisioning switches need to be checked in the **Company Settings** of your company:

Edit Company Settings > *Company Settings* :

> **i Note**
>
> If the SAP Best Practice pre-configured instance has been copied, all Employee Central related switches are disabled by default and need to be enabled again.
>
> If the instance was not copied, most of the provisioning settings will already be enabled in your company based on the licensing.
>
> Check the below listed switches and enable the missing one based on your scope.

> **i Note**
>
> For utilizing the search capabilities (control + F) in Provisioning, the exact text of the setting is listed.

Switch	Status
Enable Advances — requires “Employee Central V2 (that is Event Reason Derivation)”, “Enable Generic Objects”, “Enable Deductions Management”, “Effective Dated Data Platform”, “Employee Profile data audit” and “Enable the Attachment Manager”	**Enabled**
Enable Deductions Management — requires “Employee Central V2 (that is Event Reason Derivation)”, “Enable Generic Objects”, “Effective Dated Data Platform”, “Employee Profile data audit” and “Enable the Attachment Manager”	**Enabled**
Enable Cost Distribution — requires “Employee Central V2 (that is Event Reason Derivation)”, “Enable Generic Objects”, “Effective Dated Data Platform”, “Employee Profile data audit” and “Enable the Attachment Manager”	**Enabled**
Enable Business Configuration in Admin Tools	**Enabled**
Enable Name Format	**Enabled**
Enable new Payment Information (MDF-based, effective-dated, and employment-specific). ⚠ Caution For existing customers, by switching on this feature via the Upgrade Center, the old direct-deposit-based UIs, APIs and objects will be irreversibly deactivated. New Payment Information is integrated into Employee Central Payroll. Integration scenarios towards 3rd party systems utilizing the old direct deposits APIs might no longer work. Check in advance and inform customers that they might need to migrate existing 3rd party integration scenarios to the new APIs, for example, compound employee API or OData API.	**Enabled**

Switch	Action
Enable Payroll Integration (Valid for SAP Payroll in ERP Systems) — requires “Enable Generic Objects”, “Enable Translation of Employee Central Foundation Objects”, “Enable the Attachment Manager” and “Employee Central Foundation Objects”	**Enable**
Language Packs	**Enable**
English US (English US)	**Enable**
Show ToDo Portlet	**Enable**
Enable Proxy Feature	**Enable**

Select *Save Feature*.

⚠ Caution

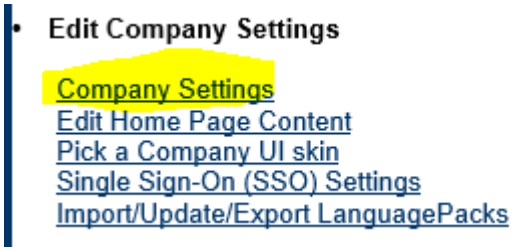
Furthermore this SAP Best Practices content requires the latest user interface for the employee profile – People Profile.

People Profile is a prerequisite for a growing number of new solutions and functionalities.

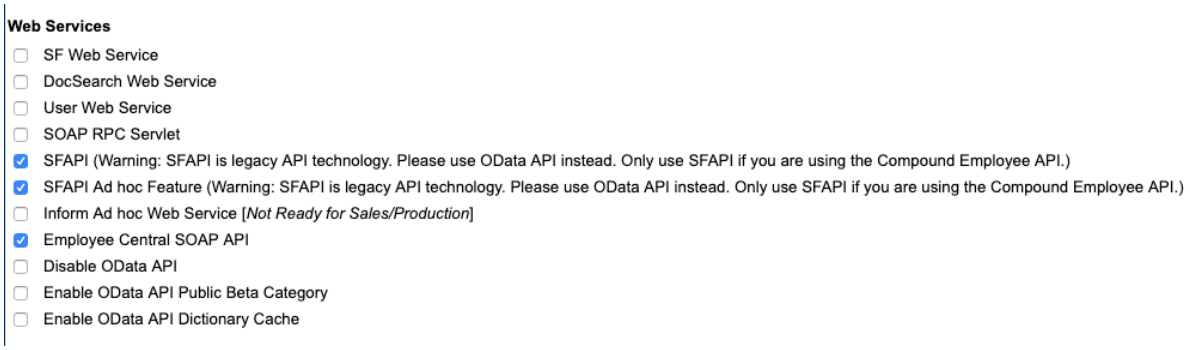
4.2.2 API Permissions

APIs must be enabled in **SuccessFactors Provisioning**.

In provisioning, choose *Company Settings*.



Select the following checkboxes to enable APIs:



4.2.3 Creating a User for Activation of SAP Best Practices Content

Use

In this activity, you create a user to run and check the upgrades for the related SAP Best Practices scope if not yet available in the system.

> **i Note**
>
> We recommend using only one User ID with a valid e-mail address to activate the SAP Best Practices content. Thus, you avoid changing ownership during the activation.

Procedure

1. Log in to **SAP SuccessFactors Provisioning** for your instance using the following link:

Link	https://<server>.successfactors.com/provisioning_login

2. Choose the company by selecting the company name.
3. Access the activity using one of the following navigation options:

Menu Path	*Edit Company Settings* > *Company Settings*

4. Search for *Admin Username*.
5. Enter the following data:

Admin Username	**Enter a value, for example** <UPCAdmin>
Admin Password	Enter password. This password needs to be changed with the first login to a password that is suitable to your company policy
Admin First Name	Enter the first name for the admin user
Admin Last Name	Enter the last name for the admin user
Admin Email	Enter the e-mail address of the Admin

> ⚠ Caution
>
> Enter a valid e-mail address. All logs and status updates regarding the implementation will be send via e-mail to this e-mail address.

6. Choose *Create Admin* to create the admin user.
7. Choose *Save*. The user has been generated.

4.2.4 Provide Role-Based Permission Access for Activation

Use

This section describes the set-up steps necessary to allow the previous created user to manage the role-based permission access.

Procedure

1. Log on to the instance of your company.
2. Go to *Admin Center*.
3. Type **`Manage Role-Based Permission Access`** in the tool search box and select the feature/tool from the list.
4. The *Manage Role-Based Permission Access* page opens.
5. Choose *Add User*.
6. In the *User Name* field, enter the super admin user name you have created before and choose *Search*.
7. In the *Search Users* portlet select the admin username and choose *Grant Permission*.
8. Log out and log on again as admin user to refresh the assigned role-based permission. Your admin user now has authorization to maintain role-based permissions.

4.2.5 Manage Upgrade Center Admin Permission

For implementing the SAP Best Practices for Employee Central, some basic permissions are needed to run the activation and to check the result. Only for this purpose create an SAP Best Practices Upgrade Center Admin role and group as described below.

> **i** Note
>
> This role and group is only needed for the implementation of the SAP Best Practices scope and can be deleted after the finalization.

4.2.5.1 Create Upgrade Center Admin Group

1. Log on to the instance of your company.
2. Go to *Admin Center*.
3. Type **`Manage Permission Groups`** in the tool search box and select the feature/tool from the list.
4. The *Manage Permission Groups* page opens.
5. Select *SAP BestPractices Upgrade Center Admin* group.
6. In the *Choose Group Members: People Pool* section, in *Pick a category*, choose *User name*.
7. In the Search Results window select the Upgrade Center admin name, for example, UPCAdmin.
8. Select *Done*. Log out and log back in as the admin user.

4.2.6 Migrate Picklists from Legacy to MDF

If the picklists in the Employee Central instance are not already migrated to MDF picklists, the following steps need to be followed for picklist conversion prior to activating SAP Best Practices content.

In order to check whether the picklists are migrated, go to *Admin center* and search for *Picklist*. If you see *Picklist Management*, it means that you are still using the legacy picklist and they have not being migrated. On the other hand, if you see *Picklist Center*, it means they have already been migrated to the MDF Picklist.

Refer to the following for Picklist Migration:

2504047 – Pre-Picklist Migration Guide

2328179 – Post Picklist Migration Guide

2816504 – Resolving Post Picklist Migration Issues

4.2.7 Activate Best Practices Content from Upgrade Center

The following upgrade center items need to be activated to enable Best Practices:

1. **Best Practices Employee Central Core Content**
2. **Best Practices Employee Central Core Content (for the relevant country localizations)**
3. **Best Practices Employee Central Position Management**
4. **Best Practices Employee Central Time Off**
5. **Best Practices Employee Central Time Off(for the relevant country localizations)**
6. **Best Practices Employee Central Global Assignment Management**
7. **Best Practices Employee Central Concurrent Employment**

Procedure

1. Log on to the instance of your company.
2. Go to *Admin Center*.
3. Type `Upgrade Center` in the tool search box and select the feature/tool from the list.
4. In the *Upgrade Center* go to the *Recommended Upgrades* section and the corresponding upgrade item, and choose *Learn more & Upgrade*.
5. You can see the feature details now.
6. Go through the *Quick Guide* to ensure that all steps needed prior to the upgrade have been completed.
7. At the bottom, choose *Upgrade Now*.
8. On the next screen, choose *Yes*.
9. Go back to the *Admin Center*.

5 Implementation

Follow the steps in this section to get started on the implementation. Adapt the integration settings based on the payroll settings and customer requirements.

All Configuration Guides can be found on the **https://help.sap.com/docs/SAP_SUCCESSFACTORS_EMPLOYEE_CENTRAL_INTEGRATION_TO_SAP_BUSINESS_SUITE/4f9aaa4dca534465858008d87e19ec80/dec700bfe8004d7aa3e7564a6b2b102a.html**.

5.1 Technical Users

5.1.1 SAP SuccessFactors Employee Central

5.1.1.1 Set up SFAPI User

1. Log on to the instance of your company.
2. Go to *Admin Center*.
3. Type **`Employee Export`** in the tool search box and select the feature/tool from the list.
4. To create a new user, for example SFAPI, first export the employee template, then adapt the template and finally import the file.
5. Choose *Export Template* and save the file on a share.
6. Fill the file with the following information:

Field Name	Value
STATUS	**active**
USERID	**SFAPI**
USERNAME	**SFAPI**
FIRSTNAME	**User**
LASTNAME	**SFAPI**
GENDER	**for example, M**
EMAIL	**for example,** sfapi@xxx.com
MANAGER	**NO_MANAGER**

Field Name	Value
HR	**NO_HR**
DEPARTMENT	**N/A**
JOBCODE	**N/A**
DIVISION	**N/A**
LOCATION	
TIMEZONE	**for example, US/Eastern**
DEFAULT_LOCALE	**for example, en_US**

7. Save the file.
8. Back in the instance type *Import Employee Data* in the tool search box and select the feature/tool from the list.
9. In field *Select an entity* choose *Basic Import*, browse for the filled file, keep file encoding **Unicode (UTF-8)**.
10. Validate the import file before importing it. Choose*Validate Import File Data*.
11. Second, import the file. Choose *Import*.
12. To reset the user's password type *Reset User Passwords* in the tool search box and select the feature/tool from the list.
13. On the *Resetting User Passwords* screen, search for the newly created user.
14. Enter *New Password* and *Confirm Password* and choose *Reset User Password*.

5.1.2 Setup SF API User Group

1. Log on to the instance of your company.
2. Go to *Admin Center*.
3. Type **`Manage Permission Groups`** in the tool search box and select the feature/tool from the list.
4. On the *Manage Permission Groups* page select *Create New*.
5. In the *Permission Group* window on the *Definition* tab, in field *Group Name* enter *SAP BestPractices SFAPI User Group*.
6. In the *Choose Group Members: People Pool* section, in *Pick a category*, choose *Username*.
7. In the *Search Results* window search for the SFAPI user name, for example *sfapi*.
8. Select the user.
9. Choose *Done*.

5.1.3 Set up SF API Permission Roles

1. Log on to the instance of your company.

2. Go to *Admin Center*.
3. Type **`Manage Permission Roles`** in the tool search box and select the feature/tool from the list.
4. On the *Manage Permission Roles* page select *Create New*.
5. The *Permission Role Detail* page opens.
6. In field *Role Name:* enter **`SAP BP SFAPI`** and in field *Description:* enter **`SAP Best Practices SFAPI User Role`**.
7. Under *Permission settings* choose *Permission...*.
8. Under *User Permissions* → *General User Permissions* select the *SFAPI User Login* checkbox.
9. Under *Administrator Permissions* → *Manage Integration Tools*, select the following checkboxes.
    - **Access to SFAPI API Audit Log**
    - **Access to SFAPI Metering Details**
    - **Access to SFAPI Data Dictionary**
    - **Allow Admin to Access OData API through Basic Authentication checkbox.**
    - **Access to OData API Audit Log**
    - **Access to Integration Center**
    - **Access to Data Replication Monitor**
10. Under *Administrator Permissions* → *Employee Central API* select the following checkboxes:
    - **Employee Central Foundation SOAP API**
    - **Employee Central HRIS SOAP API**
    - **Employee Central Foundation OData API (read-only)**
    - **Employee Central HRIS OData API (read-only)**
    - **Employee Central Foundation OData API (editable)**
    - **Employee Central HRIS OData API (editable)**
11. Under *Administrator Permissions* → *Metadata Framework* select the following checkboxes:
    - **Admin access to MDF OData API**
    - **Import Permission on Metadata Framework**
12. Under *Administrator Permissions* → *Manage User* select the following checkbox:
    - **Employee Export**
13. Choose *Done*. You will now revert to the *Permission Role Detail* page.
14. Scroll down to section *3. Grant this role to...* and select *Add...*.
15. On the *Grant this role to...* page select *Grant this role to: Permission Group* and select *SAP BestPractices SFAPI User Group*. For the target population, select *Everyone*.
16. Choose *Done*.
17. Choose *Save Changes* to update the role.
18. Log out and log on again as admin user to refresh the assigned role-based permissions.

5.1.3.1 Set API Login Exceptions

1. Log on to the instance of your company.
2. Go to *Admin Center*.
3. Type **`Password & Login Policy Settings`** in the tool search box and select the feature/tool from the list.
4. Choose the link *Set API login exceptions...*.

5. Choose *Add*.
6. In the upcoming window, enter the following settings:

Field Name	Entry Value
Username	The API user, for example SFAPI
Maximum password age (days)	Set to -1 days
IP address restrictions	If you need to restrict IP addresses, consult the Regions page.

7. Choose *Save & Close*.

5.1.4 Enhance Administrator Permission for Monitoring

1. Log on to the instance of your company.
2. Go to *Admin Center*.
3. Type **`Manage Permission Roles`** in the tool search box and select the feature/tool from the list.
4. Search for an existing Administrator role, such as *SFCC Super Admin (EC)*.
5. Open the role.
6. On the *Permission Role Detail* screen, choose the *Permission...* button.
7. Check the following settings:

Administrator Permissions		
Manage Integration Tools	X	Access to SFAPI Audit Log
		Access to SFAPI Data Dictionary
		Admin access to OData API
		Access to OData API Audit Log
		Access to OData API Metadata Refresh and Export
		Access to Data Replication Monitor
Employee Central API	X	Select All
Metadata Framework	X	Admin access to MDF OData API

8. Choose *Done*.
9. Choose *Save Changes*.

5.2 Set up Replication Target System

1. Log on to the instance of your company.
2. Go to *Admin Center*.
3. Type **`Manage Data`** in the tool search box and select the feature/tool from the list.
4. On the *Manage Data* page *Create New: Replication Target System*.
5. Create a new entry based on the following values:

Field Name	Value
External Name	<Description>
External Code	<Logical system of the Employee Central Payroll system> for example: **<ERP-SID>CLNT<CLNTID>**
Relevant for Payroll Integration	Yes

6. Choose *Save*.

> **i** Note
>
> If the Replication Target System node is not available under *Admin Center* → *Manage Data*, enabling Payroll Integration is necessary under Provisioning Access. Refer to SAP Note 2246342 for further details.

6 Permission Roles

The following permission role is delivered as part of this solution.

Role	Description	Permissions	Comment
SAP Best Practices SFAPI User Role	API Login Permission	Permission for API access for Employee Central	

Important Disclaimers and Legal Information

Hyperlinks

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

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

Videos Hosted on External Platforms

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

Beta and Other Experimental Features

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

Example Code

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

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP