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

Setting Up *Supplier Quote Automation with SAP Ariba Commerce Automation* **(1L2)**

THE BEST RUN SAP

Content

1 Purpose

The purpose of this document is to describe the required technical configuration for the integration of SAP S/4HANA system with the Ariba network. You need to configure the settings described in this guide manually after the automated installation process is completed. This document describes the setup of direct connection between SAP S/4HANA and the Ariba network (without using middleware).

Once you completed this configuration guide, you will need to make some more settings in both, the SAP S/4HANA system and the Ariba network buyer account that are described in the document "Ariba Spot Quote OP Process Integration Configuration - Customer Tasks". For more information, see the *Administration Guide for the Implementation of SAP S/4HANA, on premise edition* which is linked in the content library (included in the documentation package).

For Software products and versions prerequisites please refer to SAP Best Practices for SAP S/4HANA (on premise)  .

2 Preparation

2.1 How to Use this Guide

For your convenience and to facilitate your work with this electronic document it has introduced several Text Form Fields. These fields can be used to store your individual system landscape and scenario integration configuration information details. This data is used in the following step-by-step descriptions automatically to enhance the readability of this document.

These fields are marked with and are highlighted in grey

Example field	Text Form

To change and update the fields proceed like this.

Procedure

1. Double-click on the highlighted “Text Form” field.
2. In the Text-Form Field Options dialogue, change the Default Text to meet your specifications.
3. Click on Ok.
4. Select whole document with shortcut `Ctrl+A`
5. Update whole document with shortcut `F9.`
6. Accept all pop-up dialogues with **Ok**.
7. Repeat steps 4 - 6 on any changed from field.

2.2 Installation Data

Fill in the following information:

Authorizations Ariba Network		
AN ID	<ANXXXXXXXXXXX>	
User Agent	<sample.buyer@ariba.com>	
SAP S/4HANA information		
SAP S/4HANA Information	System ID	<S4 System ID>

Authorizations Ariba Network		
	Client	<S4 Client >
	Instance Number	< Instance Number >
	Host	ldciqe4.wdf.sap.corp

3 Direct connectivity setup

3.1 Security Setup

When sending a cXML message to Ariba Network, the sender must authenticate itself. Ariba Network offers different authentication methods (authentication with client certificate or Shared Secret password) that are also supported by the add-on.

For direct connectivity, the SAP S/4HANA system always opens the connection by executing the following actions:

- Push of cXML messages to Ariba Network (synchronous)
- Polling Agent which fetches pending messages from Ariba Network (synchronous)

The on-premise component opens the connection to the Cloud, thus supporting the highest level of security. A proxy or reverse proxy in the demilitarized zone (DMZ) is not required.

SAP S/4HANA system communicates with Ariba Network through the HTTPS protocol, encrypting transmitted data.

3.1.1 SSL Connection Setup

1. If you opted for shared secret authentication, please continue with step 4. If you have opted for client certificate authentication, you need to create a new identity. To create a new identity, on the *Trust Manager* screen, choose *Environment* > *SSL Client Identities* .(Information: You have to create a new Identify)
2. On the *SSL Client Identities of System Overview* change view, create the following settings:

Field Name	User Action and Values
Identity	**ARIBA**
Description	**Ariba Network Client**

3. Save your entries and go back twice.
4. For HTTPS SSL encryption, go to https://buyer.ariba.com and download the server certificate from Ariba using your browser.
5. For example, if you are using Internet Explorer, click on the padlock and then click *View Certificates.*
6. On the *Details* tab page, choose *Copy to File* and export it in the Base-64 encoded X.509 format.
7. To import the server certificate into the SAP S/4HANA system, select the relevant SSL Client entry, navigate to the *Certificate* group box and choose *Import certificate*.
8. If you opted for client authentication, please select the created ARIBA entry.
9. If you opted for shared secret authentication, please select the SSL Client (Anonymous) entry.
10. To add the imported certificate to the certificate list, choose the *Add to Certificate List* button.

11. Restart the Internet Communication Manager (ICM) to make the changes active.

1. To access the ICM monitor, choose *Administration* > *System Administration* > *Monitor* > *System Monitoring* > *ICM Monitor.* You can also access the ICM monitor using transaction **SMICM**. Restart the ICM in the ICM monitor by choosing *Administration* > *ICM* > *Restart* > *Yes*. For more information, see Using the ICM Monitor.

3.1.2 Authentication via Shared Secret

Proceed as follows:

Maintain the Shared Secret password in the Define Credentials for Ariba Network Customizing activity. For more information, see Add-On Customizing.

1. The Shared Secret password is stored in the secure storage ABAP DB in SAP S/4HANA system.
2. The add-on supports a Shared Secret password for Ariba Network with a maximum length of 36 characters.
3. Note that for authentication with Shared Secret password, the Shared Secret password has to be provided in the Sender element of the cXML payload.
4. According to security requirements, passwords must not be written to logs, protocols or traces. Therefore, the Shared Secret password is not visible in transactions such as **SXMB_MONI** where the XML message monitoring and tracing takes place since business users can also have authorization for message monitoring transactions. However, when you activate an Internet Communication Framework (ICF) recording using transaction **SICF**, the system logs the Shared Secret password in the corresponding ICF trace. This is acceptable as far as security is concerned because the ICF recording is only for administrators and requires the S_ADMI_FCD authorization.
5. In the profile of your account in the Ariba Network, select the Shared Secret authentication method in the cXML setup.

3.1.3 Authentication via Certificate

If you opted for shared secret authentication, please skip this step.

Prerequisite

1. Get the client certificate from a Certification Authority (CA) which is trusted by Ariba.When you purchase a signed digital certificate, it must refer to an organization that is trusted by Ariba Network. You can use a digital certificate issued by any issuing organization, however it must reference a root certificate from a trusted Certificate Authority.
2. Import the private key of the certificate into the SAP S/4HANA system by using Trust Manager (transaction **STRUST**)
   Only certificates in Personal Security Environment (PSE) format can be imported with Trust Manager. Certificates in other formats must first be converted into PSE format. The conversion can be done using the

command line tool `SAPGENPSE`. The tool can be installed with SAP Cryptographic Library installation package. For more information, see SAP Cryptographic Library Installation Package.
For example, to convert from P12 (Public-Key Cryptography Standards) format to PSE, enter the following command line:
sapgenpse import_p12 -v -r **<root certificate>** -p **<Target PSE file><Source File>**

Procedure

1. On the *Trust Manager* screen, choose *Environment* > *SSL Client Identities*.
2. To import the *.pse file with private key of the certificate in Trust Manager, mark the created Ariba SSL Client entry, and from the menu bar, choose *PSE* > *Import*.
3. Enter the password for the certificate, if required.
4. Save your *.pse file by choosing *PSE* > *Save as* > *SSL Client*, and enter **ARIBA** as the SSL Client.
5. Navigate to the *Own Certificate* group box on the *Trust Manager* screen, and double-click the certificate to add it to the certificate list.
   The certificate is displayed in the certificate list.
6. To import the root certificate into the SAP S/4HANA system, select the created Ariba SSL Client entry, navigate to the *Certificate* group box and choose *Import certificate*.
   To add the imported certificate to the certificate list, choose the *Add to Certificate List* button.
7. Restart the Internet Communication Manager (ICM) to make the changes active.
   To access the ICM monitor, choose *Administration* > *System Administration* > *Monitor* > *System Monitoring* > *ICM Monitor.* You can also access the ICM monitor using transaction **SMICM**. Restart the ICM in the ICM monitor by choosing *Administration* > *ICM* > *Restart* > *Yes*. For more information, see Using the ICM Monitor.
8. Configure the Web services in SOA Manager (transaction **SOAMANAGER**). For more information about setting up the SOA Manager, see the documentation in the SAP Help Portal: Configuration of SOA Manager.
   Follow the steps described in the documentation and find the consumer proxies: *cXMLSynchronousOutboundAdapterMessage_Out* (`CO_ARBFND_PRX_OADP_OUT`) and *cXMLGetPendingDataRequest_Out* (`CO_ARBFND_PRX_GPDQ_OUT`). The definition of this consumer proxies is described in
   Define Outbound Services (Consumer Proxy) [page 15]
   1. In the *Details of Consumer Proxy* group box, navigate to the *Configurations* tab page, select the logical port.
   2. In the *Configuration of Logical Port* group box, navigate to the *Consumer Security* tab page, choose the *X.509 SSL Client Certificate* radio button, and enter **Ariba** in the *SSL Client PSE of transaction STRUST* field.
9. In the profile of your account in the Ariba Network, select the *Certificate* authentication method in the cXML setup and enter the public key of the certificate.

3.2 Configuration of RFC Connections

Use

We recommend that you establish an **SM59** connection to Ariba Network - just to be able to ping the network and check technical reachability.

Before proceeding, it is important that you have uploaded the AN-Certificate SSL Connection Setup [page 7]

For that you have used the transaction **STRUST**.

For HTTPS SSL encryption, you first have to get the server certificate from Ariba and then import it into the SAP S/4HANA system using Trust Manager (transaction **STRUST**).

Procedure

Access the activity using one of the following navigation options:

Transaction Code	**SM59**
IMG Menu	*Tools* > *ALE* > *ALE Administration* > *Runtime Settings* > *Maintain RFC Destinations*

1. On the *Configuration of RFC Connections* screen, select *HTTP Connections to External Server* and choose *Create*.
2. On the *RFC Destination* screen, create the following settings:

Field Name	User Action and Values
RFC Destination	For example, **ARIBA_PROD_TEST**
Connection Type	**G (HTTP Connection to External Serv)**
Description	For example, **Connection to Ariba productive system**

3. Choose *Enter.*
4. Create the following settings on the respective tabs:

Technical settings	
Target host	**<Target host system>**, for example, **service.ariba.com**
Service No.	**<System ID>**, for example, **443**

Technical settings	
Path Prefix	For example, **`/ANSapGateway.aw/ad/cXML`**
Proxy Host	**`proxy`**
Proxy Service	**`8080`**
Proxy User	
Proxy PW Status	
Logon with User	Select the *Do Not use a User* radio button.
Logon with Ticket	Select the *Do Not Send Logon Ticket* radio button.
Security Options	
SSL	Select the *Active* radio button.
SSL Certificate	Choose ANONYM SSL Client (Anonymous).

5. Save your entries.

3.3 Manage and Test Enterprise Services (SOA)

Check and Initial Run SRT_ADMIN

Procedure

Log on to Client '000'. Attention: This is essential.

Access transaction **`SE38.`**

In the *Program* field, enter report name **`SRT_ADMIN`** and choose *Execute*.

If one of the following fields are initial, run this report (without changing the other selection criteria):

Name of ABAP Connection

Name of Inbound Destination

Choose *Execute.*

Alternative approach:

1. In the SAP S/4HANA system, access transaction **SRT_TOOLS**.
2. On the *SOA Runtime Tools* screen, expand *Technical Configuration* and double-click *Technical Configuration of SOAP Runtime*.
3. On the *Technical Configuration of SOAP Runtime* screen, select the following radio buttons:
   - *Automatic Setup*
   - *Run Technical Setup*
4. Choose *Execute (F8)* to start the configuration.

If you do not have enough authorizations, a result can look like this:

```
Technical Configuration of SOAP Runtime

Configuration not successful

No administration authorization

Authorization for object S_USER_SAS missing

Authorization for object S_USER_AGR missing

Authorization for object S_RFC_ADM missing
```

If you have all the necessary authorization, the result should be:

```
Technical Configuration of SOAP Runtime

Configuration performed successfully

Generated password for user DELAY_LOGON: #V5} gdU/J$L[xpnpN9s=2kB7${Ds)6<DEX&6HfEY

User DELAY_LOGON created

Configuration for WS Security logon created

Service user 'DELAY_LOGON' is consistent

Service user created: SAP_WSRT

Role SAP_BC_WEBSERVICE_SERVICE_USER assigned to service user: SAP_WSRT

Service destination WS_SRV_SAP_WSRT783 created/confirmed

Technical setup successfully processed

Profile for role SAP_BC_WEBSERVICE_SERVICE_USER generated and activated
```

3.3.1 Initial Run in Customizing Client

Log on to the Customizing Client, for example, client 100, and run the report **SRT_ADMIN** (without changing the selection criteria).

> **i** Note
>
> **Run in more clients**

You have to run this report in all clients with cXML exchange.

3.3.2 Define bgRFC Supervisor Destination

Use

> **i Note**
>
> It is sufficient to carry out this step only once in a system.

In this activity, you define a supervisor destination for the background RFC (bgRFC). Using the supervisor destination, the system retrieves the configuration settings for the bgRFC scheduler and starts or stops the schedulers as required on each application server.

With the supervisor destination, the system connects to the Ariba Network (AN) to find the right object and update it.

Inbound destination refers to a destination within your system rather than an external system that is called. The destination can be used later in the update report `ARBERP_BUS2081_EXTRACT_STS_UPD` (in the *bgRFC Inbound Destination* field).

Prerequisite

Your IT administrator has defined an RFC destination (ABAP Connection) in transaction **SM59**, for example, with the name *BGRFC_SUPERVISOR*.

Ensure that the following prerequisites are fulfilled:

- In client 000 of your SAP S/4HANA system, you have created a bgRFC supervisor user (with the user type *Service*) in transaction *User Maintenance (**SU01**)*, for example, user *BGRFCSUPER*. You have assigned the Authorization Role for bgRFC Supervisor User (SAP_BC_BGRFC_SUPERVISOR) to the user *BGRFCSUPER*.
- In transaction *Configuration of RFC Connections (**SM59**)*, you have created a bgRFC supervisor destination, for example, destination BGRFC_SUPERVISOR, with the following settings:
- Connection Type: **3 (ABAP Connections)**
- On the *Technical Settings* tab, you have left the *Target Host* field empty. This has the effect that the RFC connection is used within the system where you have created it.
- On the *Special Options* tab, you have specified the transfer protocol *Classic with tRFC*.

For more information, see SAP Help Portal at http://help.sap.com/nw70 ▶ *Application Help* ▶ *Function-Oriented View* ▶ *SAP NetWeaver by Key Capability* ▶ *Application Platform by Key Capability* ▶ *Platform-Wide Services* ▶ *Connectivity* ▶ *Components of SAP Communication Technology* ▶ *Classical SAP Technologies (ABAP)* ▶ *RFC* ▶ *Queued Remote Function Call (qRFC)* ▶ *bgRFC (Background Remote Function Call)* ▶ *bgRFC Configuration* ▶ *Creating a Supervisor Destination. / Creating Inbound Destinations* ▶

Procedure

1. Access the activity using the following navigation option:

Transaction Code	**SBGRFCCONF**
IMG Menu	*Integration with Other SAP Components* > *Business Network Integration Integration with the Ariba Network* > *Framework Settings* > *Direct Connectivity Settings* > *Define bgRFC Supervisor Destination*

2. On the *bgRFC Configuration* screen, navigate to the *Define Inbound Dest.* tab and create a new destination. Choose any name, for example, **ARBERP**.
3. Choose *Save*.
4. Navigate to the *Define Supervisor Dest.* tab and specify the supervisor destination that you have created before (**SM59**).
5. On the *Scheduler: App. Server* tab, enter all application servers that exist in your system landscape.
6. Save your entries.

3.3.3 Generate Jobs

Use transaction **WSIDPADMIN**, do not change selection criteria and schedule these jobs.

Results are the following information messages:

- Job SAP_BC_IDP_WS_SWITCH_BD scheduled
- Job SAP_BC_IDP_WS_SWITCH_BDID scheduled

3.3.4 Check the Results of Your Technical Settings

Procedure

1. Access transaction **SE38**.
2. In the *Program* field, enter report name **SRT_ADMIN** and choose *Execute*.(Alternatively, you can use transaction code **SRT_TOOLS**).
3. Before you start this report, select the *Check Technical Settings* checkbox.
4. Choose *Execute*.
5. On the *Check Administration Environment of SOAP Runtime* screen, select the *Check specific client* radio button, enter your client number, and choose *Execute* to start again.

Result

You receive a green status for all areas. Attention: This is essential.

3.4 Define Outbound Services (Consumer Proxy)

Procedure

1. Access the activity using the following navigation option:

Transaction Code	**SOAMANAGER**
IMG Menu	*Integration with Other SAP Components* > *Integration Component for Ariba Network* > *Framework Settings* > *Direct Connectivity Settings* > *Manage and Test Enterprise Services*

2. *SOA Management (<Systemname;Client>)* opens in a separate window. On the *Service Administration* tab, choose the link to *Web Service Configuration*. All services have to be defined in this interface.
3. On the *Web Service Configuration (<Systemname; Client>)* view, click on the *Design Time Object Search* tab, enter the following search criteria and choose *Search* to start the search:

Field Name	User Action	Values
Object Type	**is**	**Consumer proxy**
Object Name	**contains**	**CXML***

The system brings up the outbound services. A configuration only has to be done for the services which exhibit a direct communication with the AN.
Services communicating directly with the AN.
   - The service named CO_ARBFND_PRX_GPDQ_OUT is the Polling Client's outbound service that exchanges data with the AN (synchronously).
   - The service named CO_ARBFND_PRX_OADP_OUT is the synchronous Outbound Adapter's outbound service that sends outgoing messages to the AN.

4. Select service `CO_ARBFND_PRX_GPDQ_OUT` (Outbound Service from the Polling Client). Show and click *Internal Name*.
5. Under *Details of Consumer Proxy: CO_ARBFND_PRX_GPDQ_OUT*, go to the *Configurations* tab and choose *Create - Manual Configuration.*
6. In the guided configuration, you have to do several steps:
   - Step 1 *Logical Port Name*: Make the following entries and choose *Next*

Field Name	User Action and Values
Logical Port Name	**ARIBA_GATEWAY**
Description	**ARIBA GATEWAY Polling Client**
Logical Port is Default	**Select this Check-box**

- Step 2 *Consumer Security:* Select the *User ID/Password* checkbox and choose *Next*
- Step 3 *HTTP Settings*: In the *Transport Binding Box*, create the following settings:

Field Name	User Action and Values
URL Access Path	For example, **/ANSapGateway.aw/ad/cXML**
URL Protocol Information	**HTTPS**
Computer Name of Access URL	
Port Number of access URL	**443**
Name of Proxy Host	**<Enter the name of your Proxy Host>**
Port Number of Proxy Host	**<Enter the Port Number of your Proxy Host>**
Make Local Call	**No Local System Call**
Compress Response	**False**

7. Repeat the previous steps for service `CO_ARBFND_PRX_OADP_OUT`.

3.5 Activate Business Transaction Events to Trigger Messages

Use

In this Customizing activity, you can activate a set of Business Transaction Events (BTEs) to record changes made to invoices in SAP S/4HANA. A job that you schedule for report *Extract Incoming Invoices relevant for StatusUpdateRequest* (ARBERP_BUS2081_EXTRACT_STS_UPD) sends the information about the changes to Ariba Network in the InvoiceStatusUpdate cXML message.

If you select the *Application Active* checkbox, the system can process all alternative function modules assigned to this Business Transaction Events (BTEs).

1. Access the activity using the following navigation option:

Transaction Code	**SPRO**
IMG Menu	*Integration with Other SAP Components* > *Integration Component for Ariba Network* > *Application Specific Settings* > *Define Message Output Control*

2. On the *Select Activity View "Activate Business Transaction Event to Trigger Invoice Status Message": Overview* screen, choose *New Entries* and create the following settings:

Application Indicator	Active	Text
ARBERP	**X**	**Ariba Integration**

3. Save your entries and go back.

3.6 Activate Application Interface Framework

Use

SAP Application Interface Framework (SAP AIF) may be used to monitor the Ariba Network integration.

Procedure

1. Start transaction **/AIF/SETUP**.
2. Make the following settings:

Field Name	User Action and Values
Test Mode	
Check Number Ranges	**X**
Check Delivery Customer	**X**
Check Engine IDs	**X**
Check Views	**X**

Field Name	User Action and Values
ALV Grid Output	**X**

3. Click *Execute (F8)*.
4. A business set is provided to configure the AIF integration:

Transaction Code	**SCPR20**
IMG Menu	*SAP Menu* > *Tools* > *Customizing* > *Business Configuration Sets* > *Activation of BC Sets*

5. On the *Business Configuration Sets: Activation* screen, enter BC set "/AIF/BNARB_1610" and click "*Activate BC Set (F7)*"

3.7 Define Interface Determination for Proxy Interface

Use

In addition to activating the BC-Set you have to configure the Interface Determination in AIF.

Procedure

1. Access the activity using the following navigation option:

Transaction Code	**SPRO**
IMG Menu	*Cross Application Components* > *General Application Functions* > *SAP Application Interface Framework* > *System Configuration* > *Interface Determination* > *Interface Determination for Proxy Interfaces*

2. On the *Change View "Define Determination Key": Overview* screen, choose *New Entries* and create the following settings:

Proxy Class Name	Field Category	Field Name
CL_ARBFND_PRX_OADP_IN	P - Field from proxy-generated structure	MESSAGE_TYPE

3. Save your entries.

4. Choose *Assign Interfaces* from the *Dialog Structure*, choose *New Entries* and create the following settings:

Proxy Class	Val. No	Operator	Value	Namespace	Intf. Name	Intf. Vers
CL_ARBFND_PRX_OADP_IN	10	Equal	Quote Request	/BNARB	QTEQ_SOUT	1

5. Save your entries and go back.

4 SAP Cloud Platform Integration setup

This chapter is only relevant if the connection to Ariba Network is made using SCP.

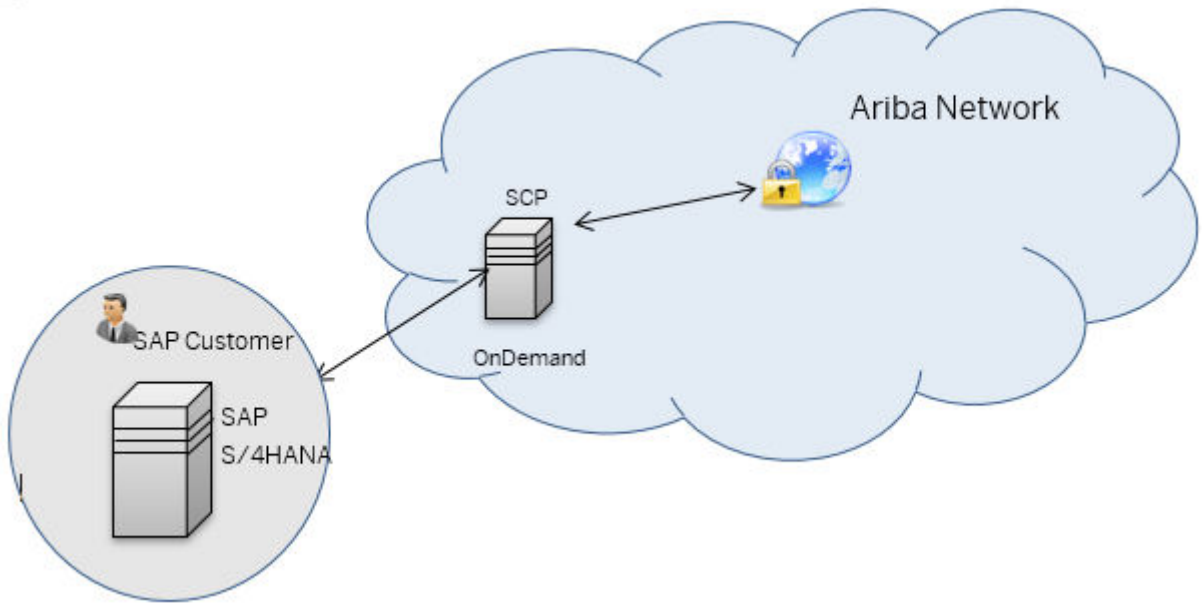
> **i** Note
>
> Before you configure the steps described in this section you need to finish the basic configurations described in chapter *Direct connectivity setup*

4.1 Prerequisites

The purpose of this section is to describe how the connection between the application system SAP S/4HANA system and the SCP tenant can be set up. A successful setup of this connection allows sending extracted data to the SCP tenant, which will then replicate the data to Ariba Network.

This chapter is only relevant if you connect to Ariba Network via SCP!

> **i** Note
>
> The steps described in this section must be performed only when the connection setup between the SAP S/4HANA and the SCP Tenant does not exist. If such a connection has already been set up, you can skip this section.



To connect an application system (in this case SAP S/4HANA) to the SCP tenant, the following information must be available for the application system:

Field	Data	Comments
SID	for example, EC6	3 coded system-ID from the SAP S/4HANA system which contains the source data
Client	for example, 120	The client in the system-ID (SID) which contains the source data

> **i Note**
>
> This set of information is unique for every system (productive, test, development).

For SCP Tenant, the following information must be provided:

Field	Data
Tenant ID	for example, avlb032
Tenant Ops URL	for example, https://tmvb008avlb032avtvlb-avlb032.hana.ondemand.com
Worker node URL	for example, https://iflmapvb008avlb032avtvlb-avlb032.intaas.hana.ondemand.com

> **i Note**
>
> To get access to the tenant, an authorization via SCN user is needed, to develop and deploy the scenarios and to deploy the keyStore.

4.1.1 Partition of Tasks

The detailed sequence of tasks depends on the desired communication security level and is explained in a separate topic. In general, tasks are partitioned between the customer and SAP as follows:

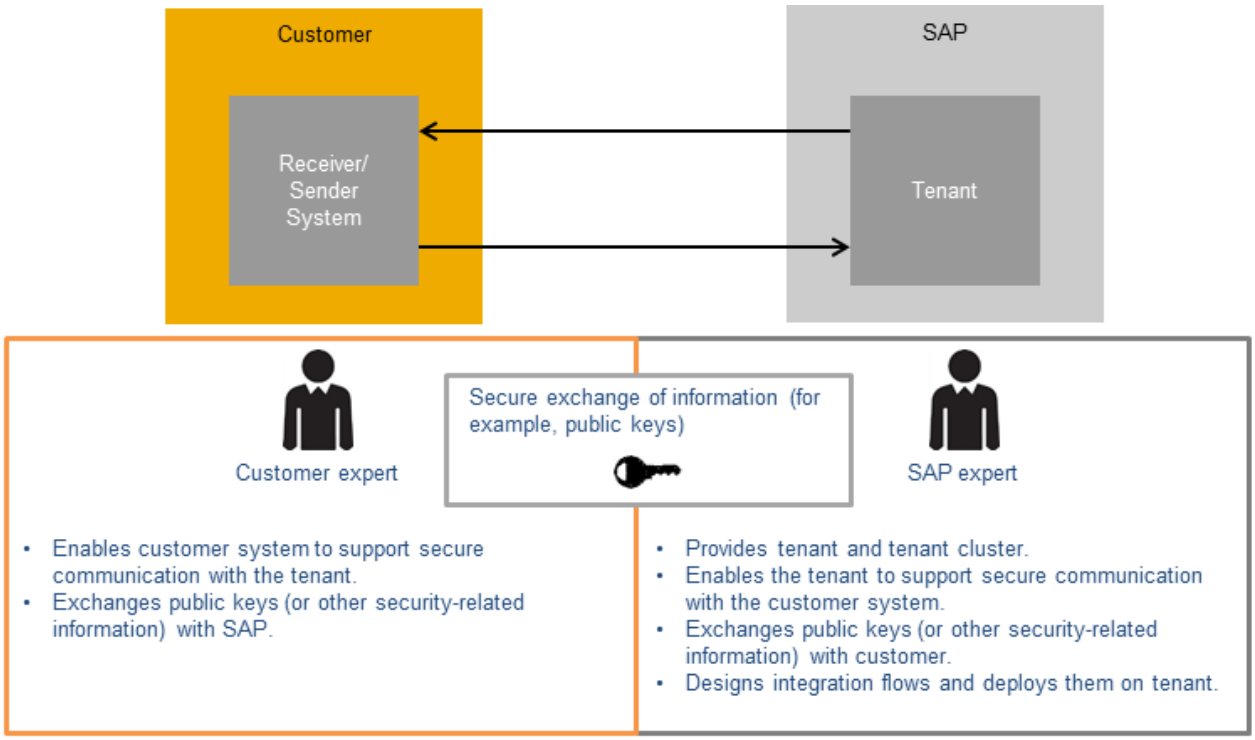
SAP provides the requested tenants and tenant clusters for the customer.For each customer system connected to SCP, separate resources (memory, CPU, and file system) are allocated in the SAP HANA Cloud. These resources are referred to as tenants.

SAP configures the customer's tenants to support secure communication (as required for the chosen authentication method).

The customer configures its systems to support secure communication.

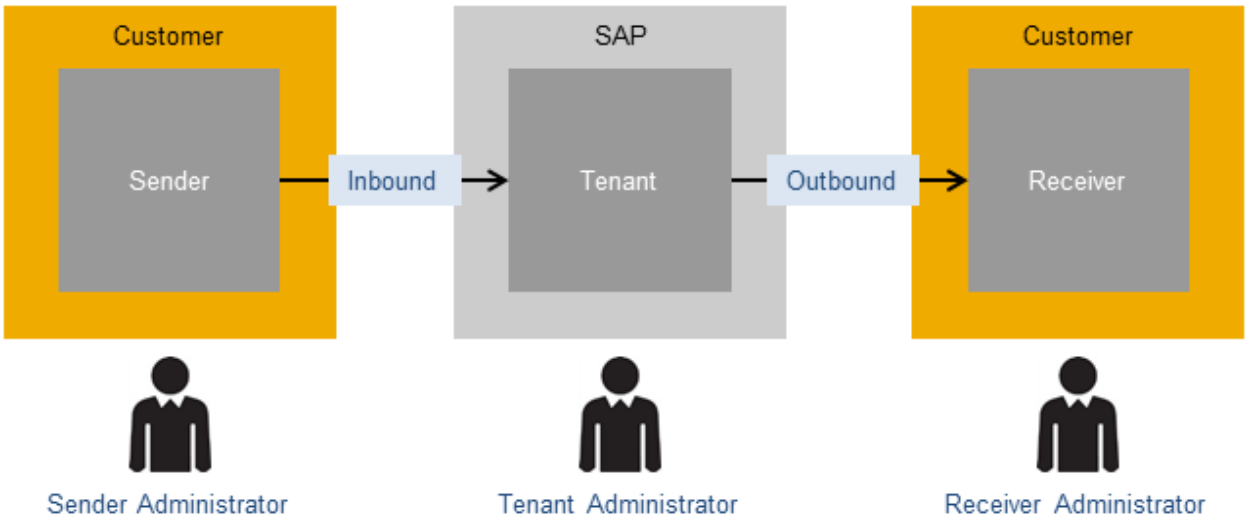
SAP designs and deploys the required iFlows on the tenant.

The following figure illustrates the partitioning of tasks:



4.1.2 Security Set Up

Security configuration involves always tasks at the side of all connected communication partners, and, therefore, different persons and roles are involved. The following figure shows the general setup when a tenant is connected to a customer system (either a sender or a receiver).



As illustrated in the figure, the general set up is that one customer system (sender system) sends a message to the tenant, and the tenant sends a message to another customer system (receiver system). To set up a secure

communication both between a sender and a tenant and between a tenant and a receiver, configuration tasks must be performed in the sender system, for the tenant and in the receiver system.

Let's assume that the tenant administrator would like to set up a secure connection to a receiver system based on asymmetric (or: public) key technology (for example, using PKCS#7). In that case, the general pattern is that the tenant administrator creates a key store with a key pair consisting of a private key (that always stays with the tenant administrator) and a public key. The tenant administrator must hand over its public key to the related communication partner - the receiver administrator. The way around, the receiver administrator hands over its public key to the tenant administrator. The tenant administrator imports the public key of the receiver into the tenant key store (and vice versa).

4.2 SSL setup in S/4 Hana System

SCP services are either secured by certificates or by basic authentication. For the backend connection, a generic certificate for the backend needs to be included into the build. The SAP S/4HANA system must be able to connect to the Internet via https protocol as a prerequisite for communication from SAP S/4HANA to the Cloud Solution. A certificate, which is signed by a valid Certification Authority is needed. This certificate needs to be imported via transaction `STRUST`.

> ⚠ Caution
>
> For certificate-based authentication a certificate signed by one of the CA mentioned in the SCP, integration service Operations Guide is mandatory. For a list of supported CAs see SAP Help Portal ▶ *SAP HANA Cloud Integration for process integration* ▶ *Designing and Operating Cloud Integration Content (for SCP) - PDF Documentation* ▶ *Operating and Monitoring SCP Integration* ▶ *Load Balancer Root Certificates Supported by SAP* ▶.

Procedure

1. Open the SAP Cloud Platform Integration tenant WEB UI
   (for example, **`https://<your SAP Cloud Platform Integration tenant URL>/itspaces`**).
2. On the *tenant* menu, choose Operations View icon.
3. Click on the tile '*KeyStore*' under Manage Security.
4. Download the following Root Certificates:
   1. Baltimore *cybertrust* root
   2. *Cybertrust sureserver* SV ca
5. Log on to SAP S/4HANA application system.
6. Access the transaction using the following navigation option:

Transaction Code	**`SE16`**

7. On the Data Browser: Initial Screen enter Table Name STRUSTSSL.

8. Navigate to *Table* Create *Entries*.
9. Confirm the Information dialog box with Enter.
10. Select *New Entries*.
11. On the *New Entries*: Overview of Added Entries screen, enter a new *SSL Client name <New SSL Client Name> (proposal- Identity: SAPCPI Description: CPI Connection)*.
12. Choose *Save* then select/ create a workbench request.
13. Access the transaction using the following navigation option:

Transaction Code	**STRUST**

14. On the Trust Manager: List screen a new entry will appear with the name *SSL Client <New SSL Client Name>*.
15. Choose the *Display* <-> *Change icon*.
16. Create a PSE (SSL Client Standard) with a certificate signed by a root CA supported by the SCP integration service load balancer in folder SSL Client <New SSL Client Name>. For more information about how to create a PSE, see *Configuring SAP NetWeaver AS for ABAP to Support SSL*.
17. It is also possible to use an already available signed certificate. In that case the p12 file has to be imported into the PSE mentioned in step 14. For more information about how to import the p12 file into PSE, see Importing a PKCS#12 File.
18. Double click the PSE in the *SSL Client <New SSL Client Name>* folder. The details of the PSE are show on the right side.
19. Choose the *Import Certificate* icon in the Certificate section.
20. Enter or select the File path to one of the public certificates of the SAP SCP integration service load balancer, that was downloaded earlier in this chapter.
21. Continue with *Enter*.
22. Choose the *Add to Certificate List* icon. The certificate appears in the Certificate List of the Own Certificate.
23. Repeat the previous steps for the second public certificate of the SAP SCP integration service load balancer.
24. Choose *Save*.

4.3 Define Outbound Services (Consumer Proxy) for Connection via SAP Cloud Platform Integration (SCP) 25

Before you go on with the configuration in this section please ensure that you have completed the configurations in chapter 3.

Procedure

1. Access the activity using the following navigation option:

IMG Menu	*Integration with Other SAP Components* > *Integration Component for Ariba Network* > *Framework Settings* > *Direct Connectivity Settings* > *Manage and Test Enterprise Services*
Transaction Code	**SOAMANAGER**

2. *SOA Management (<System name; Client>)* opens in a separate window. On the *Service Administration* tab, choose the link to *Web Service Configuration*. All services must be defined in this interface.
3. On the *Web Service Configuration (<System name; Client>)* view, click on the *Design Time Object Search* tab, enter the following search criteria and choose *Search* to start the search:

Field Name	User Action	Values
Object Type	**Is**	**Consumer proxy**
Object Name	**Contains**	**CXML***

The system brings up the following consumers proxies

4. CO_ARBFND_PRX_GPDQ_OUTPolling Client's outbound service that exchanges data with the AN (synchronously).
5. CO_ARBFND_PRX_OADP_OUTOutbound Adapter's outbound service that sends data to the AN

4.3.1 Configuration of the Outbound Consumer CO_ARBFND_PRX_GPDQ_OUT for SAP HANA Cloud Integration

1. Select outbound consumer CO_ARBFND_PRX_GPDQ_OUT (show and click to *Internal Name*)
2. Under *Details of Consumer Proxy:* CO_ARBFND_PRX_GPDQ_OUT, go to the *Configurations* tab and choose *Create* - *Manual Configuration*
3. In the guided configuration, you have to do the following steps. *Logical Port Name*: Make the following entries and choose *Next*

Field Name	User Action and Values
Logical Port Name	**HCI_CALL**
Description	**HCI GATEWAY Polling Client**
Logical Port is Default	**Select this Check-box**

4. *Consumer Security:*
5. For Basic Authentication: Select the **`User ID/Password`** checkbox and choose *Next*
6. For Certificate Authentication: Select the **`X.509 SSL Client Certificate`** checkbox and choose *Next*
7. *Messaging tab:* In the field *Message ID protocol*, select **`Suppress ID Transfer`**
8. In the *Transport Setting* tab create the following settings.

Field Name	User Action and Values
URL Access Path	**`/cxf/Ariba/Inbound`**
URL Protocol Information	**`HTTPS`**
Computer Name of Access URL	**`SCP Worker Node URL. For example, iflmapvb010v0082avtvlb-v0082.intaas.hana.ondemand.com`**
Port Number of access URL	**`443`**
Name of Proxy Host	<Enter the name of your Proxy Host>
Port Number of Proxy Host	<Enter the Port Number of your Proxy Host>
Make Local Call	**`No Local System Call`**
Compress Response	**`False`**

9. Press *Finish*
10. To test the Ping Web services, under *Details of consumer proxy:* CO_ARBFND_PRX_GPDQ_OUT, choose *Ping Web Service* or display this logical port and use the Icon in the header line Ping Web Service. A successful message looks like this: *"Web service ping failed (RC=403). Service Ping ERROR: Forbidden".*

4.3.2 Configuration of the Outbound Consumer CO_ARBFND_PRX_OADP_OUT for SAP Hana Cloud Integration

1. Select outbound consumer CO_ARBFND_PRX_OADP_OUT (show and click to *Internal Name*)
2. Under *Details of Consumer Proxy:* CO_ARBFND_PRX_OADP_OUT, go to the *Configurations* tab and choose *Create* - *Manual Configuration*
3. In the guided configuration, you have to do the following steps. *Logical Port Name*: Make the following entries and choose *Next*

Field Name	User Action and Values
Logical Port Name	**`HCI_GATEWAY`**

Field Name	User Action and Values
Description	**Send messages to Ariba**
Logical Port is Default	**Select this Check-box**

4. *Consumer Security:*
5. For Basic Authentication: Select the **User ID/Password** checkbox and choose *Next*
6. For Certificate Authentication: Select the **X.509 SSL Client Certificate** checkbox and choose *Next*
7. *Messaging tab:* In the field *Message ID protocol*, select **Suppress ID Transfer**
8. In the *Transport Setting* tab create the following settings.

Field Name	User Action and Values
URL Access Path	**/cxf/Ariba/outbound**
URL Protocol Information	**HTTPS**
Computer Name of Access URL	**SCP Worker Node URL. For example, iflmapvb010v0082avtvlb-v0082.intaas.hana.ondemand.com**
Port Number of access URL	**443**
Name of Proxy Host	<Enter the name of your Proxy Host>
Port Number of Proxy Host	<Enter the Port Number of your Proxy Host>
Make Local Call	**No Local System Call**
Compress Response	**False**

9. Press *Finish*
10. To test the Ping Web services, under *Details of consumer proxy: CO_ARBFND_PRX_OADP_OUT.* choose *Ping Web Service* or display this logical port and use the Icon in the header line Ping Web Service. A successful message looks like this: *"Web service ping failed (RC=403). Service Ping ERROR: Forbidden".*

4.4 Configuration in SAP Cloud Platform Integration

The typical flow from SAP S/4HANA to ARIBA using SCP as middleware will be as follows:

SAP S/4HANA will call the outbound SOAP service to SCP using the settings in SOAMANGER.

SCP will receive the incoming message and without performing any mapping will call Ariba cXML gateway.

Ariba will send the response back, which will be routed back to SAP S/4HANA.

4.4.1 Manage Authorization and certificates

To connect with Ariba, you need to download the public certificate to make SSL Connection to Ariba:

1. For HTTPS SSL encryption, go to https:\\buyer.ariba.com and download the server certificate from Ariba using your browser.
2. Add this certificate in your SCP tenant system.jks, by providing these certificates to Cloud operation team.
3. Following roles should be assigned to your SCN user, in SAP Cloud Platform Integration (SCP) tenant.

4.4.2 Construction of Integration flows

1. Open the SAP Cloud Platform Integration tenant WEB UI
2. On the tenant menu choose *Design*.
3. Choose *Create* to create a new integration package.
4. Enter a name (for E.g.: **`S4_Ariba_SQ_Integration`**). Technical name appears automatically.
5. Enter a Short description about the Integration.
6. Save.
7. Select the tab *Artifacts*.
8. Click on *Add*. Choose **`Integration Flow`**
9. Choose *Create*, Enter the name (e.g.: **`S4_to_Ariba_Inbound`**), save.
10. A point to point integration flow is created.
11. Select the integration flow and click on *edit*, a tools pallet appears.
12. Mouse hover on the sender, an arrow appears (connector). Click on the arrow and extend it to connect to the start symbol inside the integration process to create a sender soap adapter.
13. A list of available adapter types appears. Select **`Soap`**, further select **`Soap 1.x`** as message protocol.
14. Mouse hover on the end symbol inside the integration process, an arrow appears. Click on it and extend it to connect to the receiver to create a receiver soap adapter.
15. A list of available adapter types appears. Select **`Soap`**, further select **`Soap 1.x`** as message protocol
16. Save the Integration Flow.
17. Go back to the package view, select the artifacts tab.
18. Repeat the steps 7-15 for the outbound Iflow (Name E.g.: **`S4_to Ariba_Outbound`**).

4.4.3 Configuration of Integration flows

1. Open the SAP Cloud Platform Integration tenant WEB UI
2. On the tenant menu choose *Design*. Click on your Integration package. Go to the *artifacts* tab.
3. Choose artifact **`S4_to_Ariba_Inbound`**, click on *edit*.

4. Select the *sender soap adapter*, enter the following details in the *connection* tab:

Field Name	Entry Value
Address:	1. **/Ariba/Inbound** 2. (This address must be unique on SAP SCP, integration service Tenant. If this scenario has to be deployed twice on same tenant, this address needs to be changed)
Service definition	1. **Manual**
Message Exchange Pattern	1. **Request-Reply**
Authentication Type	1. **Certificate-based Authentication**
For certificate Authentication	1. Choose Browse and select the certificate stored using step *Export SAP S/4 Hana Public Certificate*.

5. Select the *Receiver soap adapter*, enter the following details in the *Connection* tab:

Field Name	Entry Value
1. Address	1. **https://service.ariba.com/ANSapGateway.aw/ad/cxml**
1. Proxy Type	1. **Internet**
1. Authentication Type	1. **None**
1. Allow Chunking	Do not Select

6. On the tenant menu choose *Design*. Click on your Integration package. Go to the *artifacts* tab.
7. Choose artifact **S4_to_Ariba_Outbound**, click on *edit*.
8. Select the *sender soap adapter*, enter the following details in the *connection* tab:

Field Name	Entry Value
Address	1. **/Ariba/Outbound** 2. (This address must be unique on SAP SCP, integration service Tenant. If this scenario has to be deployed twice on same tenant, this address needs to be changed)
Service definition	1. **Manual**
Message Exchange Pattern	1. **Request-Reply**
Authentication Type	1. **Certificate-based Authentication**
For certificate Authentication	1. Choose Browse and select the certificate stored using step *Export SAP S/4 Hana Public Certificate*.

9. Select the *Receiver soap adapter*, enter the following details in the *Connection* tab:

Field Name	Entry Value
Address	1. **https://service.ariba.com/ANSapGateway.aw/ad/cxml**

Field Name	Entry Value
Proxy Type	1. **`Internet`**
Authentication Type	1. **`None`**
Allow Chunking	Do not Select

10. Save. Deploy.

5 Configuration of the Ariba Network buyer account

The Ariba Network buyer account needs to be configured to meet customer requirements. This chapter describes settings in the Ariba Network Buyer account configured by the customer.

As the Ariba Network allows for a flexible configuration of the process, this document provides a straight forward setup that allows the integration between S/4HANA OP and the Ariba Network.

5.1 Configure Business Application ID for S/4 HANA OP

The settings you make here, represent the S/4 HANA OP. If you already integrate S/4 HANA OP with the Ariba network for purchase orders and/or invoices it is very likely that the below entries already exist, and this chapter can be skipped.

Prerequisite

Your Ariba Network account supports multi-ERP.

Procedure

1. Log on to your Ariba Network buyer account.
2. Choose the *Administration* tab.
3. Choose *Configuration.*
4. On the *Configuration* screen, choose *Business Application IDs*. (Note: the exact name of this configuration step may be slightly different depending on the exact type of your Ariba Buyer account).
5. In the *Lists of System IDs* screen, click *Create* and create an entry with *System ID* and *Unique Address ID* "<S/4HANA>". <S/4HANA> is the logical system ID of your S/4HANA OP system. Enter the rest of required information according to your needs. Click *Save*.
6. In the *List of System IDs* screen, locate the just created *System ID* "<S/4 HANA>" and click on *End Points*.
7. In the *List of End Points* screen, click *Create*. (A pop-up may appear that asks to take over existing cXML setup, in the following steps, we assume that you chose *No*)
8. On the Configure End Point screen
   - Create an *End Point ID* "<S/4 HANA>". <S/4 HANA> is the logical system ID of your S/4 HANA OP system
   - Select integration type "cXML"

- Select *authentication method* “Shared Secret”
- Enter and confirm *Shared Secret*
- In the *Profile URL* section, locate the field *Profile URL*.
- If the field *Profile URL* is not empty, delete the content. The field should be blank.
- In the section *Post URL* look for the field POST URL.
- If the field is not empty, delete the content. The field should be blank.

9. Save your entries.

5.2 Configure Business Application ID for Ariba Network Quote Automation

The settings you make here, represent the Ariba Network. If you already integrate S/4 HANA OP with the Ariba Sourcing it is very likely that a part of the below entries already exist and a part of this chapter can be skipped.

Prerequisite

Your Ariba Network account supports multi-ERP.

Procedure

1. Log on to your Ariba Network buyer account.
2. Choose the **`Administration`** tab.
3. On the *Configuration* screen, choose *Business Application IDs*.

> **i** Note
>
> The exact name of this configuration step may be slightly different depending on the exact type of your Ariba Buyer account.

> **i** Note
>
> If you don't find this link, your system is probably not endpoint-enabled.

4. In the *Lists of System IDs* screen, click *Create* and create an entry with *System ID* and *Unique Address ID* “Ariba”. Enter the rest of required information according to your needs. Click *Save*.
5. In the *List of System IDs* screen, locate the just created *System ID* “Ariba” and click on *End Points*.
6. In the *List of End Points* screen, click *Create*. (A pop-up may appear that asks to take over existing cXML setup, in the following steps, we assume that you chose *No*)
7. On the Configure End Point screen:
   - Create an *End Point ID “<S/4 HANA>”*

- Select integration type “*cXML*”
- Select *authentication method* “**`Shared Secret`**”
- Enter and confirm *Shared Secret*
- Click **`Save`**

8. Back on the Configure End Point screen:
   - Create an *End Point ID* “Ariba”
   - Select integration type “*cXML*”
   - Select *authentication method* “**`Shared Secret`**”
   - Enter and confirm *Shared Secret*
   - Enter profile URL: https://s1.ariba.com/Buyer/cxmlchannel/<ANID> where <ANID> is the Ariba network ID of the buyer account.

     > **i** Note
     >
     > The URL will be different for your Ariba Network!

   - In the section *Post Url* look for the field POST URL.
   - If the field is not empty, delete the content. The field should be blank
   - Click *Save*

> **⚠** Caution

Due to an existing limitation in the Ariba Network it is a requirement that you have one System ID and one assigned End Point set up as default. Even if your system landscape does not require a default system/end point, you need to define them.

Please have a look at the *List of System IDs* screen, if a System ID set to *Default* is already existing. Note that the System ID set as *default* needs to have an assigned End Point also set up as *Default*. You can check this in the *List of End Points* corresponding to the *Default System ID*. If you cannot find a *Default End Point* you can set up an existing one to default or create a new one (e.g. “default”).

5.3 Supplier Enablement

For each supplier, you want to send RFQs, an active relationship with that supplier is required. This chapter describes how to set up the relationship with a supplier that already exists on the Ariba network (i.e. have an Ariba Network ID, ANID).

5.3.1 Active Relationships

Procedure

1. Log on to the Ariba Network (AN) with your Buyer account.
2. Navigate to the *Supplier Enablement* tab and choose the *Active Relationships* sub tab.
   If you find the supplier, you want to connect with, in the *Current Suppliers* table, you can continue with section *Assign Private ID*.
   If the supplier is not in the *Current Suppliers* table, there is no active relationship with the supplier yet. Continue with the following steps:
3. Choose*Search for Suppliers*(NOT *Search*)
4. Fill in appropriate search criteria and choose *Search*.
5. Select the supplier found, and choose *Actions* and *Add to Selected Suppliers*.
6. You have to review the supplier's profile. The profile can also be downloaded.
7. In the Selected Suppliers overview, open the supplier by choosing its link.
8. To establish the relationship, choose *Request a Relationship*.

> ⚠ Caution
>
> Note that the supplier must accept the relationship. If the supplier has not accepted it, the supplier does not appear under *Active Relationships*.

5.3.2 Assign Private ID

Use

Supplier master records in S/4HANA OP use IDs for identification. Customers with several ERP and/or S/4HANA OP systems may even use different IDs assigned to the same supplier in each respective system.

The settings described in this chapter link a supplier in the Ariba Network (as identified per it's ANID) to the supplier IDs used in the customer's and other systems.

Procedure

1. Log on to the Ariba Network (AN) with your Buyer account.
2. Navigate to the *Supplier Enablement* tab and choose *Active Relationships*.

3. Choose *More Actions* > *Edit*.
4. On the *Edit Preferences for Supplier: <your supplier name>* screen, go to the *Enter supplier identifiers for the procurement application* sub screen and choose *Add.*
5. Relevant for Multi-ERP: In the *Add Supplier Unique Key* dialog box, choose one of your systems and enter the relevant vendor ID for this system (Vendor ID, for example, 300000).
6. In the example, this tells the Ariba Network that this supplier has the ID 300000 in system *<System ID>* (this is the *System ID* of your S/4HANA OP system).
7. Relevant for Single-ERP: First Field is Vendor ID (for example, 300000).
8. In the dialog box, choose *Save*.
9. Repeat steps 5 and 6 for all your systems.
10. Choose *Save* on the *Edit Preferences for Supplier: <your supplier name>* screen

5.4 Quote Automation Rules

Use

The settings you make here configured the Quote Request flow and the category matching rules to specify whether you want only your approved vendors or all Ariba Network suppliers to participate in a product or service category. To route to Quote Automation, you need to choose the option *Ariba Network.*

Procedure

1. Log on to the Ariba Network (AN) with your Buyer account.
2. Choose the *Administration* tab.
3. Choose *Configuration.*
4. On the *Configuration* screen, choose *Quote Automation*.
5. Choose Quote Automation Rules tab.
6. Make following settings:
7. Quote Request Routed Via: *Ariba Network*
8. Default Rule: *All Suppliers*

5.5 Commodity Mapping

Use

Ariba uses the United Nations Standard Products and Services Code (UNSPSC) classification domain for mapping commodities. However, the S/4 HANA system might use different standards for mapping commodities. Configuring commodity mapping ensures that the commodity codes used in the S/4 HANA system are mapped to the UNSPSC codes used in Ariba Network.

Ariba Network provides the possibility to upload commodity code maps from an Excel spreadsheet. To get hold of a spreadsheet with the correct format, first do a download of existing mappings, then add the commodity mappings you want to create in Ariba Network and upload the spreadsheet. This is described in the following step-by-step instructions.

Procedure

1. Log on to the Ariba Network.
2. Choose the *Administration* tab.
3. Choose *Configuration*.
4. On the *Configuration* screen, choose *Quote Automation*.
5. Go to *Commodity Mapping*tab
6. Select *Download Active Mappings*
7. Your browser will now download the file *CommodityMapping.csv*.
8. Open the file and add an entry that maps the own domain code to UNSPSC code set. The domain that is used for material groups in S/4 HANA is the S/4 HANA system's ID.
9. The structure of the table is:

Domain	System ID of the S/4 HANA system
Unique Name	Commodity code ID should be identical to the material ID in the S/4 HANA system
Name	Name or description of the commodity code should be identical to the description of the material group in the S/4 HANA system
UNSPC Code	Code representing the commodity as per the UNSPSC classification system. Ariba recommends using level 4 codes, e.g. 45111615
UNSPC Description	Description of the commodity as per UNSPSC

Domain	Unique Name	Name	UNSPSC Code	UNSPSC Description
<S/4 HANA>	L001	Trading Materials	45111615	Projection lenses

10. Save the spreadsheet.
11. Go to *Upload your CSV File* and search for the previously created file
12. Choose *Upload*

6 Configuration in S/4HANA OP Edition

Setting up the connection to the Ariba Network requires some basic configuration activities as described hereafter.

6.1 Activate cXML message types

Use

In this activity, you decide which messages are to be routed through the Ariba Network. Please notice that only the messages in the table below are relevant for your scenario. You can activate the required cXML message types and ignore all other cXML messages.

Procedure

1. Access the transaction using the following navigation path:

Transaction Code	**SPRO**
IMG Menu	*Integration with Other SAP Components* > *Business Network Integration* > *Integration with the Ariba Network* > *Framework Settings* > *Define Basic Message Settings*

2. Set the flag to *Active* for following messages:

Application Component ID	Object Type	cXML Message Type	Direction	Active
BNS-ARI-SE-ERP	**Request for Quotation**	**QTEQ**	**Outbound**	**select**
BNS-ARI-SE-ERP	**Quote**	**QTEM**	**Inbound**	**select**

3. Save your entries

6.2 Credentials and End Points

Use

In this configuration activity, you specify the credentials that identify your company on Ariba Network and enable end points. You can make the required settings as follow:

Procedure

1. Access the transaction using the following navigation path:

Transaction Code	SPRO
IMG Menu	*Integration with Other SAP Components* > *Business Network Integration* > *Integration with the Ariba Network Framework Settings* > *Define Credentials and End Points for Ariba Network*

2. Choose *New Entries* and create the following settings:

Ariba Network ID	Shared Secret	Test Account	Enable System ID	System ID	Enable End Points
ANID of your buyer account	Ariba Network Buyer Account Shared secret	Identifies a test account	Used if multiple buyer systems use the same Ariba Network buyer account. In case you are unsure what best fits your situation, enable it.	System ID (if enabled)	Select *Enable end points for authentication and polling.* An Ariba Network ID can have multiple end points. An end point is a document routing placeholder that ensures documents from Ariba Network are sent to the required destinations (system).

3. Save your entries.

4. To specify the *End Points* please select the just created entry for the Ariba Network Buyer ID and add a New End Point with the following settings:

SAP-Internal Key	Ariba End Point ID	Shared Secret
Please use the System ID, entered in the previous step	Please use the *End Point ID* "<S/4 HANA>", created in the Ariba Network Buyer account (usually the same as the System ID)	Ariba Network Buyer Account Shared secret

5. Save your entries.

For more information on end points go to:

https://connect.ariba.com

After you logged on, you can go to the *Search*-Tab. In the Search-field you should enter *Buyer Administration Guide* and then click on the *Submit* button. Please open the entry *Buyer Administration Guide* and search in the pdf-document for *End points.*

6.3 Assign network ID to Company Code

Use

In this configuration activity, you assign Ariba Network IDs (ANID) to company codes in your S/4HANA OP System. The Ariba Network ID is being sent along with each document (for example, request for quotation) to the Ariba Network and identifies the sender of the document. You may use the same ANID for all company codes. Assign an ANID to each company code that communicates with Ariba. Do not assign more than one ANID per company code.

Procedure

1. Access the transaction using the following navigation path:

Transaction Code	SPRO
IMG Menu	*Integration with Other SAP Components* > *Business Network Integration* > *Integration with the Ariba Network* > *Application-Specific Settings* > *Assign Ariba Network ID to Company Code*

2. Choose *New Entries* and create the following settings:

Ariba Network ID	Company Code	Company Name
ANID of your buyer account	Company Code	The company code's name

3. Save your entries.

6.4 Output Parameter Determination

Use

In this activity, you define settings relevant for the output of requests for quotation.

Procedure

1. Access the transaction using the following navigation path:

Transaction Code	**SPRO**
IMG Menu	*Integration with Other SAP Components* > *Business Network Integration* > *Integration with the Ariba Network* > *Application-Specific Settings* > *Define Message Output Control* > *Method 2: Use SAP S/4HANA-Based Output Management* > *Define Business Rules for Output Determination*

2. On the *Output Parameter Determination* screen, under *Select Business Rules*, select the following criteria:

Screen Element	User Action and Values
Show Rules For	**Request for Quotation**
Determination Step	**Channel**

3. Create one entry in the table as follow:

Output Type	Channel	Exclusive Indicator
EXTERNAL_REQUEST (External request)	*XML (XML)*	*-(false)*

4. Activate your entries.

5. Save your entries.

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