SAP SuccessFactors ♡

Integrating SAP SuccessFactors HCM Suite with SAP Task Center

THE BEST RUN **SAP**

Content

1 Process for Setting Up Integration with SAP Task Center

Setting up integration between SAP SuccessFactors and SAP Task Center is a multistep process that requires configuration on both sides of the integration.

Here is an overview of the process:

1. Enable the integration in SAP SuccessFactors, following instructions in this guide.
2. Download a trust certificate from SAP Cloud Platform cockpit, following instructions for SAP Task Center.
3. Register a OAuth2 client application in SAP SuccessFactors, following instructions in this guide.
4. Save the API key generated during the OAuth2 registration.

> ⓘ Note
>
> To view the API key, go to ▶ *Admin Center* > *API Center* > *OAuth Configuration for OData* ▶ and choose *View* on the registered application list.

5. Configure a new destination in SAP Cloud Platform cockpit, following instructions for SAP Task Center.

Integrating SAP SuccessFactors HCM Suite with SAP Task Center
Process for Setting Up Integration with SAP Task Center

PUBLIC   **3**

2 Supported Tasks for Enhanced To-Do Integration

Get an overview of the to-do tasks supported by *Enhanced To-Do Integration*.

Module	Task Type on SAP Task Center	Comment
Opportunity Marketplace	Assignment Offer	
Opportunity Marketplace	Employee Change Requests (Assignment Application)	
Opportunity Marketplace	Employee Change Requests (Assignment Publishing)	
Opportunity Marketplace	Employee Change Requests (Acceptance of Assignment Offer)	
Performance & Goals	Evaluate Performance	
Performance & Goals	Collect 360 Feedback	
Compensation	Compensation Planning	
Recruiting	Interview Assessment	
Recruiting	Offer Approval	
Performance & Goals	Calibrate Ratings and Results	
Employee Central	Foundation Object Change Requests	
Employee Central	Foundation Object Change Requests - Sent Back	
Employee Central	Employee Change Requests	
Employee Central	Employee Change Requests - Sent Back	
Employee Central	MDF Workflow Requests - Employee-Related	
Employee Central	MDF Workflow Requests	
Employee Central	MDF Workflow Requests - Employee-Related, Sent Back	
Employee Central	MDF Workflow Requests - Sent Back	
Employee Central	Time Off Requests	⚠ **Restriction** For employees with a clock-time based profile, SAP Task Center only tracks the time duration, but not the start and end date of the absence. This affects single day absences only, not multiple day absences.

Module	Task Type on SAP Task Center	Comment
Employee Central	Employee Profile Complete	
Employee Central	Temporary Time Information Approvals	
Platform	Job Profile Requests	
Platform	Job Profile Change for My Acknowledgment	
Employee Central	Time Sheet Requests	
Succession Management	Talent Pool Nominee	
Employee Central	Alerts	
Employee Central	Workflow Delegation Request	Part of Auto Delegation
Employee Central	Upcoming Delegation	Part of Auto Delegation
Onboarding	Complete New Hire Tasks	
Onboarding	New Hire Data Review	
Onboarding	Offboard Team Members	
Onboarding	Complete Knowledge Transfer Tasks	
Onboarding	Offboard Team Members	
Onboarding	Perform Rehire Verification	
Onboarding	Complete e-Signing of Employee Documents	
Onboarding	Complete Section 2 and Section 3 of Form I-9	
Succession & Development	Mentor Approval	

3 Enabling Push of Task Updates to SAP Task Center

To enable task updates to be pushed to SAP Task Center, you need to register SAP Task Center in the Integration Service Registration Center in SAP SuccessFactors.

Prerequisites

- You've created a new service instance as described in step 1 under Creating the Primary Destination with the Technical User.

  > ⓘ Note
  >
  > In this step, you get the service key that contains the values required for the Integration Service Registration Center.

- You've enabled Admin Alerts 2.0 in your system. For more information, please refer to Admin Alert Versions.

Procedure

1. In the SAP SuccessFactors system, register SAP Task Center on the *Integration Service Registration Center* page as described under Registering your Tenant for an Integration Service.
2. In the *Integration Service Registration Center*, enter the service key details you received when following the prerequisites for creating a new service instance.

Integration Service Registration Center for SAP Task Center

Required Entries	Details
Destination URL	Copy the "endpoints" > "inbox_rest_url" link from the service key into this field.
	Remove everything that comes after **".com"**.
OAuth URL	Copy the "uaa" > "url" link from the service key into this field.
	Add **"/oauth/token"**.
Client ID	Copy the "uaa" > "clientid" link from the service key into this field.
Client Secret	Copy the "uaa" > "clientsecret" link from the service key into this field.

3. Choose *Register*.

4. Choose *Ok*.

Next Steps

If the registration is not valid, the push of to-do tasks to SAP Task Center fails. In this case, you get an alert in the SAP SuccessFactors system for the ▌ *Admin Alerts 2.0* ⟩ *Domain Event* ⟩ *Failed Domain Events* ▐ alert type. You then need to correct the data on the Integration Service Registration Center page.

4 Registering Your OAuth2 Client Application

Register your client application so that you can authenticate API users using OAuth2. After you register an application, you'll get an exclusive API key for your application to access SAP SuccessFactors OData APIs.

Prerequisites

You have the ▶ *Manage Integration Tools* ❯ *Manage OAuth2 Client Applications* ◀ permission.

Procedure

1. Log into your instance as an administrator.
2. Go to ▶ *Admin Center* ❯ *API Center* ❯ *OAuth Configuration for OData* ◀ and choose *Register Client Application*. You can also access the tool by searching *Manage OAuth2 Client Applications* in Action Search.
3. On the new OAuth client registration screen, enter the following information:

Option	Description
Company	The name of your company. This value is prefilled based on the instance of the company currently logged in.
Application Name	(Required) A unique name of your OAuth client.
Description	(Optional) A description of your application.
Application URL	(Required) A unique URL of the page that the client wants to display to the end user. The page contains more information about the client application. This is needed for 3-legged OAuth, however it isn't currently supported.
Bind to Users	(Optional) You can enable this option to restrict the access of the application to specific users including business users and technical users. ⓘ Note A business user in this context is a user who has permissions to call SAP SuccessFactors APIs for integration purposes. A technical user is a system-generated user created for integrating SAP SuccessFactors with other SAP products and solutions. Refer to About Technical User for more information.

Option	Description
User IDs	(Required if you enabled the *Bind to User* option) Enter the user IDs separated by comma.

The binding of business users and technical users works as follows:

- If you don't bind any user to the application, all business users can request OAuth tokens but technical users can't.
- If you bind both business users and technical users to the application, only these users can request OAuth tokens.
- If you bind only technical users to the application, these technical users and any business user can request OAuth tokens.
- If you bind only business users to the application, only these users can request OAuth tokens.

> ⓘ Note
>
> Contact your system administrator or Technical Support if you don't know the technical user ID of your instance.

Option	Description
X.509 Certificate	(Required) The certificate corresponding to the private and public key used in the OAuth 2.0 authentication process. In this flow, SAP SuccessFactors require the public key and the client application has the private key. To register a client application, you must install the public key in SAP SuccessFactors.

You can obtain a certificate from a trusted service provider, or generate a self-signed certificate using a third-party tool. Either way, the certificate must be encrypted using a secure signature algorithm. Although both RSA-1 and RSA-2 algorithms are supported, we recommend using RSA-2 for better security.

If neither option is available, you can also generate an X.509 certificate in SAP SuccessFactors. If you choose to provide

For more information, see the *Related Information* section of this topic.

> ⓘ Note
>
> For better security, we recommend that you use a self-signed certificate or one from your trusted service provider.

Option	Description
	In a `.pem` file, the X.509 certificate is a BASE64-encoded string enclosed between `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`. Enter only the enclosed string without the beginning and ending lines. Otherwise, an error occurs.
	⚠ Caution When you change or regenerate an X.509 certificate for an application, the existing application client configurations are invalidated. This could lead to application failure until you update the configurations with the new certificate information.

4. Choose *Register* to save your registration.

Results

You've successfully registered your client application for OAuth2 authentication. An API key is generated and assigned to your application. You can view the API key by choosing *View* on the registered application list.

You can also edit, disable, and delete an OAuth2 client registration.

4.1 Creating a X.509 Certificate Using Your Own Tools

You can use tools such as OpenSSL to create an X.509 certificate.

Prerequisites

There are different tools you can use to create X.509 certificates. In this example, we'll show you how to use OpenSSL to create a certificate. For Windows users, download the tool at https://www.openssl.org ↗ . For Mac and Linux users, OpenSSL is available with the native command-line tools such as Terminal.

Context

X.509 certificates are used in many Internet protocols, including TLS/SSL. An X.509 certificate consists of a public key and a private key. The public key contains the identity information, such as a hostname, an organization, or

an individual. The public/private key pair is used to establish secure communication between your application and SAP SuccessFactors.

Procedure

1. Go to the OpenSSL library in your command-line tool.

   For Mac and Linux users, call OpenSSL directly in the command tool under the default path. For Windows users, the entry point is the openssl binary, located in the installation folder, for example: `C:\Program Files\OpenSSL-Win64\bin\`.

2. Use the `openssl` command to create an X.509 certificate. The example below shows how to create a certificate using the recommended SHA-2 signature algorithm:

   ```
   $ openssl req -nodes -x509 -sha256 -newkey rsa:2048 -keyout private.pem -out
   public.pem
   ```

   > ⓘ Note
   >
   > **private.pem** and **public.pem** are the example names of the public/private key pair generated with this command. You can change them to any names of your choice.
   >
   > Although SAP SuccessFactors support certificates signed using either SHA-1 or SHA-2 algorithms, we recommend that you use SHA-2 for better security.

3. Enter the following information when prompted:

   Provide at least one of these values to create a certificate.

Option	Description
Country Name	Enter a two-letter country code of the entity to which the certificate is issued. A country code represents a country or a region. Example: **AU**
State or Province Name	Name of state or province of the entity to which the certificate is issued.
Locality Name	Name of locality of the entity to which the certificate is issued.
Organization Name	The entity to which the certificate is issued.
Organization Unit Name	The organization unit of the entity to which the certificate is issued.
Common Name	The hostname or IP address for which the certificate is valid. The common name (CN) represents the hostname of your application. It's technically represented by the commonName field in the X.509 certificate. The common name doesn't include any protocol, port number, or path. For example: **www.bestrun.com**
E-mail Address	Enter your e-mail address.

Results

A public/private key pair is generated and saved to the local drive with the names you specified in the command.

> **⚠ Caution**
>
> Only the public key is required when you register an OAuth2 client application in SAP SuccessFactors. The private key must be kept secure under all circumstances. Do not share the private key with others. If you lose the private key, you must create a new certificate.

Example of a public key:

```
-----BEGIN CERTIFICATE-----
MIIB9jCCAV+gAwIBAgIUKR82LgtkNBccdypYD26K87zZ+vYwDQYJKoZIhvcNAQEE
BQAwDTELMAkGA1UECwwCRVAwHhcNMTkwOTI2MDIwNDUyWhcNMTkxMDI2MDIwNDUy
WjANMQswCQYDVQQLDAJFUDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwKva
NZCOGcuY90/BudS+qQic+A31uM8mLtmI60R1iEjgEWGBCxSiDb2h8mQJiXwkul9W
ebaazP7hkqkdNoJgV/6NE7++GKyyS8fIhJgeWSb6EelMFhjQ0nZKzbZX5ms3I91n
twzkcHtKCQi/gi/Rouhlk/P/QVcrzSgHUHqJNy0CAwEAAaNTMFEwHQYDVR0OBBYE
FHHbgqnnhm3GAJ4gy2IuEDxpLye7MB8GA1UdIwQYMBaAFHHbgqnnhm3GAJ4gy2Iu
EDxpLye7MA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEAG5CoqcEy
15vUpj5VfJeR/DS70tPIinp/TCC9kRO/++TSnPbqVcfPr8vIyc4L3MPKjXFBsefE
vtfHGGucVtv5N1+4U/b9NxNFbuH2MP7W3swZ4WM72Na+W6iOhwesOr0p3IcOfxc3
RNCnagFmtbDFxAlPXQ0d+m+N5gxLRoCX1hE=
-----END CERTIFICATE-----
```

Example of a private key:

```
-----BEGIN PRIVATE KEY-----
MIICdQIBADANBgkqhkiG9w0BAQEFAASCAl8wggJbAgEAAoGBAMCr2jWQjhnLmPdP
wbnUvqkInPgN9bjPJi7ZiOtEdYhI4BFhgQsUog29ofJkCYl8JLpfVnm2msz+4ZKp
HTaCYFf+jRO/vhisskvHyISYHlkm+hHpTBYY0NJ2Ss22V+ZrNyPdZ7cM5HB7SgkI
v4Iv0aLoZZPz/0FXK80oB1B6iTctAgMBAAECgYAid5vVsUJ6gt2egHobkF97Rbsu
9PBcW1JtVyUTUW/lLYRIF7VKEirbYm0yO4spOTgozx1dMLmIqqAX6ID9W114kN/g
lz1c2/jMg+YGp+FNCjULygjfIwtGfpX8G0qYWza5oarzVbbGA1cvpHjyNMGV7ure
7syrjIXUighkaKrxgQJBAObVbGTVr/5xxScB1mPYoBe02JMyTzuVW0ts7NyfxXJu
w9vUoMDLV+2wuDE4w8/gUkKf26eojn3kwD708V6lG4kCQQDVrVC7HcXYfU4wkr5S
JPMQzAln0RUf6LgFpgIDPDKpq7VUti1A9aQUbddxlcudFjO57ksr2yU9sOLQgh3A
+2GFAkAWkRDavsVI48h5asWR11C3YJe3tDhow848DncNjpUX/dop+JyKnJaJBzjK
nxkNjomcN9KajnD3v9BHl1ytewi5AkA8IAWscUc/kJrUziXhpWYD3vXykYG5Ndm6
NSkx0dmLprZifNSlB7nAyduqqXTe4eVyNxxN3d9PyZs5ArPuno2lAkAQ8WiHbqGA
JlO6R9+D6HiWywpCaQ0oh6H/+84mb1ew2SUw1mFxROxgfsRVNUe+ahs3nSIhoba0
cqS0ZSBtNDxV
-----END PRIVATE KEY-----
```

4.2 Creating an X.509 Certificate in SAP SuccessFactors

You can create an X.509 certificate in SAP SuccessFactors HCM suite if you're unable to create a certificate using your own tools.

Context

> **⚠ Caution**
>
> We don't recommend creating the X.509 certificate in the API Center and downloading the private key. It's a less secure approach because downloading the private key increases the risk of exposing it. Only consider this approach you're unable to create an X.509 certificate using your own tools.

Procedure

1. Log into your instance as an administrator.

2. Go to ▌ *Admin Center* ❯ *API Center* ❯ *OAuth Configuration for OData* ▐ and choose *Register Client Application*. You can also access the tool by searching *Manage OAuth2 Client Applications* in Action Search.

3. On the new OAuth client registration screen, choose *Generate X.509 Certificate* and enter the following information:

Option	Description
Issued By	Value set to `SuccessFactors`
Common Name	The hostname or IP address for which the certificate is valid. The common name (CN) represents the hostname of your application. It's technically represented by the commonName field in the X.509 certificate. The common name doesn't include any protocol, port number, or path. For example: `www.bestrun.com`
Organization	(Optional) The entity to which the certificate is issued.
Organization Unit	(Optional) The organization unit of the entity to which the certificate is issued.
Locality	(Optional) Name of locality of the entity to which the certificate is issued.
State/Province	(Optional) Name of state or province of the entity to which the certificate is issued.
Country	(Optional) Enter a two-letter country code of the entity to which the certificate is issued. A country code represents a country or a region. Example: `AU`
Validity	(Optional) The number of days for which you want the X.509 certificate to be valid. If left empty, the validity defaults to 365 days. ⓘ Note Validity check works only when the *Enable validity check* option is selected.
Enable validity check	Indicates whether or not the system checks the validity of the certificate. If disabled, the certificate never expires. If checked, you can either specify the validity period in days in the *Validity* field, or leave it empty so that the validity defaults to 365 days.

4. Choose *Generate*.

Results

A new X.509 certificate is generated and filled in the *X.509 Certificate* field on the new OAuth2 client registration screen. Continue your registration in Registering Your OAuth2 Client Application [page 8] with this certificate.

> ⚠ Caution
>
> Both the public key and private key are available to you in the generated certificate. You must save the private key before you register your client application. Only the public key is available for viewing when the client application is registered. The private key must be kept secure under all circumstances. Do not share the private key with others. If you lose the private key, you create a new one.

5 Post Refresh Activities for Instance Refresh

Specific post refresh activities for the SAP SuccessFactors integration with SAP Task Center are required if you use the Instance Refresh tool.

Once you receive an email notification with refresh status as *Successful*, you must perform the following activities:

- Configure the Identity Provisioning Service (IPS) user sync so that the new user data is synced to SAP Cloud Identity Authentication Service (IAS). For more information, please refer to Post Refresh Activities.
- Delete the property *inbox.enabled*, and add it again with the value *true* after a couple of minutes.
  This deletes the `Task Cache` and repopulates it for the primary destination. For more information, please refer to Creating the Primary Destination with the Technical User.

6 Change History

Learn about changes to the documentation for Setting Up Integration with SAP Task Center in recent releases.

2H 2023

Type of Change	Description	More Info
Change	We removed the page *Enabling To-Do Task Integration Between SAP Success-Factors and SAP Task Center* because you don't need to upgrade *Enhanced To-Do Integration* anymore. We've also removed references to the *Enhanced To-Do Integration* upgrade center action.	Supported Tasks for Enhanced To-Do Integration [page 4]
Changed	We have moved the Change History to the end of the guide.	Process for Setting Up Integration with SAP Task Center [page 3]

1H 2023

Type of Change	Description	More Info
Change	We removed the page *Reduced Scope* because we now support global assignments and concurrent employments in Employee Central as well as attachments.	
Change	We've added a note that states that debug locales aren't supported.	
Changed	We added new tasks from Opportunity Marketplace.	Supported Tasks for Enhanced To-Do Integration [page 4]

2H 2022

Type of Change	Description	More Info
Change	We added that the permission ▷ *Administrator Permissions* ❯ *Manage Workflows* ❯ *Prevent Quick Approval of Workflow* ❯ hides approve/decline buttons in to-do approval tasks.	

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 an 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.

THE BEST RUN **SAP**