Set-Up Instructions | PUBLIC
SAP S/4HANA
2020-09-17

Setting Up *Social Collaboration Integration* **(1JB)**

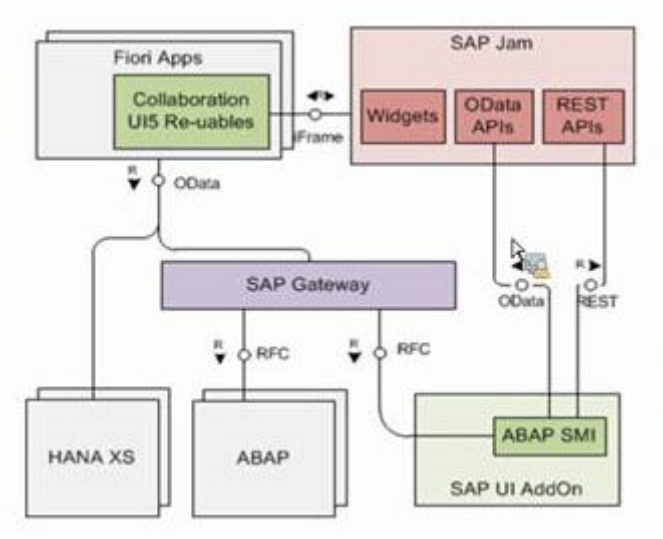
THE BEST RUN SAP

Content

1 Purpose

This document describes additional configuration steps that you must carry out in the productive system on customer site to activate the SAP S/4HANA On-Premise Social Collaboration. As these configuration steps are company-specific, they cannot be delivered by SAP, and must be carried out by the company setting up the SAP solution.

The following figure gives you an overview of the systems and their connection within SAP S/4HANA On-Premise Social Collaboration.



The configuration is divided into two main sections:

- Exchange certificates for trusted connectivity.
- Configure ABAP Social Media Integration (ABAP SMI)

> **i Note**
>
> A constant Internet connection is required to allow the cloud solutions to work properly.

2 Preparation

Before starting with the configuration, it is essential to understand what we want to achieve.

- From a business user perspective, we want to use SAP Jam functionality to facilitate collaboration related to business data from the back-end system directly from the user's SAP Fiori launchpad. This collaboration could entail, for example, sharing directly from SAP S/4HANA in SAP Jam, receiving SAP Jam notifications in the SAP Fiori launchpad, or viewing a SAP Jam group's feed in a specific SAP Fiori app. To achieve this, we require multiple integrations on the application level. From a business user perspective, we want to use SAP Jam functionality to facilitate collaboration related to business data from the back-end system directly from the user's SAP Fiori launchpad. This collaboration could entail, for example, sharing directly from SAP S/4HANA in SAP Jam, receiving SAP Jam notifications in the SAP Fiori launchpad, or viewing a SAP Jam group's feed in a specific SAP Fiori app. To achieve this, we require multiple integrations on the application level.
- We need to provide single sign-on (front-end SSO) between all applications to ensure that users can also navigate to any involved system without having to log in multiple times with various credentials.
- The system landscape must include an ABAP-based SAP S/4HANA on-premise system that supports SAP Jam integration with ABAP SMI.
- User authentication between SAP S/4HANA and SAP Jam requires identical e-mail addresses for users in both systems (see Preparation).
- The SAP Jam administrator tasks are performed in the SAP Jam Administrator console. You can access the Administrator console by selecting Admin from the Welcome drop-down menu.

Before you perform the configuration steps described in the following sections, check that your server URL and the user names are set up.

SAP Jam Server URL

In several procedures in this section, the server URL that you received from SAP Jam Product Support during the licensing process is required. Use it whenever you are requested to enter *<your server URL>*

Example

< https://sapdeviam.sapjam.com/>

User Names

In the standard delivery, the SAP Jam user name corresponds to the email address of the user defined in the back-end system.

We assume that you have registered each user in SAP Jam with a unique email address, since the back-end user will be mapped to this email address in the back-end system to access SAP Jam.

To check whether the SAP Jam user names are present in the user master record of your back-end system, proceed as follows:

1. Run transaction *SU01*.
   The *User Maintenance Initial* screen appears.
2. In the *User* field, enter the *user name*.
3. On the *Address tab*, in the *Communication group box*, verify that a valid address is present in the *E-Mail Address* field.

The default implementation retrieves the data from the user master record. If you want to use a source other than the user master record, set up the user mapping in BAdI CLB2_USER_MAPPIN.

Tenant Host Name of Your SAP S/4HANA On-Premise System

In several procedures in this section, the tenant and host name that you received from SAP Product Support during the licensing process is required. Use it whenever you are requested to enter <tenant hostname>.

Example

<https://myXXXXXX.s4hana.ondemand.com>

2.1 Important Transactions

The following table lists the transactions you should be familiar with when performing the configuration steps for connecting SAP Jam with your business application.

> ⚠ Caution
>
> Make sure that you have the appropriate authorizations.

Transactions and Reports in SAP S/4HANA On-Premise Back-End Systems

Transaction Code	Description
`SE38`	Allows you to execute reports.
`RCLB2_FILL_CUSTOMIZING`	Report that allows you to fill all ABAP SMI Customizing tables and replaces dedicated CLB2 transaction calls such as the following: Service Provider Settings (`CLB2_PLATF`) Application Settings (`CLB2_APPLI_PLATF`) Configuration REST Tunnel (`CLB2_TUNNEL`)
`SAML2`	Allows you to configure SAML2.0 in an ABAPsystem.
`STRUST`	Launches the TrustManager.

For more information about these transactions, see the relevant documentation in your SAP system.

2.2 Basic S/4HANA Configuration – Exchange Certificates

This section describes the tasks you required for basic S/4HANA configuration.

The following steps need to be performed on the front end server.

2.2.1 Enter HTTP Proxy Settings

Communication from a company network with the outside world takes place by means of an HTTP proxy. This section explains how you set up the HTTP service for the communication with SAP Jam.

Procedure

1. In Customizing for *SAP NetWeaver*, choose *UI Technologies* -> *SAP Jam Integration* -> *Define HTTP* Service (or run transaction SICF). The *Define Services* screen appears.
2. Choose *Execute* (F8) without making further specifications.
3. On the *Maintain service* screen, choose *Client* -> *Proxy Setting* (CTRL+F2). The *Proxy Configuration for HTTP Client* screen appears.
4. On the *HTTPS Protocol* tab, in the *Host Name* and *Port* fields, enter the default values that the system uses for proxy access. If you use global defaults, you can leave the *Host Name* and *Port* fields empty.
5. Choose *OK*.

Results

You have entered the HTTP proxy settings.

2.2.2 Exchange SAP Jam Certificate

This section describes how to set up SAP Jam as a trusted system in the back end.

Prerequisite

Ensure SAML2 is activated. To check this, follow the steps below:

1. Run transaction SAML2.
   The SAML 2.0 Configuration of ABAP System screen appears.
2. Choose *Enable SAML2 Support* --> Create *SAML2 Local Provider*

Field Name	Values
Provider Name	Enter the name of your provider. We recommend entering your tenant host name. The provider name is needed later in procedure *Registering Identity Provider*, so it can be entered in the service provider 's company. Change the default by adding a company-specific prefix.
Operation Mode	Enter *Service Provider*.

3. Leave all other wizard settings at their default values.

Context

Procedure in SAP Jam

1. Go to the SAP Jam Web site using the browser of your choice.

> **i Note**
>
> Depending on your browser, the download procedure may vary.
>
> Example: MS Internet Explorer:
> 1. Choose the *lock* in the address bar
> 2. Choose *View certificates*
> 3. Choose *tab Details* -> Copy to file
> 4. Base-64 encoded X.509 (.CER) as the format for the export file

2. View your SSL certificate and navigate to the self-signed root certificate authority (CA).
3. To export the certificate to a base64-encoded file, select *Base-64 encoded X.509 (.CER)* as the format for the export file.

> **⚠ Caution**
>
> You can choose whether you want to use a client certificate or a consumer application certificate. We recommend the consumer application certificate as it has a longer validity (10 years as opposed to three).
>
> You can use dialog report SSF_ALERT_CERTEXPIRE to check the validity period of your certificate. This report allows you to display warnings before the certificate expires. For more information, see the documentation for the report in the system.

Context

In this step, you set up the Secure Sockets Layer (SSL) channel.

Procedure in SAP S/4HANA Back-End System

1. Run transaction STRUST.
   The *Trust Manager* screen appears.
2. In the *dialog structure*, double-click SSL Client (Anonymous).

   > **i** Note
   >
   > The name of the entry in the dialog structure may be slightly different in your system, since it can be named individually during creation.

3. Choose *Import Certificate*.
4. Open the certificate file you saved to a file as described in the previous section.
   The file appears in the *Certificate group box.*
5. Choose *Add to Certificate List*.
   The SAP Jam certificate file appears in the *Certificate List group box*.
6. Save your entries.

Results

You have imported the HTTPS SAP Jam certificate and set up SAP Jam as a trusted system.

2.2.3 Preparing SAML 2.0

To authenticate a user with SAP Jam, the system uses assertion tickets based on Security Assertion Markup Language, version 2.0 (SAML2).

Context

The basic SAML2 authentication flow is as follows:

1. The back-end system is identified to SAP Jam in the form of an Identity Provider (IdP). This happens when you make an entry in a specific company and provide the IdP certificate. This establishes a trust relationship between the back end and SAP Jam.
2. The back-end system provides an assertion that confirms that the specified user has been authenticated in the back-end system.
3. This assertion is sent to SAP Jam. As SAP Jam has a trust relationship with the back end, the user- assuming the user belongs to the company - is considered to be registered.
4. A session ID is issued to identify users to SAP Jam for the next operation.

To set up the identity provider in the current client, follow the procedure below.

Procedure

1. Run transaction `STRUST`.
2. Double-click the *SSF SAML2 Service Provider - S* node. The system displays the details.

   > **i Note**
   >
   > In some systems, this node may be entitled differently, for example, SSF S2SVPS.

3. In the *Own Certificate* group box, double-click the *Subject* field.

   > **i Note**
   >
   > To ensure that you select the correct file, check that the *Subject* field in the *Own Certificate* and the *Certificate group boxes* display identical data. In releases lower than SAP NetWeaver 7.4, the *Subject* field was called *Owner*.

4. Choose *Export Certificate*.
5. In the *Select File* dialog, specify where you want to save the certificate.
6. Select the *Base64* option as the file format.
7. To save the file, choose *Continue*.The *File was saved* message appears.

Results

You have successfully exported the IdP certificate. You will need this certificate later for the procedure *Registering Identity Provider*.

2.2.4 Preparing OAuth SHA1

Normally, the application-based OAuth requires a consumer key and secret to be stored in the back-end system for each external application ID. The *external application ID* is the technical representation of the SAP Jam's OAuth client in the back-end system.

ABAP SMI, however, uses a variant that replaces the secret with a SAML assertion, similar to the SAML 2.0 authentication scenario. For this approach, only one entry is necessary in Secure Store and Forward (SSF), and no secrets need to be stored here. The consumer key for each application still needs to be set up.

A client based on OAuth (2-legged or 3-legged) is required by some administrative APIs that are run in an application. By default, RSA-SHA1 is used for encryption.

As part of the standard delivery, the SSF application exists in the system with the name CLBOAU (= CoLlaBoration OAuth) and the parameters mentioned inCreating an SSFA Instance for OAuth [page 10]

- If it is missing for any reason, follow the procedure *Creating an SSFA Instance for OAuth*, before you complete section *Issuing Certificates for SSF CLBOAU (OAuth)*.
- If you see the entry *SSF Collaboration Integration* in the dialog structure on the *Trust Manager* screen, skip section *Creating an SSFA Instance for OAuth*, and continue with section *Issuing Certificates for SSF CLBOAU (OAuth)*.

2.2.4.1 Creating an SSFA Instance for OAuth

This section describes how to create an instance of the SSFA application type CLBOAU.

Context

The entry CLBOAU should be available in the system as it is part of the standard delivery. You only should perform this procedure if it is unavailable.

Procedure

1. Run transaction STRUST.
   The *Trust Manager screen* appears. You see the SSFA application you created in the dialog structure.
2. To create a new Personal Secure Environment (PSE), right-click the *SSFA entry*, and choose *Create*.
3. Complete the fields as follows:

Field Name	Values
Name	Enter **`SSF Collaboration Integration`**.
Algorithm	Select **`RSA`**.

4. Save your entries.

Results

You have created the SSFA with the name CLBOAU. To issue the certificate, continue with sectionIssuing Certificates for SSF CLBOAU (OAuth) [page 10]

2.2.5 Issuing Certificates for SSF CLBOAU (OAuth)

This section describes how to issue the `SSF CLBOAU` certificate.

Prerequisites

The SSF application type CLBOAU exists in the system or you have created it as described in Creating an SSFA Instance for OAuth.

Procedure

1. Run transaction `STRUST`.The *Trust Manager* screen appears.
2. In the dialog structure, double-click the *SSF Collaboration Integration* node.The system displays the details.
3. In the *Own Certificate* group box, double-click
4. Choose *Export Certificate*.

> **i** Note
>
> The *Subject* field in the *Own Certificate* and the *Certificate* group boxes must contain identical data.

5. In the *Select File* dialog, specify where you want to save the certificate. Make sure to select the *Base64* option as the file format.
6. To save the file, choose *Continue*.The *File was saved* message appears.

Results

You have retrieved the SSF certificate. You will need the certificate later for procedure *Setting Up the OAuth Client* in SAP Jam.

2.3 Configuring SAP Jam

This section describes how to set up SAP Jam to trust your application as a SAML Identity Provider. It also describes how to set up the OAuth client in SAP Jam so that the application users can make status posts to SAP Jam from within your application.

Prerequisites

- You have completed the configuration tasks described in Basic Back-End Configuration.
- You have the authorization of a company administrator in SAP Jam.

2.3.1 Registering Identity Provider

In SAP Jam, each back-end system and client you want to connect must be published as an identity provider (IdP).

Prerequisite

You have the IdP certificate file in your current client as described inPreparing SAML 2.0 [page 8]

Context

This section describes how to register your identity provider in SAP Jam.

Recommendation

Apply the following naming convention:

<tenant host Name> Example https://myXXXXXX.s4hana.ondemand.com

Procedure

1. Log on to SAP Jam as a company admin.
2. From the *Admin* menu, choose *Integrations* => *SAML Trusted IDPs*.
3. On the *SAML Trusted IDPs* screen, choose *Register your SAML Trusted IDP*.
   The *Register a New SAML Trusted Identity Provider* screen appears.
4. To register the identity provider that you created in the back-end system, enter the following values:

Field Name	Values
IDP ID	Enter the provider name you assigned in the back-end system(Preparing SAML 2.0 [page 8]). The names in SAP Jam and in the back end must be identical. Enter your **<tenant hostname>**. Example https://myXXXXXX.s4hana.ondemand.com
*X509 Certificate (Base64) **	Paste the SAML signing certificate into the text box. This is thebase64-encodedfile you saved as described in section Preparing SAML 2.0 [page 8]
Enabled	Enable the checkbox to specify that SAML assertions will be accepted from this IdP.
Administrative Area	Choose *Company*.

5. Choose *Register*.

Result

You have authenticated your application for SAP Jam using a SAML2 assertion.

2.3.2 Setting Up the OAuth Client

This step describes, how to register your application as an OAuth client in SAP Jam.

Context

You have to register each application that you want to use for each SAP system and client.

Procedure

1. Log on to SAP Jam as a company admin.
2. On the *Admin* screen, choose *Integrations* > *OAuth Clients* > *Add OAuth Clients*.
   The *Register a New OAuth Clients* screen is displayed.
3. On the *Register a New OAuth Clients* screen, enter the following data:

Field Name	Value	Description
Name	**<tenant hostname>**, for example: **https://myXXXXXX.s4hana.ondemand.com**	In the back-end system, this application is linked with the application you specify in the report in the procedure *Run the ABAP SMI Customizing Report* in the field *External Application ID*.
Integration URL	**http://www.acme.com**	Enter your company domain, for example, the link to the homepage of your company or an application.
X509 Certificate(Base64)	**<SSF OAuth certificate>**	To use RSA-SHA1 signatures for calls in the application context, paste the SSF OAuth certificate into the text box. This is the base 64-encoded file you saved as described in section Preparing OAuth SHA1 [page 9]. If you leave this field blank, SAP Jam supplies a consumer secret as the result. With it, you can use either PLAINTEXT or RSA-HMAC instead of RSA-SHA1.

4. Save your entries.

> **i Note**
>
> You need the generated OAuth key from SAP Jam for the procedure in section Configuring ABAP SMI [page 14]. To copy the OAuth key, display the details of the OAuth client that you saved, choose *View* and copy the key.

Result

You've registered your application as an OAuth client in SAP Jam.

2.4 Configuring ABAP SMI

This section describes how to configure ABAP SMI in the SAP S/4HANA on-premise back-end system.

> ⚠ Caution
>
> The back-end system you have to configure for the installation of SAP Fiori apps is the SAP Fiori ABAP front-end server, usually co-deployed with the SAP
>
> NetWeaver Gateway server.

These Customizing settings could not be preconfigured by SAP as they are specific to each customer system and client. You have to customize your local server and application settings.

Prerequisites

You have completed the configuration tasks described in the following sections:

- Basic Back-End Configuration - Exchange Certificates.
- Configuring SAP Jam.

2.4.1 Run the ABAP SMI Customizing Report

Prerequisites

You have completed the steps described inBasic Back-End Configuration - Exchange Certificates.

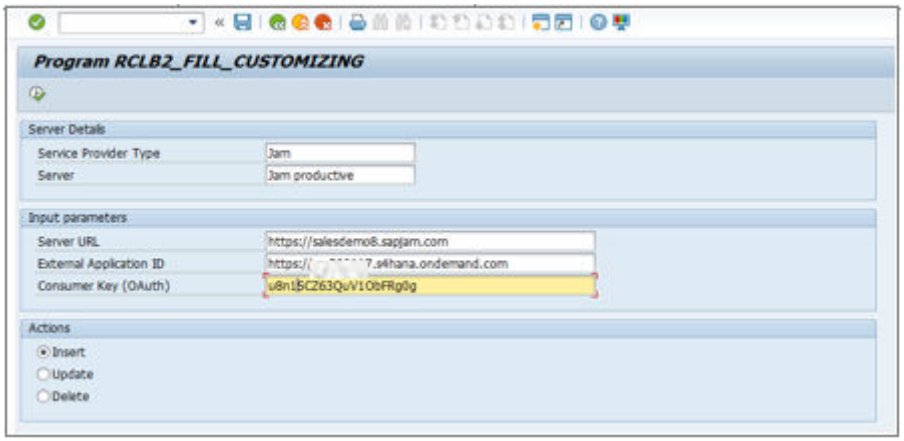
Context

Perform this step for each server to which you want to connect.

Procedure

1. Run transaction /se38.
2. Enter the program name `RCLB2_FILL_CUSTOMIZING` and press F8 or choose *Execute*. The *report* screen appears.
3. Complete the fields as follows:

Field	Value	Description
Service Provider Type	**Jam**	
Server	**Jam productive**	
Server URL	**<SAP Jam servername>**	Enter the SAP Jam server, for example, **https://salesdemo8.sapjam.com**.
External Application ID	**<tenant hostname>**	Enter the external application ID that you used for the client registration in SAP Jam. We recommend the following format: **<tenant hostname>**
Consumer Key (OAuth)	**<OAuth key>**	Enter the key you retrieved from SAP Jam when the OAuth client was saved.
Action	**Insert**	Choose *Insert* to fill all corresponding ABAP SMI Customizing tables.



Choose *Execute (F8)*.

Result

The connectivity between SAP Jam and the SAP S/4HANA on-premise system is now set up. Note that the integration will only work if users have identical email address assigned in both systems (SAP S/4HANA and SAP Jam).

2.5 Optional: Enabling profile picture in Fiori launchpad and create remote catalog.

To use the integration in the SAP Fiori launchpad, you need to do the following:

- If User profile picture in Fiori launchpad is not shown after upgrade,

follow SAP Note: https://launchpad.support.sap.com/#/notes/0002644609

Additional information:

https://help.sap.com/viewer/a7b390faab1140c087b8926571e942b7/7.52.2/en-US/81c29d0060014c2d857015b91dc8f9cc.html

https://help.sap.com/viewer/a7b390faab1140c087b8926571e942b7/7.52.2/en-US/6107ee41f89a43c9af0aa279fe039cca.html

- Create a remote catalog
- http://help.sap.com/saphelp_uiaddon10/helpdata/en/8a/16cbefad40430a872767400a913baa/content.htm
- Assign the catalog to a role
- http://help.sap.com/saphelp_uiaddon10/helpdata/en/ef/1293f3b19d4756bc08535bd30f3786/content.htm

3 Appendix

3.1 Ticket Component

In case of issues during the configuration, open an SAP support ticket for the following component.

Component	Comment
CA-UI2-AR-SM	Social Media Collaboration

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.

Gender-Related Language

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

www.sap.com/contactsap

THE BEST RUN SAP