SAP Ariba Cloud Integration Gateway how to guide
Ariba Network

SAP

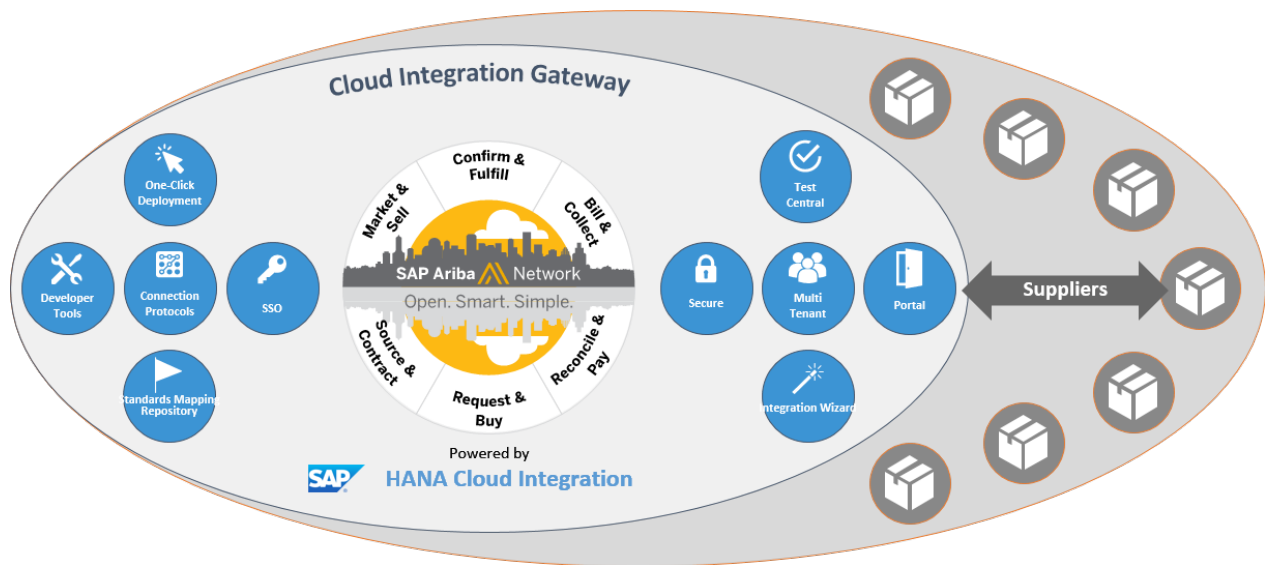SAP Ariba

Content

About the SAP Ariba Cloud Integration Gateway

The SAP Ariba Cloud Integration Gateway is a self-service gateway that allows suppliers to configure and integrate to Ariba Network and transact with buyers seamlessly.

Using the SAP Ariba Cloud Integration Gateway, you can:

- Configure your integration between Ariba Network and your ERP application to manage one or more buyer-supplier trading relationships.
- Specify the mapping configuration.
- Validate and self test transaction documents.
- Monitor and track the integration lifecycle overall.

> **i Note**
>
> The SAP Ariba Cloud Integration portal provides online help for the tasks associated with each page. To view help information for a page, click the Help button on the top left of the page. Instructions, tips, and notes are displayed in a text pane to the right of the page. You can also enter text in the search field inside the pane to initiate a search within the help text.

About document types

Document types are the documents you send or receive from Ariba Network.

There are different types of documents. UN-EDIFACT, ASC-X12, OAGIS, and PIDX follow different naming conventions for the document types. The file size is limited to 100 MB. You can send multiple document types within an EDI envelope; however, the combined payload must be less than 100 MB. Individual transactions (after

splitting the envelope) must be less than 40 MB. If a file or transaction fails this validation, a custom error message is displayed. The following table lists the supported document types in the available document formats and in cXML as a reference:

Document types	cXML	UN-EDIFACT D96A	GS1 GUSI	ASC-X12 v4010	OAGIS v9.2	PIDX	EANCOM 97	EANCOM 2002
Purchase Order	OrderRequest CopyRequest: SAP Ariba Supply Chain Collaboration	ORDERS	multiShipmentOrder	850	ProcessPurchaseOrder	OrderCreate	—	ORDERS
Sales Orders	SalesOrderRequest	—	—	—	ProcessPurchaseOrder	—	—	—
Purchase Order Change Request	OrderRequest CopyRequest: SAP Ariba Supply Chain Collaboration	ORDCHG	—	860	ProcessPurchaseOrder	OrderChange	—	ORDCHG
Purchase Order Response	ConfirmationRequest	ORDRSP	—	855	AcknowledgePurchaseOrder	OrderResponse	—	—
Advanced Shipment Notice	ShipNoticeRequest CopyRequest: SAP Ariba Supply Chain Collaboration	DESADV	despatchAdvice	856	NotifyShipment	AdvanceShipNotice	—	DESADV
Invoice	InvoiceDetail InvoiceDetailRequest	INVOIC ⓘ **Note** Also for standard D01B	—	810	—	Invoice	INVOIC	INVOIC

Document types	cXML	UN-EDIFACT D96A	GS1 GUSI	ASC-X12 v4010	OAGIS v9.2	PIDX	EANCOM 97	EANCOM 2002
Invoice Response	StatusUpdateRequest	—	—	—	—	InvoiceResponse	—	—
Technical Acknowledgment	StatusUpdateRequest	CONTRL	—	997	ConfirmBOD	—	—	—
Goods Request (Inbound)	ReceiptRequest	RECADV	ReceiptAdvice	861	ProcessReceiveDelivery	Receipt	—	—
Forecast Visibility	ProductActivityMessage	—	ConsumptionReport	830	NotifyPlanningSchedule	—	—	—
ComponentConsumptionRequest	ComponentConsumptionRequest	—	—	866	NotifyInventoryConsumption	—	—	—
ForecastCommit	ProductReplenishmentMessage	—	—	830	NotifyPlanningSchedule	—	—	—
MO/PO	ProductReplenishmentMessage	INVRPT	—	866	NotifyProductionOrder	—	—	—
Inventory	ProductReplenishmentMessage	INVRPT	ReplenishmentRequest InventoryStatus	846	NotifyInventoryBalance	—	—	—
Functional Acknowledgment	StatusUpdateRequest	APERAK	—	824 / 864	ConfirmBOD	—	—	—
PR	PaymentRemittance	REMADV	—	820	ConfirmBOD	—	REMADV	REMADV
Scheduling Agreement Release/ Delivery Schedule	OrderRequest	DELFOR	GoodsRequirement	—	ProcessPurchaseOrder	—	—	—

Document types	cXML	UN-EDIFACT D96A	GS1 GUSI	ASC-X12 v4010	OAGIS v9.2	PIDX	EANCOM 97	EANCOM 2002
Scheduling Agreement Release/ Delivery Schedule - JIT	OrderRequest	DELJIT	—	862	ProcessPurchaseOrder	—	—	—
Scheduling Agreement Release/ Delivery Schedule - Commit (Forecast Commit Data)	OrderRequest	—	—	—	ProcessPurchaseOrder	—	—	—
Consignment Movement List	ProductReplenishmentMessage	INVRPT	ReplenishmentProposal	—	—	—	—	—
Transport Request	TransportRequest	IFTMIN	—	204	—	—	—	—
Transport Confirmation	TransportConfirmation	IFTSTA	—	214	—	—	—	—
Quality Notification (Outbound)	—	—	—	842	—	—	—	—
Quality Notification (Inbound)	—	—	—	842	—	—	—	—

When configuring an integration project you have to consider the relevant document types in the steps *Connection* and *Mappings*.

You also need to be aware of the document types using *Schema Validation* and *Test Transformation*.

Error handling in the SAP Ariba Cloud Integration Gateway

Get to know how the SAP Ariba Cloud Integration Gateway does error handling and helps you configure your cloud integration project.

Error Validation for Fields

In case you miss to fill a required field or enter an incompatible value, the field will be highlighted in red when you are trying to save or activate a function. This validation is done for select boxes as well as free text fields.

The gateway validates fields that require an entry in a specific format accordingly. An example is the URL within the project configuration which needs to have an `https://` URL due to security reasons and you may not enter any other type of URL.

Getting started

To connect to the Cloud Integration Gateway, you must have the following:

- An active supplier account on Ariba Network. For more information, see *Registering With Ariba Network for Suppliers* in the ▶ **Product Documentation** ❯ **Getting Started** ❯ section of the Learning Center.
- A valid trading buyer -supplier relationship on Ariba Network. For more information about configuring your Ariba Network buyer account, see the *Ariba Network Buyer Administration Guide*.
- Configure your Ariba Network account to send and receive transaction documents from Cloud Integration Gateway.
- Configure your Ariba Network account to send and receive EDI documents. For more information, see *Configuring Document Routing* in the ▶ **Product Documentation** ❯ **Administration and Configuration** ❯ section of the Learning Center.
- Configure your system to support IETF Applicability Statement 2 (AS2) documents
- Configure your digital certificates to use the HTTPS or AS2 transport. For more information about obtaining a digital certificate, see the *Ariba cXML Solutions Guide* in the ▶ **Product Documentation** ❯ **Administration and Configuration** ❯.

All procedures at a glance

An overview of all procedures in the context of the SAP Ariba Cloud Integration Gateway.

Prerequisites

Description	Related Information
Describes the way from Ariba Network to the SAP Ariba Cloud Integration Gateway.	Logging in to the Cloud Integration Gateway [page 12]
Describes the way from Ariba Network to the SAP Ariba Cloud Integration Gateway and how to change the routing method on the Ariba Network.	Enabling the Cloud Integration Gateway on Ariba Network [page 13]
Change the routing method on Ariba Network.	Configuring the Routing Methods for Non-cXML Transaction Documents [page 13]

Description	Related Information
All about users, roles, and permission settings.	Assigning User Permissions for the Ariba Cloud Integration Gateway [page 14]
Your first task when visiting the SAP Ariba Cloud Integration Gateway. You can also edit this information later.	Adding your ERP System Information [page 19]

Wizard Steps

Description	Related Information
This step is the first one after selecting **Create a new Integration Project** on the **Home** page.	Providing Basic Information [page 30]
Configure connections within a project.	Configuring Ariba Network Connection [page 31]
Set up your mapping using data maps.	Configuring Data Maps for Incoming and Outgoing Transaction Documents [page 33]
Enter data as cross reference between you and your partner.	Specifying Buyer and Supplier Information [page 34]
Double check your project configuration.	Confirming your Project Configuration [page 36]
Create a test script and schedule the testing.	How to test your project configuration [page 36]
Get ready for deployment.	Scheduling and Activating the Project on the Production Environment [page 40]

Preparation or Troubleshooting

Description	Related Information
Track or monitor your transactions.	Tracking Transaction Documents [page 44]
Test a connection with this tool.	Testing the connection to Ariba Network [page 46]
Validate your syntax with standard schemas.	Validating Syntax [page 48]
If your syntax is correct, validate that the transformation works.	Validating the Transformation with XSLT's [page 50]

Accessing the SAP Ariba Cloud Integration Gateway

You can access the SAP Ariba Cloud Integration Gateway from your Ariba Network account or using the email inviting you to register on Ariba Network. You need to set up the SAP Ariba Cloud Integration Gateway to access it.

If you are a user who is newly added to the Ariba Network account with permissions to access the SAP Ariba Cloud Integration Gateway, you receive an invitation to register on Ariba Network.

Enter your system information the first time you log in to the SAP Ariba Cloud Integration Gateway. The SAP Ariba Cloud Integration Gateway stores the information you provide when you log in. When you log in again, the SAP Ariba Cloud Integration Gateway displays the Home page.

You can edit the system information that you enter on the SAP Ariba Cloud Integration Gateway at ❘▶ *Username* ❭ **Basic Data** ❭ **Edit** ❭ .

Related Information

[How to add your ERP system information \[page 19\]](#)

Configuring your Ariba Network account to access SAP Ariba Cloud Integration Gateway

Suppliers using Ariba Network can send and receive non-cXML transaction documents using the SAP Ariba Cloud Integration Gateway. You need to set up the SAP Ariba Cloud Integration Gateway and also configure the routing method to send and receive non-cXML transaction documents from SAP Ariba Cloud Integration Gateway to Ariba Network. Supplier administrators need to assign roles and permissions for users to access the SAP Ariba Cloud Integration Gateway.

For more information about users, roles, and permissions, see *Seller Account Settings and Profile Configuration* in the ❘▶ **Product Documentation>** ❭ **Administration and Configuration** ❭ **Account Settings and Profile Configuration** ❭ section of the Learning Center.

For more information about routing methods, see *Configuring Document Routing* in the ❘▶ **Product Documentation** ❭ **Administration and Configuration** ❭ section of the Learning Center.

Related Information

[How to login to the SAP Ariba Cloud Integration Gateway \[page 12\]](#)
[How to enable the SAP Ariba Cloud Integration Gateway on Ariba Network \[page 12\]](#)
[How to configure the routing methods for non-cXML transaction documents \[page 13\]](#)

How to login to the SAP Ariba Cloud Integration Gateway

Context

You can access the SAP Ariba Cloud Integration Gateway from your Ariba Network account or using the email inviting you to register on Ariba Network. You need to set up the SAP Ariba Cloud Integration Gateway to access it.

> **i Note**
>
> SAP Ariba Cloud Integration Gateway displays an alert message to suppliers 30 days before the date of expiry of their certificate and enables them to update their certificate.

Procedure

1. Log in to your Ariba Network account.
2. Click **Company Account Settings** in the upper right corner of the dashboard.
3. Select **Electronic Order Routing**.
4. Click **Configure Ariba Cloud Integration Gateway (non-native integration)**.
5. Click **Go to the Ariba Cloud Integration Gateway**. The **Cloud Integration Gateway** page appears.
6. Enter your ERP system information. You need to enter this information only the first time you log in.
7. Click **Save**.

Related Information

How to enable the SAP Ariba Cloud Integration Gateway on Ariba Network

Context

To send and receive non-cXML transaction document from the cloud integration gateway, you need to setup and enable the SAP Ariba Cloud Integration Gateway on Ariba Network. You also need to configure your routing method to send and receive non-cXML transaction document from the SAP Ariba Cloud Integration Gateway.

Procedure

1. Log in to your Ariba Network account.
2. Click **Company Account Settings** in the upper right corner of the dashboard.
3. Select **Electronic Order Routing**.
4. Click **Configure Cloud Integration Gateway (non-native integration)**.
5. Click **Enable the Ariba Cloud Integration Gateway**.
6. Click **Save**.

   A new link to access the SAP Ariba Cloud Integration Gateway appears.
7. Click **Close**.
8. On the **Electronic Order Routing** page, choose the **Cloud Integration Gateway** routing method from the dropdown menu in the **Routing Method** column. You need to specify the routing method for each of the transaction documents that you want to send in a non-cXML format.
9. Specify the corresponding configuration values in the **Options** column.
10. Click **Save** and then **Close**.

> ℹ **Note**
>
> You need to have the required user permissions to access the SAP Ariba Cloud Integration Gateway.

Related Information

How to assign user permissions for the SAP Ariba Cloud Integration Gateway [page 14]
All procedures at a glance [page 9]

How to configure the routing methods for non-cXML transaction documents

Context

You need to set up the SAP Ariba Cloud Integration Gateway before you configure the routing methods for non-cXML transaction documents.

Procedure

1. Log into your Ariba Network account.
2. Click **Company Account Settings** in the upper right corner of the dashboard.

3. Select **Electronic Order Routing**.

4. On the **Electronic Order Routing** page, choose the **Cloud Integration Gateway** routing method from the dropdown menu in the **Routing Method** column. You need to specify the routing method for each of the transaction documents that you want to send in a non-cXML format.

5. Specify the corresponding configuration values in the **Options** column.

6. Click **Save** and then **Close**.

Related Information

How to assign user permissions for the SAP Ariba Cloud Integration Gateway

Context

Supplier administrators can assign predefined permissions to users accessing the SAP Ariba Cloud Integration Gateway. You need to create a role and associate the required permissions for the role, before you can create users.

Procedure

1. Log in to your Ariba Network account.

2. Click **Company Account Settings** in the upper right corner of the dashboard.

3. Select ▌▶ **Account Settings** ❯ **Users** ▌.

4. Click **Create Role**. Enter a distinctive name for the role.

5. (Optional) Enter a description for the role. Descriptions can be useful later, if you want to review or revise the structure of your roles.

6. Check the checkbox next to one or more of the following permissions for the new role. Each role must have at least one permission:

   ○ **Ariba Cloud Integration Gateway Configuration**: Allows you to create, modify, and maintain projects on the SAP Ariba Cloud Integration Gateway.

   ○ **Ariba Cloud Integration Gateway Access**: Allows you to view and search for projects available on the SAP Ariba Cloud Integration Gateway.

7. Click **Save**.

   Ariba creates the role and returns you to the **Users** page.

8. Click **Create User** to create a user for the SAP Ariba Cloud Integration Gateway.

Related Information

Trusted certificate authorities

A table with trusted certificate authorities (CA) you can use for your connection to Ariba Network.

Table 1: Certificate Authorities

C=	O=	OU=	CN=
US	GeoTrust Inc.		bc.gdp-edi.net
US	Entrust Inc.	See www.entrust.net/legal-terms	Entrust Root Certification Authority - G2
US	Symantec Corporation	Hosting Operations	service.ariba.com
US	VeriSign Inc.	VeriSign Trust Network	VeriSign Universal Root Certification Authority
US	Symantec Corporation	Symantec Trust Network	Symantec Class 3 Secure Server SHA256 SSL CA
PL	Unizeto Sp. z o.o.	-	Certum CA
US	VeriSign Inc.	VeriSign Trust Network	VeriSign Class 3 Secure Server CA - T1
US	VeriSign Inc.	VeriSign Trust Network	VeriSign Class 3 Secure Server CA - G3
US	VeriSign	Class 3 Public Primary Certification Authority	
US	VeriSign	VeriSign Trust Network	VeriSign Class 3 International Server CA - G3
US	VeriSign Inc.	VeriSign Trust Network	VeriSign Class 1 Public Primary Certification Authority - G3
US	thawte Inc.	Certification Services Divisio	thawte SSL CA - G2
US	thawte Inc.	Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only	thawte Primary Root CA

C=	O=	OU=	CN=
DE	TC TrustCenter GmbH	TC TrustCenter Class 2 L1 CA	TC TrustCenter Class 2 L1 CA XI
DE	TC TrustCenter GmbH	TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA II
DE	SAP Trust Community		SAP Passport CA
US	GTE Corporation	GTE CyberTrust Solutions, Inc.	GTE CyberTrust Global Root
US	GoDaddy.com Inc.	http://certs.godaddy.com/repository/	Go Daddy Secure Certificate Authority - G2
US	GoDaddy.com		Go Daddy Root Certificate Authority - G2
US	The Go Daddy Group Inc.	Go Daddy Class 2 Certification Authority	
US	Entrust Inc.	See www.entrust.net/legal-terms	Entrust Root Certification Authority - G2
US	Entrust Inc.	www.entrust.net/rpa is incorporated by reference	Entrust Certification Authority - L1C
US	Entrust Inc.	www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)	Entrust.net Certification Authority (2048)
US	DigiCert Inc.	www.digicert.com	DigiCert Secure Server CA
US	DigiCert Inc.	www.digicert.com	DigiCert High Assurance EV Root CA
US	DigiCert Inc.	www.digicert.com	DigiCert High Assurance CA-3
US	DigiCert Inc.	www.digicert.com	DigiCert Global Root CA
US	Cybertrust Inc.	GTE CyberTrust Solutions	Cybertrust SureServer Standard Validation CA
IE	Cybertrust Inc.	CyberTrust	Cybertrust Public SureServer SV CA
GB	AddTrust AB	AddTrust External TTP Network	COMODO High-Assurance Secure Server CA
PL	Unizeto Technologies S.A.	Certum Certification Authority	Certum Level IV CA
SE	AddTrust AB	AddTrust External TTP Network	AddTrust External CA Root

C=	O=	OU=	CN=
US	GeoTrust Inc.	(c) 2008 GeoTrust Inc. - For authorized use only	GeoTrust Primary Certification Authority - G3
BE	GlobalSign nv-sa	Root CA	GlobalSign Root CA
	GlobalSign	GlobalSign Root CA - R2	GlobalSign
	GlobalSign	GlobalSign Root CA - R3	GlobalSign
US	GeoTrust		RapidSSL CA
US	Entrust Inc.	See www.entrust.net/legal-terms	Entrust Certification Authority - L1K
US	Entrust Inc.	See www.entrust.net/legal-terms	Entrust Root Certification Authority - G2
US	Entrust Inc.	www.entrust.net/CPS is incorporated by reference	Entrust Root Certification Authority
BM	QuoVadis Limited		QuoVadis Root CA 2
US	Equifax	Equifax Secure Certificate Authority	
DE	SAP Trust Community		SAP Passport CA
DE	SAP-AG		SSO_CA
CH	SwissSign AG		SwissSign Gold CA - G2
CH	SwissSign AG		SwissSign Platinum CA - G2
CH	SwissSign AG		SwissSign Silver CA - G2
US	thawte Inc.	Certification Services Division,	thawte Primary Root CA - G3
IE	Baltimore	CyberTrust	Baltimore CyberTrust Root
US	VeriSign Inc.	VeriSign Trust Network,	VeriSign Class 3 Public Primary Certification Authority - G5
GB	COMODO CA Limited		COMODO RSA Organization Validation Secure Server CA
US	Symantec Corporation	Symantec Trust Network	Symantec Class 3 Secure Server CA - G4
US	GeoTrust Inc.		GeoTrust Global CA

C=	O=	OU=	CN=
US	GeoTrust Inc.		GeoTrust SSL CA - G3
GB	COMODO CA Limited		COMODO RSA Certification Authority

Data center hosting and certification

SAP Cloud Platform is an open platform-as-a-service offering for developing cloud applications in a fully provisioned environment. For more information about SAP's cloud platform, see SAP Cloud Platform.

Using a cloud-based integration platform imposes dedicated security measures on the software vendor (SAP) that hosts the platform as well as on those (the customers) who use the platform. SAP processes customers' sensitive data and saves it on its own data center. Data centers are sensitive entities that are exposed to hazards on many fronts. SAP equips its data centers with security measures to protect customers' data from unauthorized access and hazards. For more information about the security aspects of SAP Cloud Platform, see the Security section in the *SAP Cloud Platform Integration guide*.

The SAP Ariba Cloud Integration Gateway is currently hosted only in SAP's Germany data center, St. Leon-Rot. For more information about the IP address range in the St. Leon-Rot data center, see the *Regions, Hosts, and IP Ranges Available for the Neo Environment* table, in the Regions and Hosts section of the *SAP Cloud Platform guide*.

A series of quality seals and certificates shows how compliant a given data center is with all the necessary security precautions. Every certification involves an inspection of certain parameters or criteria. Many certification organizations perform their inspections in accordance with various standards. Multiple auditing firms conduct audits based on national and international standards, such as ISO 27001, SOC 1 /SSAE 16 and SOC 2. The SAP data center is also audited according to these standards. Once the audit is successfully passed, the data centers receive a certificate or attestation report verifying their compliance with the respective standard.

SAP ensures that these certificates are valid at every data center where cloud solutions are run. For more information about SAP's certificates, see Certificates. For more information about the certification of St. Leon-Rot, see the Certificate page.

Viewing the Home page

The **Home** page displays the following:

Integration Projects	Display the table of projects.
	Allows you to create or edit a project.
	Gives you the opportunity to copy or delete a project.

Tools	Test your connection to Ariba Network.
	Test the syntax of your transaction document.
	Test the transformation of your transaction document.
Transaction Tracker	Track the transaction documents that you have sent and received.
	Download payloads and attachments.

In the top left corner of the application open the *Navigation* menu. From this menu you get access to the **Home** page from anywhere in the application. There, you also find the **My Configurations**, **Resources**, and the **Test Central** pages.

My Configurations	This is an overview page to have quick access to all configured projects, its connections, mappings, cross references, and authorizations.
Resources	This pages contains documentation and connection requirements.
Test Central	This page lists the available test scripts and also allows you to create custom test scripts.

Related Information

How to add your ERP system information

Context

The SAP Ariba Cloud Integration Gateway asks you for the ERP system information only the first time you log in to the gateway. In case you need support with the SAP Ariba Cloud Integration Gateway, this information is helpful to connect you with the support team, which is best acquainted with your ERP system.

Procedure

1. Select your
   a. *ERP name*
   b. *ERP version*
   c. *Middleware*

2. Click **Save**.

Results

The SAP Ariba Cloud Integration Gateway **Home** page appears.

Related Information

[All procedures at a glance [page 9]](#)

Configuring an Ariba cloud integration project

With a project, you set an end point for your connection with the Ariba Network and configure, as well as test, the integration with one or more customers.

About Ariba cloud integration projects

To keep it simple, and if your system setup is suitable, it is recommended to integrate with all customers in one project.

Basic Information ➡ Connection ➡ Mappings ➡ Cross Reference ➡ Test ➡ Deployment

When you create a project, do the following:

- Configure a connection to your end point and to the Ariba Network.
- Configure your data map for transaction documents to Ariba Network.
- Setup the buyer and supplier profile information.
- Test your project configuration and sign off to production.

Related Information

How to provide basic information [page 30]
How to configure Ariba Network connection [page 30]
How to configure data maps for incoming and outgoing transaction documents [page 33]
How to specify buyer and supplier information [page 34]
How to test your project configuration [page 36]
How to schedule and activate the project on the production environment [page 40]

About the Ariba Network connections

The Ariba Network connection defines the communication channel that is used to exchange data from your system to the Ariba Network.

> i Note
>
> SAP Ariba Cloud Integration Gateway currently supports only secure communication channels. SAP does not allow the use of non-SSL channels with SAP Ariba Cloud Integration Gateway because of security concerns.

For each connection you decide to use it with one or all document types.

To connect using VAN, choose *Select VAN (Optional)*. Choosing this option prepopulates all the necessary fields for your connectivity using the VAN previously configured in the SAP Ariba Cloud Integration Gateway. You are not required to upload any certificate as it is defaulted by the VAN connection.

The following table describes all fields for the configuration in detail:

EDI Transport Type	Field Name	Description
HTTPS, AS2, and RNIF	*Environment*	The default value is *TEST / PRODUCTION*. This value allows you to use this connection for testing and production purposes. You may also configure a connection specific as *TEST* or *PRODUCTION*. **i Note** Declare at least one connection per project for productive use.
	Document Format	You can choose one of the following formats based on the EDI transport type: • UN-EDIFACT • ASC-X12 • OAGIS • PIDX
	Document Type	The default value for this field is *ANY*, which means that you use this transport type for all available document types. You might also select only one document type.
	URL	The URL where you want to receive your transaction documents. It is a free text field and your browser validates your entry. A valid URL starts with `HTTPS://`.

EDI Transport Type	Field Name	Description
	Authentication Type	You can choose between *Basic* and *Certificate* based authentication.
		Basic This authentication type needs your username and password.
		> **i Note** You need to get a special user from the Cloud Identity Service Registration to use this authentication method. To get this user, select *Basic* and follow the instructions. You can reset the password from the Cloud Identity Service portal at https://aribaoperations.accounts.ondemand.com. When you reset the password, use the same email ID that was used for creating the original account.
		Certificate This is done within a dialog that enables you to add or reuse certificates. If you want to reuse a certificate that you already added, select it in the *Certificate Name* section. The certificate must match the certificate that is configured for the Ariba solution to which you need to send the transaction document.
AS2	*Ariba AS2ID Test*	This field is the Ariba AS2 ID for Test and cannot be changed. It is for your reference only.
	Ariba AS2ID Production	This field is the Ariba AS2 ID for Production and cannot be changed. It is for your reference only.
	Trading Partner AS2 ID	This is your AS2 ID.
	Ariba VAN Interchange ID	This field contains your Ariba VAN Interchange ID.
	VAN AS2 ID	This field contains your VAN AS2 ID.
	MDN Type	You can choose to use the synchronous or the asynchronous MDN type.
	MDN URL	This is the URL where you want to receive the Message Disposition Notifications.
	Secure/Multipurpose Internet Mail Extensions (S/MIME) Type	Possible values are: • signed • encrypted • signedAndEncrypted • plain

EDI Transport Type	Field Name	Description
	Digital Certificate Encryption Algorithm	Available algorithms are: • RC2 • TripleDES • AdvancedEncryptionStandard-128 • AdvancedEncryptionStandard-192 • AdvancedEncryptionStandard-256
	Digital Certificate Signing Algorithm	Available algorithms are: • Secure Hash Algorithm 1 • Secure Hash Algorithm 2-224 • Secure Hash Algorithm 2-256 • Secure Hash Algorithm 2-384 • Secure Hash Algorithm 2-512 • MD Algorithm
	Message Encryption Certificate	Paste your certificate here. Leave this blank if the same certificate is used in *Authentication Certificate*.

> **i Note**
>
> AS2 files are sent with the same filename every time. SAP Ariba does not provide unique filenames on the AS2 file. For unique identification, utilize the MessageID within the payload.

About mappings for transaction documents

Ariba Network creates a mapping, between your transaction document format and the format used by the Ariba Network, from your defined data maps.

You always use your own format to configure data maps. It does not matter if you are the receiving or sending party, you do not need to consider the format of the Ariba Network. The format of the Ariba Network and its mappings are defined in the background.

Fieldname	Description
Direction	The direction depends on if you want to receive or send this document within this project. Use *receive* for transactions sent to you or *send* for transactions sent from you.

Fieldname	Description
Document Format	Here you can see the format of the transaction document that you have chosen under **Connection**. Possible values are: *UN-EDIFACT* *ASC-X12* *OAGIS* **PIDX** **EANCOM 97** **EANCOM 2002**
Document Format Version	For every document format, normally multiple versions exist. Choose one of the supported versions for your document format from the dropdown menu. The entries in the menu depend on your document format choice.
Document Type	Defines the type of document you want to create a mapping for. The type code depends on the document format. Use the supported document types listed in: About document types [page 4]

About buyer and supplier information

Enhance your mapping with a set of technical qualifiers and IDs.

This additional information is content from your transaction document. By extracting this specific information and cross referencing it to your Ariba Network ID, the document is routed to your trading partner through Ariba Network. While the mapping is always done against Ariba Network format, the cross reference data is the way to define specific data for you and your trading partner. All cross references you created in a project are available in every project that has the same document format definition (see step *Connection*). This means you need to be careful when you are editing cross references, because they could be used in another project.

Table 2: Fieldname and description of buyer and supplier information

Fieldname	Description
Trading Partner Ariba Network ID	This is your own Ariba Network ID. You cannot change this, it is connected to yourAriba Network account.
Trading Partner EDI Qualifier	This field contains the qualifier that defines the type of ID that is used in the *Trading Partner EDI Interchange ID*. ⚙️ Example If you use your DUNS number as seller interchange ID the qualifier is 01. List of valid EDI qualifiers [page 27]
Trading Partner EDI Interchange ID	This field can contain any identifier. It is a free text field. Fill it with an identifier that is aligned with your defined qualifier.

Fieldname	Description
Trading Partner EDI Group ID	This field can contain any identifier. It is a free text field. Fill it with your EDI Group ID.
Customer Name	This field is only available in case you have chosen to integrate with all customers at the beginning of the project configuration. Select the customer you want to trade with.
Customer Ariba Network ID	This is Ariba Network ID of the customer. It is connected to the customers Ariba Network account.
Ariba Qualifier ID	This field contains the qualifier that defines the type of ID that is used in the *Ariba Interchange ID*. This is predefined and cannot be changed.
Ariba Interchange ID	This field contains the identifier that is aligned with the defined qualifier and is automatically filled.
Customer EDI Group ID	This field can contain any identifier with up to **14 characters**. It is a free text field. Fill it with your customers EDI Group ID.
Trading Partner OAGIS ID *Customer OAGIS ID* *Trading Partner DUNS* *Customer DUNS*	The instance of an entity within the scope of the integration. Trading partner DUNS and customer DUNS are applicable when you use PIDX-based integration.
Ariba VAN Interchange ID	This field can contain any identifier. It is a free text field. Fill it with your Ariba VAN Interchange ID.
GSI EAN ID	This free text field can contain any identifier. GSI EAN ID applies to the trading partner when you use EANCOM-based integration.

Table 3: List of valid EDI qualifiers

Qualifier	Description	Qualifier	Description
01	Duns (Dun & Bradstreet)	24	The College Board's Admission Testing Program 4-Digit Code of Postsecondary Institutes, or ATP
02	SCAC (Standard Carrier Alpha Code)	25	American College Testing Program 4-Digit Code of Postsecondary Institutions, or ACT
03	FMC (Federal Maritime Commission)		
04	IATA (International Air Transport Association)	26	Statistics of Canada List of Postsecondary Institutions
08	UCC EDI Communications ID (Comm ID)		
09	X.121 (CCITT)	27	Carrier Identification Number as assigned by Health Care Financing Administration (HCFA)
10	Department of Defense (DoD) Activity Address Code	28	Fiscal Intermediary Identification Number as assigned by Health Care Financing Administration (HCFA)
11	DEA (Drug Enforcement Administration)		
12	Phone (Telephone Companies)	29	Medicare Provider and Supplier Identification Number as assigned by Health Care Financing Administration (HCFA)v
13	UCS Code (The UCS Code is a Code Used for UCS Transmissions; it includes the Area Code and Telephone Number of a Modem; it Does Not Include Punctuation, Blanks or Access Code)		
		30	U.S. Federal Tax Identification Number
14	Duns Plus Suffix	32	U.S. Federal Employer Identification Number (FEIN)
15	Petroleum Accountants Society of Canada Company Code	34	Medicaid Provider and Supplier Identification Number as assigned by individual State Medicaid Agencies in conjunction with Health Care Financing Administration (HCFA)
16	Duns Number With 4-Character Suffix		
17	American Bankers Association (ABA) Transit Routing Number (Including Check Digit, 9 Digit)		
18	Association of American Railroads (AAR) Standard Distribution Code	35	Statistics Canada Canadian College Student Information System Institution Codes
19	EDI Council of Australia (EDICA) Communications ID Number (COMM ID)	36	Statistics Canada University Student Information System Institution Codes
20	Health Industry Number (HIN)	37	Society of Property Information Compilers and Analysts
21	Integrated Postsecondary Education Data System, or (IPEDS)	AM	Association Mexicana del Codigo de Producto (AMECOP) Communication ID
22	Federal Interagency Commission on Education, or FICE	NR	National Retail Merchants Association (NRMA) - Assigned
		SN	Standard Address Number
23	National Center for Education Statistics Common Core of Data 12-Digit Number for Pre-K-Grade 12 Institutes, or NCES	ZZ	Mutually Defined

About configuration confirmation

Before you get to test your integration project you have to confirm your project configuration.

This page appears when selecting **Next** on the *Cross Reference* step. Review your configuration for each step. To edit any part of your project click the pen symbol in the *Details* column. Select the *Information* symbol to see all relevant data for that part of your project.

Sections	Description
Configuration Confirmation	Shows data from the *Basic Information* step. Not editable.
Connection Details	Displays details for connections. The available columns are: *Customer*, *Document Type*, *Transport*, *URL* and *Environment*.
Transaction Documents for the Project	Displays details for mappings. The available columns are: *Customer*, *Direction*, *Document Type*, *Format*, *Format Version* and *Data Map Status*.
Cross References	Displays details for cross references. The available columns are: *Name*, *Standard*, *Type*, *Value* and *Status*.

About project testing

The project testing is the last step before deployment.

General

- After you complete the configuration of your project, it is recommended that you test the project before deployment. Designed as a self-service, you are responsible to choose the correct test scripts. Please review your configuration thoroughly and define your test scenario accordingly.
- The SAP Ariba Cloud Integration Gateway provides you with test cases for all document types. A group of test cases is a test script.
- During testing, the connection and document types are taken from the project. The payload for the transaction documents is a standard payload used for testing purposes.
- There are two types of test cases:

  Inbound Communication from supplier to Ariba Network

  Outbound Communication from Ariba Network to the supplier

  Only outbound documents have the payload and attachments.
- Test scripts can have multiple test scenarios. Each test scenario consist of multiple test cases. The test cases in a test scenario are executed in a sequential order. You can opt to select different test scenarios from the available list.
- Custom values in test cases are specific for buyers. If you change the value during your test script configuration it changes for all test cases for that buyer.
- You can define characteristics for documents, such as the value, mandatory, and modifiable. The characteristic is globally applicable, but you can override it for individual test cases.

- A test case can consist of multiple documents per document type. If one of these documents passes the test and gets the status *Completed* the test case is considered successful.

Requirements

- Your project is fully configured.
- You checked and confirmed your configuration.

Limitations

- Each project can only have one test script.
- Once a test is scheduled, it cannot be modified.
- Only outbound test cases can be rerun.
- The results page shows only a status and an expected result for a test case. To see details for each message look at the **Transaction Tracker**.

Test Script and Scheduling

- The test script for a project is configured in the project step **Test**.
- Within the step **Test** all test cases related to the selected document types and customer are available. TheSAP Ariba Cloud Integration Gateway preselects required test cases. Select optional test cases manually.
- Schedule the start of your testing. When you return to the project after your scheduled date and time, you are directed to the test results page.

Test Results

- The **Test** step in the project wizard displays the test results, after the scheduled time.
- Test results are retrieved dynamically, so the first load after executing the tests might take some time.
- Test script status stay pending, as long as there are unfinished test cases.
- Rerun failed outbound tests from the **Test** step.

Creating an Ariba cloud integration project

Creating a project requires some configuration steps before you can deploy it on production.

Select **Create a new Integration Project** on the *Home* page to start a new integration project.

How to provide basic information

Add some basic information to your integration project as the first step of the project wizard.

Context

Procedure

1. Enter a *Project Name*.
2. Select a customer to integrate with.
3. Select **Next**.

Related Information

[All procedures at a glance [page 9]](#)

How to configure Ariba Network connection

Decide which connection is going to be used for this project and follow the procedure:

Context

You can either choose an existing connection or add a new connection.

Before deploying a project, you can test the connectivity configured for the project. This capability helps you validate the connection details that you have entered in the Connection page and ensure the connectivity between SAP Ariba Cloud Integration Gateway and your SAP Ariba system.

> **ℹ Note**
>
> AS2 connections currently don't support compressed messages.

> **ℹ Note**
>
> To facilitate traffic between the SAP Ariba Cloud Integration Gateway and the middleware or the ERP system, you might need to configure the firewall settings to permit unbound traffic from the following IP address range:
>
> 155.56.128.1 to 155.56.255.254

Procedure

- **General steps for HTTPS, AS2, and VAN connections:**
  a. Choose the *Transport Type*.
  b. Define the *Environment* of your connection.
  c. Define the *Document Format* for the connections of this integration project.
  d. Enter the name for your connection in the *Name* field.
  e. Define the *Document Type* for this connection in the *Connect To Trading Partner* section.
  f. Enter the *URL* for your service, including host, port and location of the service.
  g. Choose the *Authentication Type* for your connection:

    ○ *Basic*
      Insert your *Username* and your *Password* that Ariba Network uses for authentication.
    ○ *Certificate*
      Download the certificate and deposit it in your system.
  h. In the *Connect Trading Partner to CIG* section, choose your *Authentication Type* to connect to Ariba Network:

    ○ *Basic*
      Enter your *Username* and your *Password* used for authentication.

      > **ℹ Note**
      >
      > You need to get a special user from the Cloud Identity Service Registration to use this authentication method. To get this user, choose *Basic* and follow the instructions.
      >
      > You can reset the password from the Cloud Identity Service portal at https://aribaoperations.accounts.ondemand.com. Ensure that you use the same email ID that was used for creating the original account.

    ○ *Certificate*
      Click in the *Authentication Certificate* field. This opens the certificate dialog. Add your certificate or reuse an existing one. If you want to reuse a certificate that you already added, choose it in the *Certificate Name* section.
      The certificate must match the certificate that is configured for the Ariba solution to which you need to send the transaction document.

If you configure an HTTPS connection, the procedure ends here.

- **Additional steps for your AS2 connection**

    a. In the section *Connect To Trading Partner*, check *Use same URL for acknowledgment* or provide an `Acknowledgment URL`.

    b. Enter the `Trading Partner AS2 ID`.

- **Additional steps for your VAN connection**

    a. In the *Connect To Trading Partner* section, check *Use same URL for acknowledgment* or provide an `Acknowledgment URL`.

    b. Enter the `VAN AS2 ID`.

- **Additional common steps for your AS2 and VAN connection**

    a. Specify values for the following:

        ○ `MDN Type`
        ○ `MDN URL`
        ○ `S/MIME Type`
        ○ `Digital Certificate Encryption Algorithm`
        ○ `Digital Certificate Signing Algorithm`

    b. In the section *Connect Trading Partner to CIG*, check *Use same certificate for message encryption* or enter a `Message Encryption Certificate`.

Results

Click **Save** to send the connection details to the target system and the response from the target system back to customers. In future, when you want to create a new connection, you are presented with a table listing all the connections available for reuse. To reuse an existing connection, click the down arrow icon of the required connection in the table **Reusable Connections**. The selected connection is now available in the table **Connection Details** for reuse with modifications as needed.

> ℹ **Note**
>
> To avoid conflicts when testing, the SAP Ariba Cloud Integration Gateway removes connections that are not compatible with the selected connection from the table **Reusable Connections** based on the document format and transport type.

Related Information

How to configure data maps for incoming and outgoing transaction documents

Add one or multiple data maps to use them within an integration project for both, incoming and outgoing transaction documents.

Context

You defined the connection for this project in the previous step. Within this step you create mappings for every transaction document type you need for this project.

> **i Note**
>
> The mapping is not required for projects with cXML document format and you would be prompted to move to next step.

Procedure

1. Select **Add new Data Map** or choose an existing data map.
2. Click **Select** and then select **Edit** in the *Action* column.
3. Select the following:

   o *Direction*
   o *Document Format Version*
   o *Document Type*

4. Select **Save**.

Next Steps

Create another data map or select **Next**.

Related Information

[About mappings for transaction documents [page 24]](#)

How to specify buyer and supplier information

Specify data for supplier as well as buyer for a specific project.

Context

In the previous step you created data maps and selected **Next**. In this step of the project wizard you add some project specific data for you and your buyer. You can either add a new cross reference or edit an existing cross reference. If the data is already defined in the master characteristic, those values would appear here.

> **i** Note
>
> Cross references are not required for projects with cXML document format and you would be prompted to move to next step.

Procedure

Scenario: No cross references available for that project

1. Enter your cross references according to the document format you defined in step **Connection**:

UN-EDIFACT, ASC-X12, EANCOM 97, and EANCOM 2002	OAGIS
Trading Partner EDI Qualifier	*Trading Partner OAGIS ID*
Trading Partner EDI Interchange ID	
Trading Partner EDI Group ID	

2. Select **Save**.

   Your cross references are saved. The next screen is for your customers' cross references.

3. Enter cross references for your customer according to the document format you defined in step **Connection**:

UN-EDIFACT, ASC-X12, EANCOM 97, and EANCOM 2002	OAGIS
Customer EDI Group ID	*Customer OAGIS ID*

4. Select **Save**.

   You see the *Cross References* overview table. Check in the *Cross References* overview table if your entries are correct.

Scenario: Project with multiple customers

5. Select **Add new Cross Reference** to add cross references for another customer.

6. Select the customer from the *Customer Name* dropdown in the *Environment: TEST* section.

7. Enter cross references for your customer according to the document format you defined in step **Connection**:

UN-EDIFACT, ASC-X12, EANCOM 97, and EANCOM 2002	OAGIS
Customer EDI Group ID	*Customer OAGIS ID*

8. Decide if you want to use the same values also in the production environment or enter the values for productive use in the *Environment: PRODUCTION* section.

9. Select **Save**.

   Check the result in the *Cross References* overview table and repeat these steps as necessary.

Scenario: Edit existing cross references

10. Click **Select** in the *Action* column and then select **Edit**.

11. Enter cross references for your customer according to the document format you defined in step **Connection**:

UN-EDIFACT, ASC-X12, EANCOM 97, and EANCOM 2002	OAGIS
Customer EDI Group ID	*Customer OAGIS ID*

12. Select **Save**.

Next Steps

Create another cross reference or select **Next**.

Related Information

About buyer and supplier information [page 25]
All procedures at a glance [page 9]

How to confirm your project configuration

Review and confirm your project configuration before you go to the *Test* step.

Context

The *Configuration Confirmation* page displays all relevant data of your project as an overview. Review your configuration for each step, having the context of all steps at a glance.

Edit parts of your project selecting the pen symbol in the *Details* column.

Procedure

1. Review and edit your
   a. connection in the *Connection Details* section.
   b. mappings in the *Transaction Documents for this Project* section.
   c. cross references in the *Cross References* section.
2. Select
   - **Confirm** to go on with the *Test* step.
   - **Close** to go back to the Home page and come back later for the confirmation.

Related Information

How to test your project configuration

Test your configuration from the previous steps in a self service scenario.

Context

Basic Information → Connection → Mappings → Cross Reference → **Test** → Deployment

This step is to test your integration project before you deploy it to production. In addition to preselected test cases, select optional test cases according to your requirements. All selected test cases together are a test script. Your

customized test script uses your configuration from the previous steps. Before testing your project configuration, you can do the following:

- Define master characteristics
- Create test script

> ℹ **Note**
>
> You can configure only one test script for a project. This means, after you select **Run Test**, you cannot modify your test script or add other test cases. Even after the test is run, you can't change the test script.

Related Information

Editing and deleting an Ariba cloud integration project

You can delete or edit a project that is not yet deployed to production.

When editing or deleting a project there might be a reused certificate included. If you delete a project, the certificate will remain available for all other project that use this certificate. In case you delete all projects using the certificate, it will also be deleted.

When you edit a certificate within a project, you will be notified if you are changing a reused certificate. If you continue changing this certificate, be aware that this change is also valid for all other projects using this certificate.

1. Go to the *Home* page
2. Click on **Select** in the *Action* column.
3. Select
   - **Delete Project** and confirm the deletion.
   - **Edit Project** which leads you to the project wizard.

Managing authorization

You can create a new account, access your profile page, and change password from the SAP Ariba Cloud Integration Gateway.

You can manage your email and password authentication from the SAP Ariba Cloud Integration Gateway.

How to manage authorization

Context

Perform the following steps to create a new account and change your password and email:

Procedure

1. Navigate to ▮▶ **Menu** ❯ **My Configurations** ❯ **Authorization** ❯.
2. Click **Create Account** for the **Cloud Identity Service User**.

   The message `Please check your emails for CIS registration. Registered email is : <your registered email id>` appears.
3. Click **OK**.
4. Check your registered email for an email from `notification@sapnetworkmail.com`.
5. To activate your account, click the **Click here to activate your account** link in the email.

   The **Please activate your user account** page appears.
6. Enter your password and click **Submit**.

   The **User account successfully activated** page appears.
7. Click **Continue**.

   The **Profile** page appears and displays the **User name** and **User ID**.

   To edit, click **Edit** or to sign out, click **Sign out**.
8. Navigate to ▮▶ **Menu** ❯ **My Configurations** ❯ **Authorization** ❯.

   The **Cloud Identity Service User** now includes the User ID, for example P000XXX, the **Change Password** and the **Change Email** buttons.
9. To change the password, click **Change Password**.

   The **Change Password** dialogue box appears.
10. Enter the new password and click **Submit**.

    You can now log in to your SAP Cloud Identity account using the new password.
11. To change the email, click **Change Email**.

    The **Change Email** warning appears.
12. Click **Accept** to change the authentication email address to your login email address.

    Your email is updated.

    > ℹ **Note**
    >
    > This email address is used by CIG for transactional communication, when you select **Basic** as your **Authentication Type**.

How to manage connections, cross references, and certificates from the My Configurations page

Context

In the *My Configurations* page, you can manage connections, cross references, and certificates without editing your project.

In the *My Connections* area, you can edit a connection that you have already used in a project or delete a connection that is not longer used in any projects. The modification to the connection in a project that is in production adds to the partner directory directly.

In the *My Cross References* area, you can edit a cross reference. To do so, you can use the edit icon provided for all the cross references that belong to the projects in the production state.

In the *List of Certificates* page, you can remove a certificate.

Procedure

1. Navigate to ▶ **Menu** ❯ **My Configurations** ❯.
2. In the *My Configurations* page, do one of the following:
   ○ Click **Connections**. In the *My Connections* area, you can edit or delete connections.
   ○ Click **CrossRefs**. In the *My Cross References* area, you can edit cross references of the projects that are in the production state.
   ○ Click **Certificates**. In the *List of Certificates* area, you can delete a certificate.

Deploying a project to production

Read everything you need to know about project deployment, its prerequisites and how it works.

About project deployment

Deploy your project to use it in the production environment.

You can deploy a fully configured project to production. The move to production deploys all newly configured settings. Any existing setting will be retained.

How to schedule and activate the project on the production environment

This is the final step of an Ariba cloud integration project configuration.

Context

After you have completed all steps of the wizard, the final step is to schedule the deployment to production.

Procedure

1. Log in to SAP Ariba Cloud Integration Gateway.
2. Edit your project and go to the **Test** step.

   The **Project Self Test Results** page appears.

   > ℹ **Note**
   >
   > A tick-mark under the **Pass/Fail** column indicates that the project has passed the self-test.

3. Select **Run Buyer Test** or **Skip Buyer Test**.

   The **Go Live** button is enabled.
4. Specify the date and time to schedule the deployment to production in *Mark Project Active On*.

5. Click **Go Live**.

Related Information

All procedures at a glance [page 9]

Tracking documents with SAP Ariba Cloud Integration Gateway

Keep track of your documents using a variety of criteria.

About tracking transaction documents

Use the monitoring for the following:

- Display all documents in a table, that match your search criteria. The table shows some information about the transaction.
- Display document details, which contains **Details**, **Activity**.
- Download source payload, target payload, attachments, MDN, or all files of a transaction.
- Download the complete list of search results as CSV.
- Reprocess transactions as a self-service.

Use the variety of search fields as it best fits your needs. The session saves your search criteria for the next time you return to the monitoring, as long as you are not closing the session.

Search Criteria	Description
Search From	Enter date and time from when the search should start.
To	Enter date and time until which the search should end.
Transaction Number	Enter a complete document number or a substring. Ensure that the search is case sensitive and you do not use wildcard characters.

Search Criteria	Description
Document Status	If you choose to type the status, it has to be an exact match to the values from the pull-down. Otherwise the search will not find anything. Use the following statuses: • *COMPLETED* Your transaction has been delivered to the final destination. • *ERROR* Your transaction has either been failing during processing or could not be delivered to the final destination. • *FAILED* Your transaction has either been failing during processing or could not be delivered to the final destination. • *PROCESSING* Your transaction is in an active process. The next status would be either *COMPLETED*, *FAILED* or *RETRY*. • *RETRY* Your transaction is in an automatically invoked loop. The delivery to the final destination ended with an error and is now retried 10 times with an timeout of 1 hour between each try.
Document Type	Use this to narrow down search result to a specific document type. Use the supported document types listed in: About document types [page 4]
Sender	Enter the name or the Ariba Network ID of the sender. ℹ Note The search is case sensitive and does not allow wildcard characters.
Receiver	Enter the name or the Ariba Network ID of the receiver. ℹ Note The search is case sensitive and does not allow wildcard characters.

Downloads

You can download the files that are available for the specific transaction. Possible files are the source payload, the target payload,MDN (AS2), and the attachments. Download single transactions as well as multiple transactions at a time. Use the checkboxes and the button **Download** to select and start your download.

In case of XML validation errors, you can download the error report from the error message popup.

Reprocess Transactions

The most common use case for this function are transactions with status *Failed*. As there are other use cases possible the reprocessing function is unrestricted. With every try to reprocess a transaction a new transaction will be generated. This new transaction will have the same *Transaction Number* as the initial transaction. By searching for this *Transaction Number* you can keep track on all relevant transactions.

How to track transaction documents

You can use search criteria to track your documents.

Context

Ariba Network processes your document. This process can be tracked in the monitoring section of the SAP Ariba Cloud Integration Gateway. You can get a quick overview with the table below the search section or go into details by selecting a transaction.

Procedure

1. Go to **Transaction Tracker**.
2. Fill the form with your search criteria:
   a. *Search From* (date and time)
   b. *To* (date and time)
   c. *Transaction Number*
   d. *Document Status*
   e. *Document Type*
   f. *Sender*
   g. *Receiver*
3. Click **Search**.
4. Analyze the results. If needed, open the document details by selecting the **Transaction Number**.

Next Steps

- You can sort, as well as filter every column to adjust the result to your needs. Download the list of results with **Results Export**.
- Download the available files for a transaction using the checkboxes and the **Download** button in the search result table.

In case of XML validation errors, you can download the error report from the error message. To view the error message, click the error message icon in the Document Status column. From the error message popup, click **Download**.

- Reprocess transactions using the checkboxes and the **Reprocess** button in the search result table.
- If needed, discard all values with **Clear** and enter new criteria as in Step 2.

Related Information

All procedures at a glance [page 9]

About test tools

The testing functionalities are available as standalone tools.

Ensure that the connection to the Ariba Network, the message structure, as well as the transformation meets the requirements. The SAP Ariba Cloud Integration Gateway provides the necessary validation tools to perform these tests proactively or as part of the troubleshooting.

Testing the connection to Ariba Network

Ensure your connection is working with the connection testing tool. The connection test is an independent feature that you can use standalone.

However in the context of SAP Ariba Cloud Integration Gateway, the test connection tool enables you to test your connections whenever required. You can test the connection as part of configuring a new connection within a project or during troubleshooting in case a message fails. You can edit the connection and save the details to start testing the connection.

How to test the Ariba Network connectivity

Context

Validate the connection for your transaction documents with the Ariba Network.

Procedure

1. Log in to SAP Ariba Cloud Integration Gateway and click the user information on top-right corner of the page.
2. Choose **Basic Data** for the user.
3. Click **Home** option and click **Test Connectivity**.
4. Put your content in *Source Input*.
5. Enter the following:
    a. *URL*
    b. *Username*
    c. *Password*
    d. *Partner ID*
    e. *Content Type*

`text/xml` for cXML and OAGIS

`text/plain` for UN-EDIFACT and ASC-X12

6. Click **Submit**.

Results

Check `Result` to see if your connection is valid. In case it is not valid, you get a message that explains the failure.

Next Steps

Select **Clear** to start with a new validation and populate the fields starting with Step 2.

Validating syntax in transaction documents

Verify and ensure the accuracy of the document structure with the help of the syntax validation tool.

About syntax validation

Ariba Network validates transaction documents sent by suppliers. Ensure that the data and format complies with the requirements of Ariba Network.

Fieldname	Description
Document Format	Use the following transaction document formats: • *cXML* • *UN-EDIFACT* • *ASC-X12* • *OAGIS* • *PIDX* You can only select a format that complies with the document type.

Fieldname	Description
Document Format Version	All supported versions of your document format are available: • *D96A* for UN-EDIFACT • *004010* for ASC-X12 • *0* for cXML • *9.2* for OAGIS • *1.6.1* for PIDX
Document Type	You can validate the syntax for the supported document types.
Content Type	Select one of the following content types: • *text/xml* • *application/edifact* • *application/edi-x12* • *application/xml*

How to validate syntax

Context

With this tool, validate the syntax of your documents against industry standard schemas used in the network.

Procedure

1. Go to **Schema Validation**.
2. Select your:
   a. *Document Format*
   b. *Document Format Version*
   c. *Document Type*
   d. *Content Type*
3. Paste your content for the transaction document in the *Source Input* text box.
4. Click **Validate**.

   The tool validates the mandatory cXML fields with the transaction document content as per the Ariba Network cXML guidelines.

Results

Check *Result* to see if your document is valid. In case it is not valid, you see an error with details.

Next Steps

Select **Clear** to start with a new validation and populate the fields starting with Step 2.

Related Information

Validating the transformation of transaction documents

Use the test transformation tool to test the XSLT.

About test transformation

To test the XSLT, it is required to populate the following fields:

Source Document Type *Target Document Type*	Available document types.	Your selection here determines the values in the next fields. Use the same value, or the corresponding value for the target format, in both *Document Type* fields.
Document Source Format *Document Target Format*	Available values are depending on the document type: • cXML • OAGIS • ASC-X12 • UN-EDIFACT	

Document Source Format Version *Document Target Format Version*	All supported versions of your document format are available: • *D96A* for UN-EDIFACT • *004010* for ASC-X12 • *0* for cXML • *9.2* for OAGIS	
Source Content Type *Target Content Type*	Available values are depending on the document format: • *application/edifact* for UN-EDIFACT • *application/edi-x12* for ASC-X12 • *text/xml* for cXML and OAGIS	
Source Input	Enter your message content here, for example, UN-EDIFACT payload.	

How to validate the transformation with XSLT

Transform your document using XSLT.

Context

If the syntax validation was successful, use this step to test the transformation of your documents. If an error occurs, the error contains an explanation.

Procedure

1. Select **Test Transformation**.
2. Select your:
   a. *Source Document Type*
   b. *Document Source Format*
   c. *Document Source Format Version*
   d. *Source Content Type*
3. Select the corresponding:
   a. *Target Document Type*
   b. *Document Target Format*
   c. *Document Target Format Version*
   d. *Target Content Type*

4. Enter your message content into *Source Input*.

5. Select **Validate**.

Results

See *Result*, the transformed document is available when processing is successful. In case of an error, you get a valid error message.

Next Steps

If you want to start another transformation with different values, select **Clear** and start with Step 1.

**Related Information**

[All procedures at a glance [page 9]](#)

Troubleshooting information

SSL handshake overview

SSL communication consists of a series of messages exchanged between two parties (client and server).

The SSL handshake between a client and server consists of nine steps, and appears as follows:

The SSL messages determine the parameters of the encrypted communication channel that the two parties plan to use. It is important that the client and server agree on the message details, such as the protocol version, cipher suites, secure renegotiation, or client certificate requests. Otherwise the handshake fails.
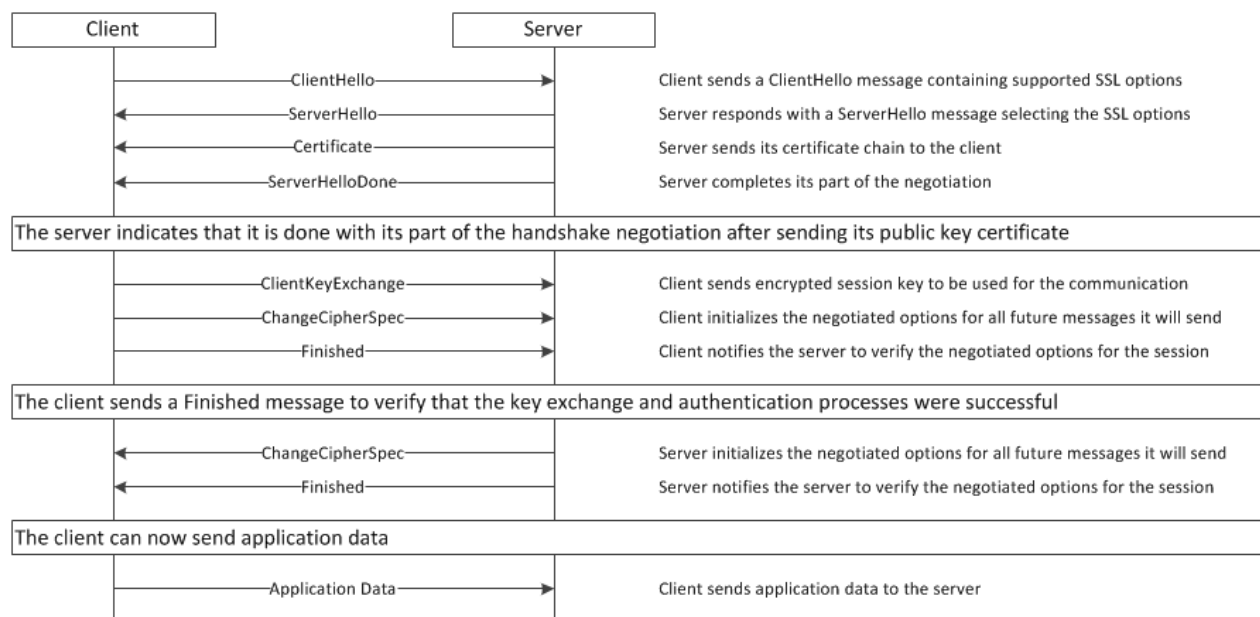
The SSL handshake has the following messaging components:

ClientHello

When a client first attempts to connect to an SSL server, it initiates the session by sending a `ClientHello` message to the server. The `ClientHello` message starts the SSL communication between the two systems.

The `ClientHello` message contains some of the following components:

Component	Content
Version	The version field contains the highest SSL version that the client supports.
Random	A random number generated by the client.
Session ID	An arbitrary sequence of bytes chosen by the server; it identifies a particular SSL session. The client may attempt to resume a previously established session by sending a non-zero session ID.
Cipher Suites	Identifies the list of ciphers suites that the client supports.
Compression	Identifies the list of compression methods that the client supports.

ServerHello

If the server is able to find an acceptable set of algorithms, it responds to the `ClientHello` message with a ServerHello message. The server may use the `ServerHello` message to allow a resumed session.

The `ServerHello` message contains some of the following components:

Component	Content
Version	The version field contains the highest SSL version supported by both the client and server.
Random	A random number generated by the server.
Session ID	Identifies a particular SSL session. If the client sends a non-zero session ID and the server locates a match in its cache, the server attempts to respond with the same value as was supplied by the client, and resume the session using the same cipher suite.
Cipher Suites	Identifies the cipher suite chosen by the server from the list of ciphers that the client supports.
Compression	Identifies the compression method chosen by the server from the list that the client supports.

Certificate

The server sends its `Certificate` message containing the server's certificate or list of (chain) certificates, depending on the selected cipher suite.

ServerHelloDone

After sending its certificate, the server sends a `ServerHelloDone` message, indicating it is done with handshake negotiation.

ClientKeyExchange

The client sends the `ClientKeyExchange` message containing the `PreMasterSecret`. The `PreMasterSecret` is sent encrypted using the public key of the server.

`ChangeCipherSpec`

Both the client and server send the `ChangeCipherSpec` message after the security parameters have been determined. The ChangeCipherSpec message activates the negotiated SSL options for the session. From this point forward, all messages are authenticated and encrypted. This stage is significant as it indicates that subsequent records are protected under the newly negotiated `CipherSpec` and keys.

Finished

Each party sends a finished message under the new algorithm, keys, and secrets. The Finished message indicates that the handshake is complete, and the parties may begin to exchange application layer data.

Resumed SSL Sessions

A resumed SSL session implements session identifier (session ID) to reestablish a previously negotiated session. When an SSL handshake is resumed, the client presents the session ID from the previously negotiated session. If the server finds the session ID in its cache and accepts the resumed session, it sends back the same session ID and the parties skip the public key operation. If the server does not accept the resumed session, it issues a new session ID and implements the full SSL handshake.
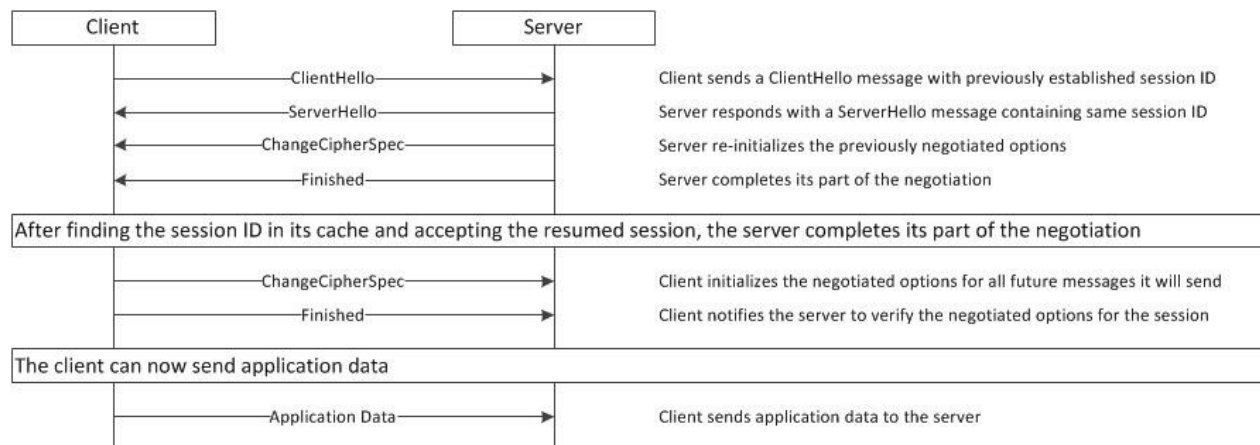
General SSL errors

Record Version Mismatch: 02

This error could indicate that the client and server do not agree on the level of SSL to use (SSLv2, SSLv3, TLS). To check if a remote server supports a particular version, use OpenSSL to run the following command (which actually checks if SSLv2 is supported): `>openssl s_client -connect hostname:443 -ssl2`

If you get the following response, SSLv2 is disabled:

- 419:error:1407F0E5:SSL routines:SSL2_WRITE:ssl handshake failure:s2_pkt.c:428:
- 420:error:1406D0B8:SSL routines:GET_SERVER_HELLO:no cipher list:s2_clnt.c:450:

Peer sent alert: Alert Fatal: bad certificate

This error can occur when the SSL server is presenting an empty CA list, which causes the client to not present its certificate at all.

iaik.pkcs.PKCSException javax.crypto.BadPaddingException: Unknown blocktype

This error might be caused by a configuration where the private key and certificate do not match (that is, they are not a pair).

Server certificate rejected by ChainVerifier

Client was presented a certificate chain that it does not trust.

Here are potential causes and corrections:

Cause	Correction
The remote server's chain is not trusted	add the root CA certificate (or at least some intermediate CA certificate from that chain) to the Client truststore
The remote server is presenting a chain with an expired CA certificate	

Cause	Correction
The remote server is presenting a chain that is out of order	Per RFC 2246, a certificate chain that looks like this: `subjectCert > intermediateCAcert > rootCAcert` can be handed out as: `subjectCert > intermediateCAcert > rootCAcert` or `subjectCert > intermediateCAcert`. To test if a remote server's chain is out of order, use the following command: `> openssl s_client -connect hostname:port -verify 6 -showcerts` This command prints each certificate in the order it was presented. Upon examination, the certificate's issuer should match the next certificate's subject, until the root is reached. The root CA certificate's issuer equals its own subject. To resolve, the remote server administrator should reconfigure the chain being handed out.

Network troubleshooting techniques and utilities

When troubleshooting network-related troubleshooting, you can use the following techniques and utilities (often core OS-provided executables) to help diagnose the cause.

ipconfig / ifconfig

The ipconfig command (on Windows) or ifconfig command (on UNIX) provides the simplest means to list network interfaces, including IP addresses for a given host.

For example, on Windows:

> Sample Code

```
D:\>ipconfig
Windows IP Configuration ...
Ethernet adapter Interface 1: Connection-specific DNS Suffix . :
IP Address. . . . . . . . . . . : 192.168.1.102
Subnet Mask . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . : 192.168.1.1
Ethernet adapter Interface 2: Media State . . . . . . . . . . : Media
disconnected.
```

Using `ipconfig /all` gives the full details of each interface (including DHCP settings and DNS server).

ping

The ping utility is the simplest means to test network connectivity to a given IP address (either local or remote).

For example, on Windows:

> **Sample Code**
>
> ```
> D:\>ping myPartner.com
> Pinging myPartner.com [69.147.125.65] with 32 bytes of data:
> Reply from 69.147.125.65: bytes=32 time=19ms TTL=54
> Reply from 69.147.125.65: bytes=32 time=39ms TTL=54
> Reply from 69.147.125.65: bytes=32 time=27ms TTL=54
> Reply from 69.147.125.65: bytes=32 time=28ms TTL=54
> Ping statistics for 69.147.125.65: Packets: Sent = 4, Received = 4, Lost = 0 (0%
> loss), Approximate round trip times in milli-seconds: Minimum = 19ms, Maximum =
> 39ms, Average = 28ms
> ```

Netstat

The `netstat` command can serve two primary purposes:

- It lists the various port numbers in use on the current host (for example, 443, 80) and their current state (for example, LISTENING); and
- It lists the various connections to and from this host and its various ports

Occasionally, corporate networks may be configured to only allow certain types of traffic (for example, HTTP or FTP) and a ping request fails. But typically, if a tcp-level ping works, then the foundation is there for other communications protocols to work.

telnet

Like the ping command, the telnet command can be used to test network connectivity to a given IP address and port on that IP address (either local or remote).

For example, from a Windows host, the following telnet response indicates that the local telnet client could not find a listening port 1520 on host myOracleHost:

> **Sample Code**
>
> ```
> D:\>telnet myOracleHost 1520
> Connecting To myOracleHost...
> Could not open connection to the host, on port 1520: Connect failed
> ```

But if that telnet command was pointed to a proper port number (for example, 1521), the console would clear (indicating the telnet session was established, and the client is awaiting the user to key in commands). In this sense, we are using telnet like a ping, but to a specific port number

Source IP Address

Every tcp request has a source IP address (that is, a "from" address) included on it when it reaches its destination. This address most likely is not the IP address shown when issuing an ipconfig command on the originating host.

Instead it is an "outbound" address, set by the network's Default Gateway or outbound proxy server. This information may be useful when the server-side network or application does IP-level filtering. There are public sites on the internet (for example, http://whatismyip.com) to which a browser can be pointed at, to provide this "outbound" IP address.

Intermittent Behaviors

Anytime there is an intermittent behavior (for example, a connection cannot be established, an established connection times out, or a request cannot find a desired resource), there could be numerous factors involved. But some common causes to keep in mind or investigate are:

- Timeout settings throughout the connection: settings on the client application, on the sending application, on components in between (such as firewall, proxy servers, load balancers) the two, etc.
- Request data sizes: consider the possibility that larger requests are causing a timeout in one of the components.
- Load-balancer presence: it could be that requests that are routed to one server node always work, but those routed to a second server node do not. To a client, this looks like an "intermittent failure".

How to troubleshoot common connection errors

Procedure

1. Check if there was a recent change or upgrade.

   If your server has stopped working after a recent upgrade it's possible that there might have been recent changes happened at your end. Verify with your technical- or network-team if there are any recent changes.
2. Check that you are using the correct URL.

   Ensure that your application has the correct URL defined (including the https protocol) to connect to SAP Ariba Cloud Integration Gateway.
3. Connection reset / Connection refused / Connection timeout.

   The http connection to the destination could not be established. This can be caused by missing Firewall clearances on the sender or receiver side or due to incorrect URLs in the communication channel.

HTTP error codes overview

HTTP errors are often caused by incorrect URLs, AS2 names, interconnected proxy servers, or too slow processing in a system. When accessing an application, every HTTP request that is received by a server is responded to with an HTTP status code. HTTP status codes are three-digit codes, and are grouped into five different classes.

The class of a status code can be quickly identified by its first digit:

- 1xx: Informational

- 2xx: Success
- 3xx: Redirection
- 4xx: Client Error
- 5xx: Server Error

> ℹ **Note**
>
> Only the error codes 4xx and 5xx are described in the next chapters.

Client error overview

Client errors, or HTTP status codes from 400 to 499, are the result of HTTP requests sent by a HTTP client. Even though these types of errors are client-related, it is often useful to know which error code a user is encountering to determine if the potential issue can be fixed by server configuration.

Error Code	Description
400 Bad Request	The 400 status code, or Bad Request error, means the HTTP request that was sent to the server has invalid syntax.
401 Unauthorized	The 401 status code, or an Unauthorized error, means that the user trying to access the resource has not been authenticated or has not been authenticated correctly. This means that the user must provide credentials to be able to view the protected resource. An example scenario where a 401 Unauthorized error would be returned is if a user tries to access a resource that is protected by HTTP authentication if enters invalid username and password.
403 Forbidden	The 403 status code, or a Forbidden error, means that the user made a valid request but the server is refusing to serve the request, due to a lack of permission to access the requested resource.
404 Not Found	The 404 status code, or a Not Found error, means that the user is able to communicate with the server but it is unable to locate the requested resource.

Server error overview

Server errors, or HTTP status codes from 500 to 599, are returned by server when it is aware that an error has occurred or is otherwise not able to process the request.

Error Code	Description
500 Internal Server Error	The 500 status code, or Internal Server Error, means that server cannot process the request for an unknown reason. Sometimes this code appears when more specific 5xx errors are more appropriate.

Error Code	Description
502 Bad Gateway	The 502 status code, or Bad Gateway error, means that the server is a gateway or proxy server, and it is not receiving a valid response from the backend servers that should actually fulfill the request.
503 Service Unavailable	The 503 status code, or Service Unavailable error, means that the server is overloaded or under maintenance. This error implies that the service should become available at some point.
504 Gateway Timeout	The 504 status code, or Gateway Timeout error, means that the server is a gateway or proxy server, and it is not receiving a response from the backend servers within the allowed time period.

Revision history

The following table provides a brief history of the updates to this guide. SAP Ariba updates the technical documentation for its cloud solutions if

- software changes delivered in service packs or hot fixes require a documentation update to correctly reflect the new or changed functionality;
- the existing content is incorrect or user feedback indicated that important content is missing.

SAP Ariba reserves the right to update its technical documentation without prior notification. Most documentation updates will be made available in the same week as the software service packs are released, but critical documentation updates may be released at any time.

Document version	Month/year of update	Updated chapter/section	Short description of change
1	January 2017	n/a	First version
2	February 2017	About Document Types	Updated to include information about PIDX.
		About the Ariba Network Connections and About Mappings for Transaction Documents	Updated to include information about RNIF and PIDX.
		Configuring the Ariba Network Connection	Updated to add information about IP range.
		About Buyer and Supplier Information	Updated to include information about Trading Partner DUNS and Customer DUNS.
		About Tracking Transaction Documents and Tracking Transaction Documents	Updated to include information about XML validation error message attachments.
3	March 2017	About the Ariba Network Connections Configuring Ariba Network Connection About Buyer and Supplier Information	Updated to include information about VAN.
		About document types	Updated to include information about: - UN-EDIFACT D96A and ASC-X12 v4010 for Goods Request (Inbound) - Application Advice - CopyRequest cXML for Purchase Order and Advanced Shipment Notice

Document version	Month/year of update	Updated chapter/section	Short description of change
		Configuring an SAP Ariba cloud integration project	Updated to include the managing authorization section.

4	April 2017	How to configure Ariba Network connection
		
		About document types
			Added information about the table listing connections available for reuse.
			
			• Renamed:
			  ○ Control to Technical Acknowledgement
			  ○ Application Advice to Functional Acknowledgement
			• Removed: Status Update
			• Added: Invoice Response

5	May 2017	About document types How to validate syntax About the Ariba Network connections	Updated to include information about: • UN-EDIFACT D96A and ASC-X12 for Transport Request • UN-EDIFACT D96A and ASC-X12 for Transport Confirmation • GS1 EANCOM for Purchase Order and Invoice • PIDX for Goods Request (Inbound) Added validation information as per Ariba Network cXML guidelines Added information about: • Ariba AS2ID Test • Ariba AS2ID Production
6	June 2017	About document types	Removed the following information: • GS1 EANCOM for Purchase Order and Invoice Updated to include information about: • GS1 GUSI for Purchase Order and Advance Shipment Notice • PIDX for Goods Request (Inbound) • ASC-X12 v4010 for Quality Notification (Inbound) • ASC-X12 v4010 for Quality Notification (Outbound) Updated information about testing.
7	July 2017	About document types	Added the following information: • EANCOM 97 for invoice. • EANCOM 2002 for purchase order and purchase order change request.

Document version	Month/year of update	Updated chapter/section	Short description of change
		How to login to the SAP Ariba Cloud Integration Gateway	Added a note on the alert message that informs suppliers of the impending expiration of their certificates.
		About the Ariba Network connections	Added a note on the support of secure communication channels with SAP Ariba Cloud Integration Gateway.
		About mappings for transaction documents	In Table 9, added EANCOM 97 and EANCOM 2002 as values in the description for the `<Document Format>` field.
		About buyer and supplier information	In Table 10, added the description for the GS1 EAN ID field.
		How to specify buyer and supplier information	In the procedure steps, added EANCOM 97 and EANCOM 2002 to the tables that describe the document formats.
		About test tools	Added sections on master characteristics and test script.
		How to configure data maps for incoming and outgoing transaction documents	Added note that mapping is not required for projects with cXML document format.
		How to specify buyer and supplier information	Added note that cross references are not required for projects with cXML document format.
8	August 2017	About document types	Added the GS1 GSU 2.1 information for the following document types: • Inventory • Scheduling Agreement Release/Delivery Schedule • Consignment Movement List
		How to manage connections and certificates from the My Configurations page	Added this new section on directly managing connections and certificates from the My configuration page.
		About tracking transaction documents	Added MDN to the list of files that you can download
		Downloads	Added MDN (AS2) as one of the possible file that you can download for a specific transaction

Document version	Month/year of update	Updated chapter/section	Short description of change
9	September 2017	About document types	Added the following documentation types: • Advanced Shipment Notice - Added DESADV for the EANCOM 2002 document type • PR - Added REMADV for the EANCOM 2002 document type
		How to configure Ariba Network connection	Added description on the capability to test connectivity
		How to manage connections, cross references, and certificates from the My Configurations page	Updated with information on directly managing cross references from the My configuration page.
		Testing the connection to Ariba Network	Updated with information on the enhanced capability to test connectivity.
10	December 2017	About the SAP Ariba Cloud Integration Gateway	Added a note about online help.

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.

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.ariba.com

SAP