Administrator's Guide for Ariba Network Integration for SAP Supply Network Collaboration
Ariba Network Integration 1.0 for SAP Business Suite
6.2 Extrinsic Elements (Extensibility) ................................................... 61
   Extrinsics in Outbound cXML Messages. ........................................... 61
   Extrinsics in Inbound cXML messages. ............................................ 61
6.3 Endpoints. ..................................................................................... 62
Document History

i Note
Before you start the implementation, make sure you have the latest version of this document. You can find the latest version at: https://service.sap.com/instguides.

The following table provides an overview of the most important document changes:

Table 1:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>2014-07-16</td>
<td>Initial version</td>
</tr>
</tbody>
</table>
1 Overview of Ariba Network Integration for SAP Supply Networ Collaboration (SAP SNC)

Ariba Network Integration 1.0 for SAP Business Suite is a non-modifying add-on for SAP Business Suite systems. It has several product instances for SAP ERP systems and SAP Supply Network Collaboration (SAP SNC) systems. This guide documents the Ariba Network Integration for SAP SNC product instance.

This add-on is required if you want to connect SAP Business Suite systems to Ariba Network. Ariba Network Integration for SAP SNC enables your SAP SNC system to send and receive messages in a format supported by Ariba, that is, cXML. You can also integrate your SAP SNC system and Ariba Network using single sign-on: in this case supplier users on Ariba Network are able to use certain functionalities of SAP SNC without having to provide their credentials every time they connect to SAP SNC.

The add-on supports the integration of a single SAP Business Suite system or of several SAP Business Suite systems with Ariba Network. The systems can be integrated directly or using a middleware. For detailed information, see SAP Community Network at http://scn.sap.com/docs/DOC-51873, System Landscape Recommendations for Ariba Network Integration 1.0 for SAP Business Suite.

1.1 Supported Processes

Message-Based Integration

Ariba Network Integration for SAP SNC supports the integration of SAP SNC with the Order Collaboration process on Ariba Network.

Message Types Used

The following cXML message types are used to enable the Order Collaboration process:

- **OrderRequest** (outbound)
- **ConfirmationRequest** (inbound)
- **ShipNoticeRequest** (inbound)
- **StatusUpdateRequest** (outbound)

**OrderRequest (Outbound)**

This cXML message enables you to transfer purchase orders (PO), changes to purchase orders, and cancellations of purchase order to Ariba Network.

Currently, the following restrictions apply to the purchase order process:

- Subcontracting purchase orders are not supported.
- The approval process for purchase orders in SAP SNC is not supported in the integration.

**OrderConfirmationRequest (Inbound)**
On Ariba Network, you can confirm or reject entire purchase orders, and you can confirm, reject, or update individual line items of purchase orders. All cases are supported by the cXML message type OrderConfirmationRequest.

The following combinations of Ariba Network order confirmation types are supported:

<table>
<thead>
<tr>
<th>Header Type</th>
<th>Allowed Confirmation Status Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>accept</td>
</tr>
<tr>
<td>AllDetail</td>
<td>allDetail, reject, unkown</td>
</tr>
<tr>
<td>Detail</td>
<td>all, but allDetail</td>
</tr>
<tr>
<td>Backordered</td>
<td>backordered</td>
</tr>
<tr>
<td>Except</td>
<td>all, but allDetail</td>
</tr>
<tr>
<td>Reject</td>
<td>-</td>
</tr>
<tr>
<td>Request to pay</td>
<td>request to pay</td>
</tr>
<tr>
<td>Replace</td>
<td>detail</td>
</tr>
</tbody>
</table>

ShipNoticeRequest (Inbound)

An incoming ShipNoticeRequest creates an advanced shipping notification (ASN) in SAP SNC, and updates the purchase order accordingly. The ASN can also contain the carrier information provided by Ariba Network.

Note

To be able to process update ShipNoticeRequest messages in your SAP SNC system, you must implement SAP Note 1801803.

Single Sign-On to SAP SNC from Ariba Network

You can enable your suppliers for certain collaboration processes that are available in SAP SNC only.

In this case, the Supply Network Collaboration section is available for the supplier in the Supplier Dashboard on Ariba Network. The configuration you make for the supplier defines which processes are available to them.

You can enable your suppliers for single sign-on for the following processes in SAP SNC:

- Forecast (Order Forecast Monitor screen)
- Replenishment (SMI Overview screen)
- Work Order Collaboration (Work Order Worklist screen)
- Supply Network Inventory (Supply Network Inventory Overview screen)
- Quality Collaboration (Quality Notification Overview screen)
Onboarding of Suppliers

You, as a customer, can decide to onboard some of your suppliers that you already have in your ERP system to SAP SNC and to Ariba Network. For that, execute the following steps:

1. In your SAP SNC system, create a business partner for each supplier you want to enable for SAP SNC and for Ariba Network. You can do this, for example, using the Core Interface (CIF), or you can create the business partners manually.
   Do not create SAP users for the suppliers.

2. In your SAP SNC system, make settings to define which supplier is enabled for which business processes. You make these settings in Customizing for Message-Based Integration or for Single Sign-On under Ariba Network Integration for SAP SNC.

   **Caution**

   You can enable a supplier either for the message-based integration scenario, or for processes in the single sign-on scenario.

3. In your SAP SNC system, run the Supplier Onboarding to Ariba Network report (transaction /SCA/ARB_INT_ONB) to generate a CSV file that contains the data of the suppliers you want to enable for the integration.

4. On Ariba Network, upload the CSV file with the supplier information.

5. On Ariba Network, enable the suppliers.

   **Note**

   For more information about steps 4 and 5, see the documentation for Ariba Network.

After completing these steps, the supplier that you enabled can log on to Ariba Network. In case they are enabled for one or more of the processes supported by the single sign-on scenario, the supplier can find the Supply Network Collaboration section in the Supplier Dashboard on Ariba Network.

As the supplier clicks a link in the Supply Network Collaboration section for the first time, a supplier user is automatically created in SAP SNC, and the authorizations you defined in Customizing are assigned to this supplier user.
2 Installation Information

2.1 Technical System Landscape

Components of the System Landscape

Ariba Network

Ariba Network is a cloud solution for business commerce networks that is offered by Ariba, an SAP company.

SAP SNC System

The SAP SNC system in this landscape has two products installed:

- SAP SNC, either as a standalone installation or as part of SAP SCM Server
  SAP Supply Network Collaboration (SAP SNC) is an application that supports participants in a complex supply chain network to collaborate efficiently with each other. SAP SNC supports, among other things, the management of inventories by suppliers and customers, timely shipments of replenishments, and advanced shipping notification and invoice creation. It also supports forecasting processes and work order collaboration.
- Ariba Network Integration 1.0 for SAP Business Suite, product instance Ariba Network Integration for SAP SNC
  Ariba Network Integration for SAP SNC connects your SAP SNC with Ariba Network. It enables SAP SNC to send and receive messages in cXML, and enables the seamless logon to SAP SNC for suppliers using Ariba Network.

ERP System

The system that your company uses to collect, store, and process data from its business activities. SAP SNC requires an ERP system as the back-end system.

SAP Process Integration System

SAP Process Integration is a middleware that facilitates the integration of business processes that span different departments, organizations, companies, and systems. SAP Process Integration mediates the data exchange between different application components.

SAP SNC requires SAP Process Integration to communicate with the ERP system.

Ariba Network Integration for SAP Business Suite can be deployed to connect to Ariba Network either through SAP Process Integration (mediated connectivity), or without SAP Process Integration (direct connectivity).

System Landscape for Ariba Network Integration for SAP SNC, Direct Connectivity

The following figure shows the system landscape for connecting an SAP SNC system to Ariba Network, without the use of SAP Process Integration.
Note that SAP Process Integration is used to connect the ERP system with the SAP SNC system.

Figure 1: System Landscape with Direct Connectivity

**System Landscape for Ariba Network Integration for SAP SNC, Mediated Connectivity**

The following figure shows the system landscape for connecting an SAP SNC system to Ariba Network with the use of SAP Process Integration.

Note that SAP Process Integration is also used to connect the ERP system with the SAP SNC system. You can use the same SAP Process Integration installation for both purposes.

Figure 2: System Landscape with Mediated Connectivity

### 2.2 Software Components of Ariba Network Integration for SAP SNC

There are several product instances for Ariba Network Integration 1.0 for SAP Business Suite. One of the instances is *Ariba Network Integration for SAP SNC*.

Ariba Network Integration for SAP SNC consists of the following software component versions:

- **ARBFNDI1 100** (Integration Component: Foundation for Ariba Integration with NW 700 100)
- **ARBFNDI2 100** (Integration Component: Foundation for Ariba Integration with NW 701 100)
- **ARBSNCI1 100** (SNC Ariba Network Integration 100)

For more information about other product instances of Ariba Network Integration 1.0 for SAP Business Suite, see the *Administrator’s Guide for Ariba Network Integration 1.0 for SAP Business Suite* on SAP Service Marketplace at [http://service.sap.com/instguides](http://service.sap.com/instguides).

### 2.3 Prerequisites for Installation

#### Required Versions of the Components of the System Landscape

You require the following releases of products and their Support Packages to be able to install Ariba Network Integration for SAP SNC, and to be able to execute the scenarios it covers.

**Ariba Network**

You can execute the end-to-end scenarios for message-based integration between SAP SNC and Ariba Network and for single sign-on from Ariba Network to SAP SNC as of the **2014 September release of Ariba Network**.
SAP Supply Network Collaboration (SAP SNC)

SAP SNC can be deployed either as an add-on to SAP NetWeaver, or as part of a full SAP SCM Server installation. Therefore, the add-on Ariba Network Integration for SAP SNC can be installed on top of an SAP SCM Server installation as well.

Table 3:

<table>
<thead>
<tr>
<th>Required Product Version</th>
<th>Minimum Support Package Level Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhancement package 1 for SAP SCM 7.0</td>
<td>10</td>
</tr>
<tr>
<td>Enhancement package 1 for SAP SNC 7.0</td>
<td>10</td>
</tr>
<tr>
<td>Enhancement package 2 for SAP SCM 7.0</td>
<td>7</td>
</tr>
<tr>
<td>Enhancement package 2 for SAP SNC 7.0</td>
<td>7</td>
</tr>
<tr>
<td>Enhancement package 3 for SAP SCM 7.0</td>
<td>1</td>
</tr>
</tbody>
</table>

SAP Process Integration

In case you would like to connect your SAP SNC system to Ariba Network using a middleware, you require one of the following releases of SAP Process Integration:

- SAP Process Integration 7.1
- SAP Process Integration 7.31

Required SAP Notes

Before installing Ariba Network Integration for SAP SNC, you must implement the following SAP Notes in your system:

Table 4:

<table>
<thead>
<tr>
<th>Software Component Version</th>
<th>SAP Note Number</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARBFNDI1 100</td>
<td>2035927</td>
<td>Error when processing outbound cXML message</td>
</tr>
<tr>
<td>SAP_BASIS 702, 730, 731, 740</td>
<td>2016414</td>
<td>Show custom error page for automatic account creation failures during SAML 2.0 logon</td>
</tr>
<tr>
<td>SAP_BASIS 702, 730, 731, 740</td>
<td>1888484</td>
<td>Save of SAML 2.0 configuration fails</td>
</tr>
<tr>
<td>SCM_BASIS 701, 702, 713</td>
<td>2021080</td>
<td>MDL: Allow internal Partner Number assignment</td>
</tr>
<tr>
<td>SCMSNC 701, 702</td>
<td>2017801</td>
<td>SNC-Ariba integration interface</td>
</tr>
</tbody>
</table>
### Other SAP Notes

Other SAP Notes that are relevant for the Ariba Network Integration for SAP SNC:

Table 5:

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1841471</td>
<td>Release strategy for ABAP add-ons for interface components</td>
</tr>
<tr>
<td>2040404</td>
<td>Release strategy for the ABAP add-on ARBSNCI1</td>
</tr>
<tr>
<td>2040351</td>
<td>Ariba Network Integration for SAP SNC: Mapping Documentation</td>
</tr>
<tr>
<td>1801803</td>
<td>Change already published ASNs</td>
</tr>
</tbody>
</table>
3 Configuration Information

3.1 Prerequisites for Connecting SAP SNC to Ariba Network

The following prerequisites apply:

- You have signed up for an Ariba Network membership.
- You have received one or several IDs, known as Ariba Network IDs (ANID). You use either a password (SharedSecret) or a client certificate with each ANID. Each credential represents a unique entity on Ariba Network, that is, your appearance to the vendors on Ariba Network.
- Ariba has provided you with a list of your vendors who have already signed up to the network, so you can start collaboration immediately. To connect with the vendors on the network, get support from your Ariba contact.

**Note**

You can execute the end-to-end scenarios for message-based integration between SAP SNC and Ariba Network and for single sign-on from Ariba Network to SAP SNC as of the 2014 September release of Ariba Network.

3.2 Establishing the Technical Connection to Ariba Network

3.2.1 Setting Up the Connection for Message-Based Integration

As described in the introduction, you can decide whether you connect your SAP SNC system to Ariba Network either directly or through SAP Process Integration. A mixture is not recommended.

This decision is a prerequisite for choosing the relevant Customizing activities later.

The following figure shows an overall picture of the interfaces used for direct connectivity:

![Figure 3: Interfaces for Direct Connectivity](image)

Even though it is not technically required, we recommend that you establish an RFC connection (transaction SM59) to Ariba Network, so that you can ping the network, and check its technical availability.
The following figure shows the technical settings of this connection:

![RFC Destination ARIBA_MTEST](image)

**Figure 5: Technical Settings for Direct Connectivity**

Create an RFC connection of connection type G. Define `service.ariba.com` as target host, enter **443** as the service number, and `/service/transaction/cxml.asp` as the path prefix.
The following figure shows the logon and security details of this connection:

![Figure 6: Logon and Security Settings for Direct Connectivity](image)

On the Logon & Security tab, select No Logon as logon procedure. SSL is active, and select ANONYM SSL Client as SSL client certificate.

**Note**

For HTTPS SSL encryption, you first have to obtain the server certificate from Ariba and then import it into the SAP SNC system using Trust Manager (transaction STRUST). For more information about certificates and security, see chapter SAP SNC System Acting as a Client [page 25] under Security Information.

For HTTPS communication, the HTTPS service must be active in your SAP SNC system. To display active services, on the ICM Monitor screen (transaction SMICM), double-click the Services button in the menu bar.

### 3.2.2 Setting Up the Connection for Single Sign-On to SAP SNC from Ariba Network

To establish the cross-domain authentication between security domains, Ariba Network Integration 1.0 for SAP Business Suite uses the Security Assertion Markup Language (SAML) 2.0 implementation. In a typical system...
landscape, the customer’s corporate network is well separated from Ariba Network, and only a limited number of communication channels are open through corporate firewalls. SAML enables the secure exchange of information using XML messages over HTTP(S) protocol.

Enabling SAML 2.0 in the SAP SNC System

By default, SAML 2.0 is not enabled in your SAP SNC system. Perform the following steps in your productive client to enable SAML 2.0:

1. Start SAML 2.0 Configuration (transaction SAML2).
   In case it is the first time you configure SAML 2.0 in the given client, the system displays the following message: Client < number> is not configured to support SAML 2.0. Choose Enable SAML 2.0 Support, then Create SAML 2.0 Local Provider to start the configuration.
2. Enter a provider name, such as <system ID>CLNT <client number>.
3. Complete the steps in the configuration wizard.
4. Activate the necessary Internet Communication Framework (ICF) services. To use the service provider, you must manually activate the following two ICF services:
   ○ /default_host/sap/public/bc/sec/saml2
   ○ /default_host/sap/public/bc/sec/cdc_ext_service

You now have SAML 2.0 enabled for the client. You can make further configuration settings in the client, such as configuring the bindings supported by the service provider, trusting an identity provider, configuring identity federation, and protecting resources with SAML 2.0. The configuration creates two Secure Store and Forward (SSF) applications, and associates Personal Security Environment (PSE) files with them. The PSE files contain the signing and encryption key pairs of the service provider.

For more information about enabling SAML 2.0 support, look for Enabling the SAML Service Provider in the documentation of your SAP NetWeaver release on SAP Help Portal at http://help.sap.com/nw.

Configuring SAP SNC as a Service Provider

In the single sign-on scenario of the add-on, the SAP SNC system is the service provider (SP), and Ariba Network is the identity provider (IdP), which authenticates users, then convey authentication information. On successful authentication, Ariba Network displays the relevant hyperlinks pointing to the SAP SNC system. The users logged on will use their Ariba Network credentials to start the SAP SNC Web UI.

To protect application-specific URLs when performing the single sign-on initiated by Ariba Network, Ariba Network Integration 1.0 for SAP Business Suite uses the RelayState parameter of SAML 2.0.

Perform the following steps to configure your SAP SNC system as a service provider in SAML 2.0:

1. Start SAML 2.0 Configuration (transaction SAML2).
2. On the Local Provider tab, choose the Service Provider Settings tab. Choose Edit.
3. Enter /sap/bc/webdynpro/scf/snc_s in the Default Application Path field.
5. Enter the application alias you agreed upon with the identity provider, and the relative path to the target application.
The following relay states, which represent the business processes available in SAP SNC in the single sign-on scenario, are available:

<table>
<thead>
<tr>
<th>Relay State</th>
<th>Application Path</th>
<th>Description of Screen in SAP SNC</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARB_SMI</td>
<td>/sap/bc/webdynpro/scf/snc_s?scr_id=SNCDMSMOVWS</td>
<td>SMI Monitor</td>
</tr>
<tr>
<td>ARB_FCST</td>
<td>/sap/bc/webdynpro/scf/snc_s?scr_id=DEMOVWS</td>
<td>Order Forecast Monitor</td>
</tr>
<tr>
<td>ARB_WO</td>
<td>/sap/bc/webdynpro/scf/snc_s?scr_id=W0ACT_S</td>
<td>Work Order Worklist</td>
</tr>
<tr>
<td>ARB_SNI</td>
<td>/sap/bc/webdynpro/scf/snc_s?scr_id=SNIDMOVW</td>
<td>SNI Overview</td>
</tr>
<tr>
<td>ARB_QUALITY</td>
<td>/sap/bc/webdynpro/scf/snc_s?scr_id=QNOVWS</td>
<td>Quality Notification Overview</td>
</tr>
</tbody>
</table>

For more information about configuring an SAP Business Suite system as a service provider, look for Mapping Relay States to Applications in the documentation of your SAP NetWeaver release on SAP Help Portal at [http://help.sap.com/nw](http://help.sap.com/nw).

### Configuring Automatic Creation and Update of Users in SAP SNC

Perform the following steps to create an ICF service and an alias, and configure them for automatic user creation and update of users in your SAP SNC system.

**Creating an ICF Service**

1. Start the Maintain Services (SICF) transaction, and choose Execute.
2. Choose the /default_host/sap/bc/saml2 node, then Create Host/Service to create the service element register_user. This will be used as an Assertion Consumer Service (ACS) endpoint.
4. Delete SAML Logon from the Logon Procedure List located at the bottom of the window.
5. On the Handler List tab, add CL_HTTP_EXT_SAML20 to the handler list.
6. Save the new ICF service node.

**Creating an External Alias**

2. Select DEFAULT_HOST as virtual host, then create the /sap/saml2/sp/register external alias.
3. On the Logon Data tab, select Alternative Logon Procedure for the Procedure. Also specify the data for client, technical user (for single sign-on), and password.
   The user that you enter here must have permission to create users and assign roles to them in the client where the SAML 2.0 service provider is configured for automatic user account creation.
4. Delete all entries, except for **Logon Through Service Data** from the **Logon Procedure List** located at the bottom of the window.

5. On the **Trg Element** tab, double-click the **register_user** ICF node, which you previously created, so that the external alias would point to this node.

6. Save the external alias.

**Implementing the BADI_SAML20_USER_CREATE_UPDATE Business Add-In (BAdI)**

1. In **BAdI Builder** (transaction SE18), display the **ENH_SAML20_USER_CREATE_UPDATE** enhancement spot.

2. On the **Enh. Spot Element Definitions** tab, select the **SAML 2.0 BAdI for automatic user creation update (BADI_SAML20_USER_CREATE_UPDATE)** BAdI, and create a BAdI implementation for it. When asked for enhancement implementation, create a new enhancement implementation, and assign it to the BAdI implementation.

   In the BAdI implementation, use implementation class `/SCA/CL_EXM_IM_ARB_SAML_USER`.

3. Save and activate your changes.

**Creating a Custom Error Page for Errors When Creating Users Automatically During SAML 2.0 Logon (Optional)**

If you want to display an error page when automatic user creation fails, you must implement SAP Note 2016414 in your SAP SNC system.

In case you implemented SAP Note 2016414, the system displays an error page when the automatic user creation fails. You can replace this standard error page with a custom one. To do so, execute the following steps:

1. Start the **Maintain Services** (**SICF**) transaction, and choose **Execute**, then choose **External Aliases**.

2. Select the `/sap/saml2/sp/register` external alias.

3. On the **Appl. Errors** tab on **Error Pages**, create an explicit response page body.

4. Enter the HTML code for your custom error page. For the available SAP-specific tags, see the Documentation in the transaction.

5. Save the changes you have made to the external alias.

**Setting Up the Connection with Ariba Network**

**Adding Ariba Network as a Trusted Identity Provider**

Opposite to the message-based integration scenario, the **single sign-on from Ariba Network to SAP SNC** scenario supports the authentication with client certificate only, and does not support the use of a **SharedSecret** password.

1. Start **SAML 2.0 Configuration** (transaction SAML2).

2. On the **Trusted Providers** tab, choose **Select** > **Manually**.

3. Enter the name and the alias of the Ariba Network identity provider.

4. Upload the **Primary Signing Certificate** file that you received from Ariba.
5. Add a new single sign-on endpoint: Select **HTTP POST** for **Binding**, and enter the URL of the Ariba Network server.

6. Save the settings you have made. Do not enable the identity provider yet.

**Setting Up Identity Federation with Ariba Network as Identity Provider**

1. Select the identity provider that you previously created. Choose **Edit**.
2. On the **Identity Federation** tab, add the **Persistent** name ID format. Select **Automatic User Creation** for **Account Federation**, and **Yes** for **Allow Identity Provider to Create NameID**.
3. Save the settings of the identity provider.
4. Select the identity provider that you have previously created for Ariba Network, and enable it.

**Maintain Number Ranges**

**Number Ranges for Users in SAP SNC**

Create number range **01** for supplier users that will be automatically created in SAP SNC. Carry out the **Create Number Ranges for Suppliers with Single Sign-On from Ariba Network** Customizing activity under [Ariba Network Integration for SAP SNC ➔ Single Sign-On](#).

**Number Ranges for Business Partner Relationships**

Make sure the number range **01** for business partner relationships is maintained. You do this in the **Define Number Ranges** Customizing activity under [Cross-Application Components ➔ SAP Business Partner ➔ Business Partner Relationships ➔ Basic Settings](#).

### 3.3 Customizing Ariba Network Integration for SAP SNC

Two integration scenarios are available to integrate your SAP SNC system with Ariba Network: message-based integration and single sign-on.

In case of message-based integration, SAP SNC and Ariba Network exchange cXML messages.

Within the single sign-on scenario, users of Ariba Network can log on to SAP SNC and access certain SAP SNC business processes.
3.3.1 Framework Settings for Connecting SAP SNC to Ariba Network

To connect SAP SNC to Ariba Network, choose [Ariba Network Integration for SAP SNC] Framework Settings and make settings in the following Customizing activities:

- **Define Credentials and End Points for Ariba Network**:
  - Enter your Ariba credentials, that is, ANID(s) and the corresponding password(s).
  - Leave the **SharedSecret** blank if you authenticate with client certificate on Ariba Network.
  - If you have not yet switched your system to productive use, select the **Test Account** checkbox.
  - Select one of the following options for **Enable End Points**
    - **End points not enabled**
      Use this option if the end points are not activated on Ariba Network.
    - **Enable end points for authentication**
      Use this option if you use end points only for authentication.
    - **Enable end points for authentication and polling**
      Use this option if you use end points for authentication and polling.

If you have decided to configure end points on Ariba Network, the credentials must **only** be specified in the view **End Points for Ariba Network**. Proceed as follows:

  - **SAP-Internal Key**
    This is an SAP-internal name for the end point; it must be unique in your SAP SNC system. This key value is used later in the Customizing activity **Define Settings for Polling Agent** for using end points in polling.
  - **Ariba End Point ID**
    This is the end point name defined on Ariba Network for your SAP system.
  - **Enter SharedSecret**
    Provide your SharedSecret value if you use a password for the communication between your SAP system and Ariba Network.

For more information about end points, see **Endpoints [page 62]**.

- **Define Basic Message Settings**
  Specify which Ariba cXML message types you intend to send and receive, and fill the corresponding **Object Type**, **Message Type**, **Direction**, **Mapping Version** and **cXML version** fields. The **Send cXML StatusUpdateRequest Message** is only valid for **inbound** cXMLs; it informs Ariba Network about successful or erroneous processing of your messages in the backend.

Based on your system architecture and connectivity decision, make settings in Customizing for either direct connectivity or mediated connectivity.

**Direct Connectivity**

For direct connectivity, choose [Ariba Network Integration for SAP SNC] Framework Settings [Direct Connectivity Settings] and make settings in the following Customizing activities:

- **Manage and Test Enterprise Services**

The Web services used for communication with Ariba Network (AN) have to be configured in the SOA Manager. A detailed configuration guide can be found in the chapter **Configuration of SOA Manager [page 54]**.
Note

After the SOA configuration steps you have to execute the technical configuration of Simple Object Access Protocol (SOAP) runtime (transaction SRT_TOOLS). For more information, search for the keyword Configuring the Web Service Runtime in the documentation of SAP NetWeaver at http://help.sap.com, and see SAP Note 1043195.

● **Maintain Certificate**

As the connection is established through HTTPS, a certificate for authentication is required. For more information, see chapter SAP SNC System Acting as a Client [page 25].

● **Define Settings for Polling Agent**

A polling mechanism is used for retrieving messages. For each Ariba Network ID you can specify which message types are expected to be received from the network. If you use end points in polling, specify the SAP-internal key value of the endpoint ID. You can also define the maximum number of messages that can be retrieved within one call to the network (no more than 100 messages is recommended). All pending messages are retrieved, but if they exceed the defined maximum, additional calls are performed. The logical port name has to match the one you have defined in the SOA Manager in the chapter Configuration of SOA Manager [page 54].

● **Define bgRFC Supervisor Destination**

You define a supervisor destination for the background RFC (bgRFC) in this Customizing activity. For more information, see Customizing for Ariba Network Integration for SAP SNC under Framework Settings ➤ Framework Settings ➤ Define bgRFC Supervisor Destination.

You can also implement the BAdI Notification About Communication Errors (ARBFND_INTEGRATION) to trigger actions in situations where errors occur during the communication between your SAP SNC system and Ariba Network. This BAdI is called if a cXML message cannot be transferred to Ariba Network (outbound direction), or a cXML message is received but cannot be processed (inbound direction). For more information, see Customizing for Ariba Network Integration for SAP SNC under Framework Settings ➤ Framework Settings ➤ Business Add-Ins (BAdIs) ➤ BAdI: Notification About Communication Errors.

**Mediated Connectivity**

For mediated connectivity, make settings in Customizing for Ariba Network Integration for SAP SNC under Framework Settings ➤ Mediated Connectivity Settings ➤ Integration Engine Administration.

Your SAP Process Integration system must be set up and connected to your SAP SNC system. The Integration Engine configuration should already contain global configuration data. If this is not the case, check the setup guides for your SAP Process Integration system.

You can also implement the BAdI Notification About Communication Errors (ARBFND_INTEGRATION). This BAdI is called if a cXML message cannot be created (outbound direction), or if a cXML message is received from SAP Process Integration but cannot be processed (inbound direction). Note that if the message cannot be transferred to SAP Process Integration, the BAdI is not triggered. For more information, see Customizing for Ariba Network Integration for SAP SNC under Framework Settings ➤ Framework Settings ➤ Business Add-Ins (BAdIs) ➤ BAdI: Notification About Communication Errors.
**Direct and Mediated Connectivity**

**Note**

For both direct and mediated connectivity, the Notification About Communication Errors (ARBFND_INTEGRATION) BAdI is only called when there are errors in cXML message communication between your SAP SNC system and Ariba Network. In this BAdI, you can implement the actions (for example, an email notification) that you want to trigger if errors occur. A sample implementation is available. For more information, see *Ariba Network Integration for SAP SNC* under Framework Settings > Business Add-Ins (BAdIs) > BAdI: Notification About Communication Errors.

### 3.3.2 Settings for Message-Based Integration

In Customizing for *Ariba Network Integration for SAP SNC* under Message-Based Integration, make settings in the following Customizing activities:

- **Assign Ariba Network ID to Customer Business Partner**
  Assign the ANID(s) that you have received from Ariba Network to the customer business partners that you want to be connected to AN.

- **Define Profiles for Message-Based Integration**
  Create profiles for message-based integration between SAP SNC and Ariba Network (message profiles). Then, specify the message types you would like to use with a given message profile.

- **Assign Message Profiles to Suppliers**
  Assign any of the previously created message profiles to any one supplier or a combination of supplier and customer.

You can also implement the following BAdIs by choosing *Ariba Network Integration for SAP SNC* > Message-Based Integration > Business Add-Ins (BAdIs):

- **BAdI: Inbound Mapping for Purchase Order Confirmations**
  To change the standard logic for mapping incoming purchase order confirmations and override the default logic for storing them, the following three methods are available:
    - BEFORE_MAPPING, which enables you to map and save cXML documents skipping the standard logic, or allows you to modify cXML documents and continue with the standard mapping and saving process
    - AFTER_MAPPING, which enables you to modify mapped values or populate additional fields once the mapping has already taken place and also allows you to skip the standard logic for saving
    - AFTER_SAVE, which enables you to save any attachments or other extensions of the incoming documents and also allows you to create and save log entries.

  The BAdI has another four methods that enable you to change certain partner-related and location-related data:
    - CHANGE_CUSTOMER for choosing the correct customer from a list of customers returned by the system or providing a customer other than the ones included in the list that the system returned
    - CHANGE_SUPPLIER for changing the supplier
    - CHANGE_LOCATION for specifying a different location
    - CHANGE_LOGSYS for changing the logical system
For more information about this BAdI, see Customizing for *Ariba Network Integration for SAP SNC* under ► Message-Based Integration ► Business Add-Ins (BAdIs) ► BAdI: Inbound Mapping for Purchase Order Confirmations.

**BAdI: Inbound Mapping for Advanced Shipping Notifications**

For changing the standard logic for mapping incoming advanced shipping notifications (ship notice cXML messages) and overriding the default logic for storing them, the following three methods are available:

- **BEFORE_MAPPING**, which enables you to map and save cXML documents skipping the standards logic, or allows you to modify cXML documents and continue with the standard mapping and saving process
- **AFTER_MAPPING**, which enables you to modify mapped values or populate additional fields once the mapping has already taken place and also allows you to skip the standard logic for saving
- **AFTER_SAVE**, which enables you to save any attachments or other extensions of the incoming documents and also allows you to create and save log entries.

The BAdI has another four methods that enable you to change certain partner-related and location-related data:

- **CHANGE_CUSTOMER** for choosing the correct customer from a list of customers returned by the system or providing a customer other than the ones included in the list that the system returned
- **CHANGE_SUPPLIER** for changing the supplier
- **CHANGE_LOCATION** for specifying a different location
- **CHANGE_LOGSYS** for changing the logical system

For more information about this BAdI, see Customizing for *Ariba Network Integration for SAP SNC* under ► Message-Based Integration ► Business Add-Ins (BAdIs) ► BAdI: Inbound Mapping for Advanced Shipping Notifications.

**BAdI: Outbound Mapping for Purchase Orders**

For changing the standard logic for mapping outgoing purchase orders, the following two methods are at your disposal

- **BEFORE_MAPPING**, which enables you to populate additional fields in the purchase order document and also allows you to override the standard mapping process
- **AFTER_MAPPING**, which enables you to modify mapped values or populate additional fields once the mapping has already taken place

The BAdI has another three methods that enable you to change certain partner-related and location-related data:

- **CHANGE_CUST_CRED** for specifying the ANID to be included in the header of the cXML message in case the customer has several ANIDs
- **CHANGE_SUPP_CRED** for specifying the ANID to be included in the header of the cXML message in case the supplier has more than one ANID
- **CHANGE_ENDPOINT_INFO** for specifying the ERP system ID to be included in the header of the cXML message in case your SAP SNC system is connected to multiple ERP systems

For more information about this BAdI, see Customizing for *Ariba Network Integration for SAP SNC* under ► Message-Based Integration ► Business Add-Ins (BAdIs) ► BAdI: Outbound Mapping for Purchase Orders.
3.3.3 Settings for Single Sign-On to SAP SNC from Ariba Network

For single sign-on integration, see Customizing for Ariba Network Integration for SAP SNC under Single Sign-On and make settings in the following Customizing activities:

- **Define Profiles for Single Sign-On to Ariba Network**
  Create profiles for single sign-on (SSO profiles) and assign roles and business processes to the profiles you created. The role assignment determines for which SAP SNC screens a supplier with the given profile has authorization. The assigned business processes are the ones the supplier with the given profile can use.

- **Assign Single Sign-On Profiles to Suppliers**
  Assign the previously created SSO profiles to the suppliers you would like to connect to SAP SNC from Ariba Network using single sign-on.

- **Create Number Ranges for Suppliers with Single Sign-On from Ariba Network**
  Define the number range you would like the system to use when creating user IDs in SAP SNC upon first logon from Ariba Network.

You can also implement the following BAdIs by choosing Ariba Network Integration for SAP SNC Message-Based Integration Business Add-Ins (BAdIs):

- **BAdI: User ID and Person Business Partner Generation**
  For customizing the user ID and person business partner ID that are created upon first logon from Ariba Network, the following two methods are available:
  - GET_USERID method, which enables you to implement a customer-specific logic for generating the user ID for the supplier user
  - GET_PERSONBP method, which allows you to implement a customer-specific logic for generating the person business partner ID for the supplier user

- **BAdI: User Management for SAP SNC-Ariba Network Integration**
  This BAdI modifies the standard process for creating users upon first logon to SAP SNC from Ariba Network using single sign-on (BEFORE_USER_CREATE) as well as the standard process for updating user data upon later logons (BEFORE_USER_UPDATE). For more information about this BAdI, see Customizing for Ariba Network Integration for SAP SNC under Single Sign-On Business Add-Ins (BAdIs) BAdI: User Management for SAP SNC-Ariba Network Integration.

3.4 Related Settings on Ariba Network

In order to be able to run the integration scenarios in your system landscape, you have to make certain settings on Ariba Network.

**Note**

The integration scenarios between Ariba Network and SAP SNC can be executed as of the 2014 September release of Ariba Network.
Make sure you have selected the following settings for your buyer account on Ariba Network under Default Transaction Rules:

- **Require the packing slip ID to be unique on ship notices**
  This rule ensures that the supplier does not enter a ship notice ID that already exists in Ariba Network. In SAP SNC, the corresponding advanced shipping notification (ASN) ID has to be unique.

- **Allow change orders for fully shipped orders**
- **Allow change orders for partially shipped orders**
- **Enable ship notice tracking on change orders**
- **Allow cancel orders for fully shipped orders**
- **Allow cancel orders for partially shipped orders**
- **Allow suppliers to send order confirmations to this account**
- **Allow suppliers to send ship notices to this account**
- **Require an actual or estimated shipping date on ship notices**
- **Require an estimated shipping date on order confirmations**
- **Do not allow suppliers to change line item description on order confirmations**

The URLs for the single sign-on scenarios have to be configured on Ariba Network, so that supplier will find the links to those processes in SAP SNC that they have been enabled for. Contact the Ariba Service Team for more information.

For more information about the above settings on Ariba Network, look up the documentation for Ariba Network, or contact Ariba.

### 3.5 Jobs to Be Scheduled

The following reports are available and need to be scheduled as regular jobs:

- **Fetch cXML messages for different message types from Ariba Network**
  (ARBFND_FETCH_CXML_MESSAGES_NEW)
  This report polls pending messages from Ariba Network and is relevant only for direct connectivity. It has to be scheduled as a variant marking all cXML messages you wish to receive and process in your SAP SNC system.

- **Deletion of Outdated Administrative Data for Messages**
  (/SCA/ARB_INT_MSG_CLEANUP)
  This report deletes the administrative data that no longer has a reference document (such as a purchase order or ASN) in the SAP SNC system. You can schedule this report as a background task or execute it yourself on a regular basis.
4 Security Information

For **direct** connectivity, the SAP SNC system opens the connection by executing the following actions:

- The SAP SNC system pushes cXML messages to Ariba Network (synchronous)
- The Polling Agent of Ariba Network Integration 1.0 for SAP Business Suite fetches pending messages from Ariba Network (synchronous)

For **mediated** connectivity, the SAP SNC system connects through SAP Process Integration. The connection functions as follows:

- The SAP SNC system pushes cXML messages to SAP Process Integration (asynchronous)
- The Ariba PI adapter triggers its Polling Agent to fetch pending cXML messages from Ariba Network. The Polling Agent in the PI adapter then pushes the cXML messages to the SAP SNC system (asynchronous).

In both use cases, only 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.

The SAP SNC system communicates with Ariba Network through the HTTPS protocol, encrypting transmitted data.

If Ariba Network Integration 1.0 for SAP Business Suite communicates with Ariba Network through SAP Process Integration, there are no special security requirements.

Ariba provides information on how to communicate with Ariba Network in the *Ariba Network Adapter for SAP NetWeaver Setup Guide*. You can contact Ariba for more information.

As the security topics for mediated connectivity through SAP Process Integration are covered by the *Ariba Network Adapter for SAP NetWeaver Setup Guide*, the next chapter focuses on direct connectivity.

**Note**

Advanced Security Configuration is available for the Ariba Network and will be the default setting as of September 30, 2016. To ensure that your Business Suite system can continue to communicate with the Ariba Network, check whether your SAP AS ABAP kernel release patch level is up-to-date. For more information, see SAP Note [2335891](http://support.sap.com/).  

4.1 SAP SNC System Acting as a Client

When sending a cXML message to Ariba Network, the sender must authenticate itself. Ariba Network offers different authentication methods (authentication with client certificate or SharedSecret password) that are also supported by Ariba Network Integration 1.0 for SAP Business Suite.

**Note**

The *single sign-on from Ariba Network to SAP SNC* scenario supports the authentication with client certificate only.
For more information about the authentication methods on Ariba Network, contact Ariba.

Note

Communication with Ariba Network is based on HTTPS. For HTTPS SSL encryption, SAP Cryptographic Library is required. For information about installation of SAP Cryptographic Library, search for the phrase The SAP Cryptographic Library Installation Package in the documentation of SAP NetWeaver at http://help.sap.com.

Authentication with Client Certificate

Proceed as follows:

1. Get the client certificate from a Certification Authority (CA) that is trusted by Ariba.
2. Import the private key of the certificate into the SAP SNC system by using Trust Manager (transaction STRUST).

   Note

   Only certificates in Personal Security Environment (PSE) format can be imported. Certificates in other formats must first be converted to 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 The SAP Cryptographic Library Installation Package in the documentation for your SAP NetWeaver release.

   For example, to convert from P12 (Public-Key Cryptography Standards) format to PSE format, enter the following command line:
   `sapgenpse import_p12 -v -r <root certificate> -p <Target PSE file> <Source File>`

   First, create a new Client Identity in Trust Manager. Choose Environment ➔ SSL Client Identities, enter ARIBA as the identity name and Ariba Network Client as the description. Save your entries.

   Second, import the private key of the certificate in Trust Manager. Proceed as follows:
   1. Select the created ARIBA SSL Client ID and choose PSE ➔ Import to import the PSE file.
   2. Enter the password for the certificate if required.
   3. Save your PSE file by choosing PSE ➔ Save as ➔ SSL Client and enter ARIBA as the SSL Client.
   4. 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 now shown in Trust Manager in Certificate List.

   3. Import the root certificate into the SAP SNC system by using Trust Manager. Proceed as follows:
      1. Double-click the SSL Client Identity ARIBA that you have created.
      2. Navigate to the Certificate group box and choose Import certificate. Add the imported certificate to the certificate list by clicking Add to Certificate List.

   4. For HTTPS SSL encryption, obtain the server certificate from Ariba. Proceed as follows:
      2. Download the certificate using your browser.

         For example, if you are using Internet Explorer, choose View ➔ Security Report ➔ View Certificates. On the Details tab page, choose Copy to File and export it in the Base-64 encoded X.509 format.
3. Import the server certificate into the SAP SNC system using Trust Manager. Double click the ARIBA SSL Client ID that you have created. Navigate to the Certificate group box and choose Import certificate. Add the imported certificate to the certificate list by clicking Add to Certificate List.

5. To activate the changes, restart the Internet Communication Manager (ICM) using transaction SMICM and choose Administration ➤ ICM ➤ Restart ➤ Yes. For more information, search for the phrase Using the ICM Monitor in the documentation of SAP NetWeaver at http://help.sap.com.

6. Configure the Web services in SOA Manager (transaction SOAMANAGER). Follow the steps described under Configuration of SOA Manager [page 54] and find the following consumer proxies:
   ○ cXMLSynchronousOutboundAdapterMessage_Out (CO_ARBFND_PRX_OADP_OUT)
   ○ cXMLGetPendingDataRequest_Out (CO_ARBFND_PRX_GPDQ_OUT)

In the Details of Consumer Proxy group box, navigate to the Configurations tab page, select the logical port. 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.

7. In the profile of your account on Ariba Network, select the Certificate authentication method in the cXML setup, and enter the public key of the certificate.

**Authentication with SharedSecret Password**

Proceed as follows:

1. Maintain the SharedSecret password in the Define Credentials for Ariba Network Customizing activity. For more information, see Framework Settings for Connecting SAP SNC to Ariba Network [page 19]. The SharedSecret password is stored in the secure storage ABAP DB in the SAP SNC system. Ariba Network Integration 1.0 for SAP Business Suite supports a SharedSecret password for Ariba Network with a maximum length of 36 characters.

    **Note**

    For authentication with SharedSecret password, the SharedSecret password has to be provided in the Sender element of the cXML payload.

    According to security requirements, passwords must not be written to logs, protocols, or traces. Therefore, the SharedSecret password is not visible in transactions such as SXMB_MONI where the XML message monitoring and tracing takes place, as business users can also have authorization for the message monitoring transactions. However, when activating an Internet Communication Framework (ICF) recording using transaction SICF, the system logs the SharedSecret password in the corresponding ICF trace. ICF recording is only intended for administrators and requires the S_ADMI_FCD authorization.

2. For HTTPS SSL encryption, obtain the server certificate from Ariba. Proceed as follows:
   2. Download the certificate using your browser.
      
      For example, if you are using Internet Explorer, choose View ➤ Security Report ➤ View Certificates. On the Details tab page, choose Copy to File and export it in the Base-64 encoded X.509 format.
   3. Import the server certificate into the SAP SNC system using Trust Manager. Double-click the SSL Client SSL Client (Anonymous) node.
Navigate to the Certificate group box and choose Import certificate. Add the imported certificate to the certificate list by clicking Add to Certificate List.

3. To activate the changes, restart the Internet Communication Manager (ICM) using transaction SMICM and choose Administration ➔ ICM ➔ Restart ➔ Yes.

4. In the profile of your account in the Ariba Network, select the SharedSecret authentication method in the cXML setup.

### 4.2 SAP SNC System Acting as a Server

No proxy or reverse proxy is required. The asynchronous inbound application service interfaces are called either internally in the SAP SNC system or by SAP Process Integration.

### 4.3 Roles and Authorizations

In Ariba Network Integration 1.0 for SAP Business Suite, you can use the authorization object ARBFND_ARB to execute reports and to process inbound messages. This object must be added by assigning the SAP Business Suite Integration Component for Ariba (SAP_ARBFND_INTEGRATION) role. To make sure the corresponding profile is available and active, you must generate the role profile using transaction PFCG.

A technical user is required in the SAP SNC back-end system to process the incoming messages. This user must not have the SAP_ALL authorization.

We recommend that you assign the roles required for the processing of purchase order confirmations and advanced shipping notifications (ASNs) to this user.

Depending on whether you use direct or mediated connectivity, you also have to assign one of the following roles:

- For **direct** connectivity:
  - Web Service Consumer (SAP_BC_WEBSERVICE_CONSUMER)
    - This role is required for using Web service protocol to communicate in direct connectivity.

- For **mediated** connectivity:
  - Exchange Infrastructure: Service User for Application Systems (SAP_XI_APPL_SERV_USER)
    - This role is required to communicate through XI protocol in mediated connectivity.
5 Operations Information

5.1 Message Monitoring

5.1.1 Direct Connectivity

Outbound Messages

A complete trace of the message processing can be found in the application log under the Ariba Integration (ARIBA_INTEGRATION) object. You can easily access the logs from the SAP Easy Access menu under [SAP Supply Network Collaboration] [Ariba Network Integration for SAP SNC] [Administration] [Display Logs for Outbound Messages] or by using the /SCA/ARB_MSG_OUT_LOG transaction.
You can search by the XML message ID, payload ID, or ID of the object (for example, PO number). You can enter the ID in the External ID field. Note that you should type an asterisk before and after an external ID, as shown in the following figure:

![Analyse Application Log](image)

Figure 7: Outbound Log for Direct Connectivity

The application log displays two entries for every outbound message. The first entry records the creation of the cXML message, the second one records its transfer to Ariba Network.

If the transfer of the outbound message is successful, the system displays a green status for both logs. Ariba Network accepts the document, and the message 201 Accepted is displayed.

The XML message IDs can be used as selection parameters for the XML monitor (transaction SXI_MONITOR) to directly access the corresponding cXML message.

**Note**

As of SAP_BASIS 7.40, you have to use the message monitor of Web Service Utilities (transaction SRT_MONI) for monitoring XML messages, instead of SXI_MONITOR.
The following figure (from SXI_MONITOR) shows how to select a cXML message by its message ID:

![Monitor for Processed XML Messages](image)

Figure 8: SXI Monitor in SAP SNC
The following figure (from transaction SRT_MONI) shows how to select a cXML message by its message ID:

![Web Service Utilities: Message Monitor](image)

**Figure 9: Selecting a cXML Message**

The monitor displays a checkered flag status for a successfully transferred message, as shown in the figure below. Given that the call to Ariba Network is synchronous, Ariba Network accepts and creates the message.
The following figure (from SXI_MONITOR) shows how a successfully transferred message is displayed in the monitor:

Figure 10: Successfully Transferred Message in SXI Monitor
The following figure shows in SRT_MONI how a successfully transferred message is displayed:

![Web Service Utilities: Message Monitor](image)

Figure 11: Successfully Transferred Message in SRT Monitor

**Inbound Messages**

Inbound messages are polled from Ariba Network by running the report *Fetch cXML messages for different message types from Ariba Network* (ARBFND_FETCH_CXML_MESSAGES_NEW). You must schedule the report to run regularly. For more information, see *Jobs to Be Scheduled* [page 24].

The add-on writes an application log entry for each executed poll and for each message retrieved from the network.

All cXML messages are displayed in the XML message monitor (transaction SXI_MONITOR).

---

**Note**

As of SAP_BASIS 7.40, you have to use the message monitor of Web Service Utilities (transaction SRT_MONI) for monitoring XML messages instead of the XML monitor (transaction SXI_MONITOR).

To filter the messages by a specific inbound message type, you can specify the interface name of the receiver by using one of the following standard selection criteria:

- cXMLConfirmationRequest_In
• cXMLShipNoticeRequest_In

The system displays the status for a message as follows:

• Checkered flag for successful processing
• Red for failed processing
• Green for queued processing

If Forward Error Handling (FEH) is activated, the system can display a yellow status. This means that the system has forwarded the issue to the FEH application.

The framework of Ariba Network Integration for SAP SNC additionally offers to send the processing status of an inbound message back to Ariba Network. You can activate this functionality in the Customizing activity Define Basic Message Settings by selecting the Send cXMLStatusUpdateRequest Message checkbox. For more information, see Customizing under Integration with Other SAP Components ➔ SAP Business Suite Integration Component for Ariba ➔ Framework Settings ➔ Define Basic Message Settings.

If this functionality is activated, an inbound message that has successfully been processed by the SAP SNC system changes the routing status of a document from Sent to Acknowledged on Ariba Network.

Inbound messages that have not been successfully processed by the SAP SNC system will change the status from Sent to Failed - provided that Forward Error Handling (FEH) is activated, and the message is discarded.
The following figure shows order confirmations with different statuses in the supplier’s outbox:

![Figure 13: Supplier’s Outbox on Ariba Network](image)

### 5.1.2 Mediated Connectivity

**Outbound Messages**

A complete trace of the message processing in SAP SNC system can be found in the application log under the Ariba Integration (ARIBA_INTEGRATION) object, OUTBOUND subobject. You can easily access the logs from the SAP Easy Access menu under SAP Supply Network Collaboration > Ariba Network Integration for SAP SNC > Administration > Display Logs for Outbound Messages or by using the /SCA/ARB_MSG_OUT_LOG transaction.
You can search by XML message ID, payload ID, or ID of the object (for example, PO number). You can enter the ID in the **External ID** field. Note that you have to insert an asterisk before and after an external ID, as shown in the following figure:

![Figure 14: Outbound Log in SAP SNC](image)

The application log displays exactly one entry for your outbound message. This entry records the creation of the cXML message.

If the message creation has been successful, the system displays a green status in the application log, and passes the message to your middleware.

The XML message IDs can be used as selection parameters for the XML monitor (transaction **SXI_MONITOR**) to directly access a cXML message.

The monitor displays a checkered flag status for a successfully transferred message. The monitor displays an error status if there is a technical connectivity issue between SAP SNC and SAP Process Integration. The system firsts sends a cXML message to SAP Process Integration, and then transfers the cXML message to Ariba Network.
The following figure shows how a successfully transferred message is displayed in the SXI monitor:

Figure 15: Successfully Transferred Message in SXI Monitor
The following figure shows how a successfully transferred message is displayed in the SRT_MONI transaction:

Figure 16: Successfully Transferred Message in SRT Monitor

The message transfer to Ariba Network has to be centrally monitored on SAP Process Integration.

Inbound Messages

Inbound messages are sent from SAP Process Integration to the SAP SNC system.

Ariba Network Integration for SAP SNC writes an application log entry for each message retrieved from SAP Process Integration.

All cXML messages are displayed in the XML message monitor (transaction SXI_MONITOR).

Note

As of SAP_BASIS 7.40, you have to use the message monitor of Web Service Utilities (transaction SRT_MONI) for monitoring XML messages instead of the XML monitor (transaction SXI_MONITOR).
To filter the messages by a specific inbound message type, you can specify the interface name of the receiver by using one of the following standard selection criteria:

- cXMLConfirmationRequest_In
- cXMLShipNoticeRequest_In

The system displays a status for a message as follows:

- Checkered flag for successful processing
- Red for failed processing
- Green for queued processing

If Forward Error Handling (FEH) is activated, the system can display a yellow status. This means that the system has forwarded the issue to the FEH application.

The framework of Ariba Network Integration for SAP SNC additionally offers to send the processing status of an inbound message back to Ariba Network. You can activate this functionality in Customizing activity Define Basic Message Settings by selecting the Send cXMLStatusUpdateRequest Message checkbox. For more information, see Customizing under Ariba Network Integration for SAP SNC > Message-Based Integration > Framework Settings > Define Basic Message Settings.

If this functionality is activated, an inbound message that has successfully been processed by the SAP SNC system changes the routing status of a document from Sent to Acknowledged on Ariba Network.

Inbound messages that have not been successfully processed by the SAP SNC system will change the status from Sent to Failed - provided that Forward Error Handling (FEH) is activated and the message is discarded.
The following figure shows order confirmations with different statuses in the supplier’s outbox:

![Order Confirmations](image)

Figure 17: Supplier’s Outbox on Ariba Network

### 5.2 Application Logs

The application log is the central tool for monitoring all activities in the SAP SNC system that is connected to Ariba Network Integration 1.0 for SAP Business Suite. You can access the application log using the generic transaction SLG1, or the transactions specific to Ariba Network Integration for SAP SNC:

- **Display Logs for Inbound Messages** ([/SCA/ARB_MSG_IN_LOG](#))
- **Display Logs for Outbound Messages** ([/SCA/ARB_MSG_OUT_LOG](#))
- **Display Logs for Single Sign-On** ([/SCA/ARB_SSO_LOG](#))

### Message-Based Integration

The SAP SNC system records all messages triggered to Ariba or received from Ariba in one or more entries under the **Ariba Integration** (ARIBA_INTEGRATION) object.
There are three subobjects for further filtering:

- **INBOUND**

Ariba Network Integration for SAP SNC processes all messages belonging to the namespace http://sap.com/xi/ARBFND1 and the below defined interfaces. Ariba Network Integration 1.0 for SAP Business Suite writes an entry to the application log. You can also review the processing status of the entries.

Messages that have been pushed into the SAP SNC system by middleware create an entry only with the subobject **INBOUND**. Messages that have been polled from Ariba Network directly into the SAP SNC system are included in both an entry with the subobject **INBOUND** and an entry with the subobject **POLLING**.

- **POLLING**

If you run the integration to Ariba Network through direct connectivity, you must schedule a polling job to retrieve messages. Each time the polling job runs, it writes an entry in the application log, listing the message type and timestamp when the system has polled.

After messages have been polled from Ariba Network, the log entry lists all message IDs (XML ID and payload ID) that have been retrieved and put in the queue for message processing.

- **OUTBOUND**

Every message leaving the SAP SNC system writes an entry to the application log with this subtype. For direct connectivity, there are two entries, one for the creation of the cXML message and the other indicating whether the message has successfully been transferred to Ariba Network.

Outbound messages triggered to Ariba Network also appear in the standard SAP SNC log under the **SNC_BIF** object and **REPLORD_I** subobject as being sent to Ariba Network.

**Single Sign-On**

The SAP SNC system also creates log entries for all the single sign-on attempts from Ariba Network. You can access these log entries from transaction **SLG1** using the /SCA/ARB object and the **SAML_SSO** subobject. You can easily access the logs for single sign-on from the SAP SNC Easy Access menu under **SAP Supply Network Collaboration** ➤ **Ariba Network Integration for SAP SNC** ➤ **Administration** ➤ **Display Logs for Single Sign-On** or by using the /SCA/ARB_MSG_SSO_LOG transaction.

**Search in the Application Log**

You can filter the application log entries by object and subobject as described above. **Date and Time** is also a filter criterion.

If you are searching for specific entries, you can also use the **External ID** field by entering a business object ID, a payload ID, or a XML message ID. Note that you have to insert an asterisk before and after the entered ID.

Since Ariba Network Integration for SAP SNC creates many entries to record the message exchange with Ariba Network, we recommend that you double check your settings for archiving your application log and make necessary adjustments. For more information, search for the phrase **Application Log - User Guidelines (BC-SRV-BAL)** in the documentation of SAP NetWeaver at http://help.sap.com.
5.3 Trace for Single Sign-On

In case a user cannot log on to SAP SNC from Ariba Network, you can analyze the trace of the single sign-on scenario by using the Security Diagnostic Tool for ABAP. You can launch the tool in your Web browser by entering the following URL: https://<host>:<port>/sap/bc/webdynpro/sap/sec_diag_tool?sap-client=<sap_client>

SAP recommends tracing the single sign-on scenario, and that you regularly delete the trace files.


5.4 Forward Error Handling

The Forward Error Handling (FEH) framework is available with SAP_BS_FND 701 and higher. For more information, search for the phrase Error and Conflict Handler in the documentation of SAP NetWeaver under http://help.sap.com.

Customizing Settings for FEH

Activate Error and Conflict Handler

You have activated Error and Conflict Handler (ECH) in your SAP application client. For more information, see Customizing for Cross-Application Components under Processes and Tools for Enterprise Applications ➔ Enterprise Services ➔ Error and Conflict Handler ➔ Activate Error and Conflict Handler. In the Activate ECH for Clients view, select the Activated checkbox.

Define Resolution Strategy

You have defined a resolution strategy that specifies whether and how processes are executed again or ended after errors or conflicts occur. You can define, for example, the periods during which a certain error can be corrected by automatically repeating the process.

For more information, see Customizing for Cross-Application Components under Processes and Tools for Enterprise Applications ➔ Enterprise Services ➔ Error and Conflict Handler ➔ Define Resolution Strategy. Ariba Network Integration 1.0 for SAP Business Suite provides the component BNS-ARI-SE-FND for which a resolution strategy can be created.

When defining error resolution strategy, you can find the following source fields:

- Business Process (PROCESS)
- Error Category (ERRORCATEGORY)
Ariba Network Integration for SAP SNC currently supports the following combinations of business processes and error categories:

- **Receive cXML ConfirmationRequest Message** (ARBFNDCONF)
  - This business process can have the following error categories:
    - **Processing Error** (PRE)
- **Receive cXML ShipNoticeRequest Message** (ARBFNDSHIP)
  - This business process can have the following error categories:
    - **Processing Error** (PRE)
- **Send cXML Message** (ARBFNDOADP)
  - This business process only applies if you use direct connectivity, and it can have the following error categories:
    - **Format Error** (FOE)
      - For example, Ariba Network may return the status codes “400” (Bad Request) or “406” (Not Acceptable), with the latter meaning that the sent cXML message was not accepted by Ariba.
    - **Authorization Error** (PRE.AUE)
      - Ariba Network returned for example the status codes “401” (Unauthorized) or “403” (Forbidden).
    - **Temporary Error** (PRE.TEE)
      - Ariba Network returned for example the status codes “560” (Temporary Server Error). This category of error should trigger an automatic retry.
    - **Processing Error** (PRE)
      - This category includes all other errors.

To process an order for which you have specified automatic retry, schedule the report **Resubmission of Postprocessing Orders** (/SAPPO/RESUBMIT_ORDERS_2).

### Postprocessing Desktop

A process postprocessing order (PPO) is created in FEH when there is an error in either inbound or outbound processing. Use **Error and Conflict Handler: Process Postprocessing Orders** (transaction ECH_MONI_SEL, available as of SAP_BS_FND 702) to analyze the errors. If this transaction is not available in your system, you can use the **Postprocessing Desktop** (transaction /SAPPO/PPO2).

The following table provides an overview of the business objects and the corresponding cXML messages for which errors may occur. Note that the business objects in the sense of FEH correspond to cXML message types.

<table>
<thead>
<tr>
<th>Business Object Type / Business Process</th>
<th>cXML Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARBFNDOADP</td>
<td>N/a.</td>
</tr>
<tr>
<td></td>
<td>This object is used for error handling of all outbound cXML messages.</td>
</tr>
<tr>
<td>ARBFNDCONF</td>
<td>Receive cXML ConfirmationRequest Message</td>
</tr>
<tr>
<td>ARBFNDSHIP</td>
<td>Receive cXML ShipNoticeRequest Message</td>
</tr>
</tbody>
</table>
Postprocessing Desktop: Edit Task

Double-click on a task to edit the details of the postprocessing order. In the Postprocessing Desktop - Edit Order: Details screen you can perform the following actions to resolve the error:

- **Repeat**
  The Repeat action restarts the processing of the cXML message. This is usually done after resolving an error, for example by changing the business object, by changing the payload, or after a temporary system issue has been resolved.

- **Display or change Payload**
  To resolve an error, it may be necessary that you change the Payload of a cXML message (see image below). You can make the required authorization settings in Customizing for Cross-Application Components under General Application Functions ➤ Error and Conflict Handler ➤ Authorization for Payload Editor.

![Figure 18: Changing Payload of a cXML Message](image)

- **Confirm**
  The Confirm action changes the order status of the PPO to Completed, closes the of the PPO, and sets the status to green. You normally use this option if an inbound cXML message could not be transferred and you have applied the changes to the business document manually.
• **Discard**

The *Discard* action also changes the order status of the PPO to *Completed*, closes the of the PPO, and sends a cXML *StatusUpdateRequest* message to Ariba Network to set the acknowledgement status of the corresponding Ariba document to *Failed*. 

---

**Figure 19: Confirming a PPO**

![Postprocessing Desktop - Display Order: Details](image)
5.5 Troubleshooting

Troubleshooting Outbound Messages

Messages can fail to be transferred from SAP SNC system to Ariba Network due to the following reasons:

- The cXML message cannot be created
- The cXML message cannot be transferred to SAP Process Integration (in case of mediated connectivity)
- The cXML message cannot be sent to Ariba Network

Troubleshooting Messages Transferring Purchase Orders
For purchase orders, you can track the creation of the cXML messages in the message processing log that you can access when displaying the purchase order in SAP SNC. This log also persists in the application log. For more information, see Application Logs [page 41].

Ariba Network Integration for SAP SNC does not create cXML messages containing data that is not supported by Ariba Network. Neither does it create cXML messages that do not contain the minimum set of required fields.

Once a cXML message has been created and you want to find out whether it has successfully reached Ariba Network, use the XML message monitor (transaction SXI_MONITOR).

The monitor displays messages that have not been transferred to Ariba Network with a red status (error status), as shown in the following figure:

![Monitor for Processed XML Messages](image)

**Figure 21: Message Transfer to Ariba Network Failed**

Depending on whether you use mediated connectivity or direct connectivity, the cause of the error must be analyzed differently:

- If you integrate with Ariba Network using **mediated** connectivity, analyze the communication between the SAP SNC system and your middleware.
- If you integrate with Ariba Network using **direct** connectivity, a synchronous call is performed from the SAP SNC system to Ariba Network. The error status of the message indicates the following possible issues:
  - Ariba Network currently cannot be reached.
  - You use the *Sending of Purchase Orders to Ariba Network* (/SCA/ARB_INT_MSG_ORDR_SEND) report to resend a purchase order document from SAP Supply Network Collaboration (SAP SNC) to Ariba.
Network. The report generates and sends a cXML message from the latest version of the purchase order document in SAP SNC.

- Your cXML message cannot be accepted by Ariba Network.
  In this case, you can view the short text of the error message by double-clicking the message. The long text of the error message, which describes the details of the error, can be found in the application log (transaction SLG1). You can search in the application log by entering the XML message ID as an external ID (insert an asterisk before and after the XML message ID). As a result, you receive two log entries: the first one with a green status, indicating that the cXML message has successfully been created; the second one with a red status, indicating that the cXML message has not been transferred to Ariba Network. Double-click the red log entry to see the messages. The error message contains a long text that you can display by clicking on Details. This error message is issued by Ariba Network. For more information, see Application Logs [page 41].

If FEH is activated, errors that occur during the transfer of cXML messages to Ariba Network create an object in FEH, and the error handling is done through FEH. For more information, see chapter Forward Error Handling [page 43].

Troubleshooting Inbound Messages

Messages that reside on Ariba Network in the outbound queue are either polled by the Ariba Network adapter from SAP Process Integration or by Ariba Network Integration for SAP SNC from the SAP SNC system.

If you use mediated connectivity, the polled messages are pushed into SAP SNC system, where the inbound processing is triggered. If the handover from the middleware to SAP SNC is not successful, the technical connectivity is likely to be the issue. Besides checking the connectivity setup between SAP SNC and the middleware, consider issues regarding the user name and password as well as authorization issues.

For both connectivity options, application-specific message processing issues can be recognized using transaction SXI_MONITOR.

By searching by the cXML message ID or cXML payload ID, you can also find an entry in the application log (transaction SLG1) that displays the error message.

**Note**

cXML messages are always retrieved from Ariba Network and placed into the inbound processing queue of the SAP Business Suite system, no matter whether they can be processed or not.

If you use direct connectivity, polling errors occur mainly due to authorization issues or due to temporary downtime of Ariba Network. For information about authorization, see Roles and Authorizations [page 28]. Failed polling attempts can be found in the application log of SAP SNC (transaction SLG1). The cXML messages remain on Ariba Network until the next successful polling, when all pending messages are picked up.

If FEH is activated, unsuccessful incoming cXML messages create an object in FEH, and the error handling is done using FEH. For more information, see Forward Error Handling [page 43].

An inbound message can fail to be processed for many reasons, for example, authorization issues, but the main reasons are application errors. For information about authorization, see Roles and Authorizations [page 28].

You can try to resolve the error and restart the message using transaction SXI_MONITOR.
The following figure shows an example of a purchase order confirmation cXML message that failed in inbound processing:

![Web Service Utilities: Message Monitor](image)

**Figure 22: Failed Purchase Order Confirmation Message**

You can double-click the cXML message and see the error message. You can also view the error message by entering the XML message ID or cXML payload ID in the application log (transaction SLG1).
You shall find one entry with the red error status, as shown in the following figure:

Figure 23: Error Message in the Application Log

In the above example, the error occurs because the current validation profile does not permit the underconfirmation of a purchase order item.
In case you are able to correct an error, go back to the XML monitor, select the message, and choose Repeat, as shown in the following figure:
Refresh the monitor, and check the message’s status again. The error status has changed to successful (marked by a checked flag), as shown in the following figure:

![Web Service Utilities: Message Monitor](image)

Figure 24: Message Status After Postprocessing

If the message contains data that you cannot process, you have the following options:

- **Recurring issue**
  You can permanently influence the data mapping and forward the data to the applications by implementing the pre-processing inbound BAdI. For more information, see [Settings for Message-Based Integration](#) [page 21].

- **One-time issue**
  If the issue is caused by incorrect data that you have received from the supplier, you can ask the supplier to correct the issue and resend the message. The failed cXML message in your inbound queue has to be canceled manually, and you can cancel the message by clicking [Cancel Processing of Messages with Errors](#).
6 Appendix

6.1 Configuration of SOA Manager

As a prerequisite, you have added Ariba's security certificate to your SAP SNC system, and set up the security settings. For more information, see chapter SAP SNC System Acting as a Client [page 25].

i Note
The configuration of Web services is required only for direct connectivity.

6.1.1 Define Inbound Services (Type Services)

Execute the Customizing activity Manage and Test Enterprise Services under Ariba Network Integration for SAP SNC Framework Settings Direct Connectivity Settings A new browser window opens. You make configuration on the SOA Management screen as follows:

1. On the Business Administration (or Service Administration) tab page, choose Web Service Administration (or Web Service Configuration).
2. Enter Service (or Service Definition) in the Search by field and CXML* in the Search Pattern field, then choose Go.

The system displays the following inbound services:
- CXMLCONFIRMATIONREQUEST_IN
- CXMLCOPYREQUEST_PAYMENTPROPOSAL (not relevant for SAP SNC integration)
- CXMLINVOICEDETAILREQUEST_IN (not relevant for SAP SNC integration)
- CXMLSHIPNOTICEREQUEST_IN
- CXMLSYNCHRONOUSOUTBOUNDADAPTER

i Note
The inbound service CXMLSYNCHRONOUSOUTBOUNDADAPTER receives cXML messages from the outbound services and sends the cXML messages to Ariba Network.

The other three inbound services (CXMLCONFIRMATIONREQUEST_IN, CXMLINVOICEDETAILREQUEST_IN, and CXMLSHIPNOTICEREQUEST_IN) receive cXML messages from Ariba Network through the outbound service of the Polling Agent and process these cXML messages in the SAP ERP system.
Configuration of the Inbound Service
CXMLSYNCHRONOUSOUTBOUNDADAPTER

Proceed as follows:

1. Choose CXMLSYNCHRONOUSOUTBOUNDADAPTER and choose Apply Selection.
2. Navigate to the Configurations tab page and choose Create Service. The SOA Management dialog box appears.
3. Enter the required values, and choose Apply Settings. The following table contains an example of a set of values you can enter:

Table 8:

<table>
<thead>
<tr>
<th>New Service Name</th>
<th>Description</th>
<th>New Binding Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYNC_OUTB_IN</td>
<td>Synchronous Outbound Service</td>
<td>SYNC_OUTB_IN</td>
</tr>
</tbody>
</table>

4. In the Configuration of Web Service ‘SYNC_OUTB_IN’: Endpoint ‘SYNC_OUTB_IN’ group box, navigate to the Transport settings tab page and choose Local System Call in the Make Local Call field.
5. Navigate to the Provider Security tab page of the group box and select the UserID/Password checkbox for the HTTP Authentication method.
6. Save your configuration.

The system displays a success message such as Binding ‘SYNC_OUTB_ADAPTER’ activated in Service ‘SYNC_OUTB_ADAPTER’. Alternatively, check the error messages and other messages at the top of the screen.

**i Note**

You will need to know the location of your newly defined inbound services to define the ports of the outbound services later on. Before you leave this transaction, note down this destination address. We recommend you also do this for the next 3 inbound services.

To note down the location information, continue with the following steps:

7. In the Details of Service Definition: CXMLSYNCHRONOUSOUTBOUNDADAPTER group box and on the Overview tab page, click the link Open WSDL document for selected binding or service. The system displays a new window.
8. Scroll down to the last line that starts with the text soap:address location= and copy this link to a separate document, for example, a Microsoft Word or Excel document. You need this link later on when defining outbound services. The following is an example of a link: http://abc1234.com:12345/sap/bc/srt/xip/sap/cxmsynchronousoutboundadapter/002/sync_outb_adapter/sync_outb_adapter

Taking the above link as an example, you can divide the link into the following parts:

- Computer name: abc1234.com
- Port number: 12345
- SICF path: /sap/bc/srt/xip/sap/cxmsynchronousoutboundadapter/002/sync_outb_adapter/sync_outb_adapter

**i Note**

Double-check the correctness of this part of the URL in transaction SICF by navigating through the default host services.
Result: You have defined the first inbound service `CXMLSYNCHRONOUSOUTBOUNDADAPTER`.

Repeat all of the above steps for each of the following services:

- `CXMLCONFIRMATIONREQUEST_IN`
- `CXMLSHIPNOTICEREQUEST_IN`

We recommend that you use the service definition to name the services you create. For example, you can use names such as `CONF_IN` and `SHIP_IN`. Note down the names you use, as you need so specify them when configuring the Polling Agent later on.

**Note**

Refresh the screen after carrying out the described activities.

### 6.1.2 Define Outbound Services (Type Consumer Proxies)

Start again from the *Web Service Administration* screen. On the *Search* tab page, enter *Consumer Proxy* in the *Search by* field and `co_arbfnd*` in the *Search Pattern* field, then Choose *Go*.

The system displays the following outbound services:

- `CO_ARBFND_PRX_CCINV_OUT` (not relevant for SAP SNC integration)
- `CO_ARBFND_PRX_GPDQ_OUT`
- `CO_ARBFND_PRX_GADP_OUT`
- `CO_ARBFND_PRX_ORDR_OUT`
- `CO_ARBFND_PRX_PAYP_OUT` (not relevant for SAP SNC integration)
- `CO_ARBFND_PRX_PAYR_OUT` (not relevant for SAP SNC integration)
- `CO_ARBFND_PRX_PAYS_OUT` (not relevant for SAP SNC integration)
- `CO_ARBFND_PRX_STAT_OUT`
- `CO_ARBFND_PRX_PCAS_OUT`

There are three groups of outbound services:

- **Services communicating directly with Ariba Network**
  
  The outbound service `CO_ARBFND_PRX_GPDQ_OUT` is for the Polling Agent. This service fetches cXML messages from Ariba Network synchronously.
  
  The outbound service `CO_ARBFND_PRX_GADP_OUT` is for the synchronous outbound adapter. This service sends cXML messages to Ariba Network.

- **Services getting data from SAP SNC and sending it to the synchronous outbound adapter**

  The outbound service `CO_ARBFND_PRX_ORDR_OUT` transfers purchase order data from SAP SNC to Ariba Network.

  The outbound service `CO_ARBFND_PRX_STAT_OUT` transfers status update data (for example, the order status update data) from SAP SNC to Ariba Network.

- **Services sending data from the Polling Agent to four inbound services**

  The adapter `CO_ARBFND_PRX_PCAS_OUT` is part of the Polling Agent and provides data to the following inbound services that send data to SAP SNC:

  - `CXMLCONFIRMATIONREQUEST_IN`
The following figure shows an overview of data communication between the services:

**Figure 25: Data Communication Between the Services**

**Configuration of the Outbound Service CO_ARBFND_PRX_ORDR_OUT**

Proceed as follows:

1. Choose the outbound service **CO_ARBFND_PRX_ORDR_OUT** and choose *Apply Selection*.
2. On the **Configurations** tab page, choose *Create Logical Port*. The **SOA Management** dialog box appears.
3. In the **General Configuration Settings** group box, select the **Manual configuration** radio button and select the **Logical Port is Default** checkbox.
4. Fill the required fields and choose *Apply Settings*. The following table contains an example of values that you can enter:

<table>
<thead>
<tr>
<th>Logical Port Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORDER_OUT</td>
<td>Outbound Order Request</td>
</tr>
</tbody>
</table>
5. Navigate to the *Transport settings* tab page and fill the required fields. Note that the data is taken from the inbound service `CXMLSYNCHRONOUSOUTBOUNDADAPTER` that you have configured in chapter *Define Inbound Services (Type Services)* [page 54]. The following table contains a set of values you can enter:

<table>
<thead>
<tr>
<th>Table 10:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL Access Path</strong></td>
<td><code>&lt;Enter URL Access Path for the</code></td>
</tr>
<tr>
<td></td>
<td><code>CXMLSYNCHRONOUSOUTBOUNDADAPTER service&gt;</code></td>
</tr>
<tr>
<td><strong>URL Protocol Information</strong></td>
<td><code>HTTP</code></td>
</tr>
<tr>
<td><strong>Computer Name of Access URL</strong></td>
<td><code>&lt;Enter Computer Name of Access URL for the</code></td>
</tr>
<tr>
<td></td>
<td><code>CXMLSYNCHRONOUSOUTBOUNDADAPTER service&gt;</code></td>
</tr>
<tr>
<td><strong>Port Number of Access URL</strong></td>
<td><code>&lt;Enter Port Number of Access URL for the</code></td>
</tr>
<tr>
<td></td>
<td><code>CXMLSYNCHRONOUSOUTBOUNDADAPTER service&gt;</code></td>
</tr>
<tr>
<td><strong>Make Local Call</strong></td>
<td><code>Local System Call</code></td>
</tr>
<tr>
<td><strong>Compress Response</strong></td>
<td><code>True</code></td>
</tr>
</tbody>
</table>

6. Navigate to the *Consumer Security* tab page, and select the *User ID/Password* checkbox. Save your configuration. The system displays a success message such as *Logical Port ORDER_OUT successfully activated*. Alternatively, check the error messages and other messages at the top of the screen.

Repeat the above described steps for the `CO_ARBFND_PRX_STAT_OUT` outbound services. Use `STATUS_OUT` for the logical port name.

**Note**

If the system displays an error message at the top of the screen, we recommend that you close the screen, reopen it, and repeat the steps.

### Configuration of the Outbound Service CO_ARBFND_PRX_PCAS_OUT

As mentioned above, this service sends data from the Polling Agent to four different inbound services. Therefore, you must define four logical ports as follows:

1. Choose the outbound service `CO_ARBFND_PRX_PCAS_OUT` and choose *Apply Selection*.
2. Navigate to the *Configurations* tab page and choose *Create Logical Port*.
   The *SOA Management* dialog box appears.
3. Choose *Manual configuration* as the configuration type, and deselect the *Logical Port is Default* checkbox.
4. Fill the required fields and choose **Apply Setting**. The following table contains an example of values you can enter:

<table>
<thead>
<tr>
<th>Logical Port Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONF_IN</td>
<td>Order Confirmation</td>
</tr>
</tbody>
</table>

5. Navigate to the **Transport settings** tab page, and check or fill the required fields. Note that the data is taken from the inbound service **CXMLCONFIRMATIONREQUEST_IN** that you have configured in chapter **Define Inbound Services (Type Services)** [page 54]. The following table contains a set of values you can check or enter:

<table>
<thead>
<tr>
<th>URL Access Path</th>
<th>&lt;Enter URL Access Path for the CXMLCONFIRMATIONREQUEST_IN service&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL Protocol Information</strong></td>
<td>HTTP</td>
</tr>
<tr>
<td><strong>Computer Name of Access URL</strong></td>
<td>&lt;Enter Computer Name of Access URL for the CXMLCONFIRMATIONREQUEST_IN service&gt;</td>
</tr>
<tr>
<td><strong>Port Number of Access URL</strong></td>
<td>&lt;Enter Port Number of Access URL for the CXMLCONFIRMATIONREQUEST_IN service&gt;</td>
</tr>
<tr>
<td><strong>Make Local Call</strong></td>
<td>Local System Call</td>
</tr>
<tr>
<td><strong>Compress Response</strong></td>
<td>True</td>
</tr>
</tbody>
</table>

6. On the **Consumer Security** tab page, select the **User ID/Password** checkbox.

7. Save your configuration. The system displays a success message such as **Logical Port 'CONF_IN' successfully activated**. Alternatively, check the error messages and other messages at the top of the screen.

Repeat steps 1 to 7 to create the other logical ports for the outbound service **CO_ARBFND_PRX_PCAS_OUT**. The information in the following table gives an example of the information you can use for the second logical port:

<table>
<thead>
<tr>
<th>Logical Port Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHIP_IN</td>
<td>Shipping Notification Request</td>
</tr>
</tbody>
</table>

Note that the required data on the **Transport settings** tab page is taken from the inbound service **CXMLSHIPNOTICEREQUEST_IN** that you have configured as described in the chapter **Define Inbound Services (Type Services)** [page 54].

**i Note**

Note down the names of the two logical ports. You will need them later on when you specify the settings for the Polling Agent in the Customizing activity **Define Settings for Polling Agent**. For more information, see
Customizing for Define Settings for Polling Agent under Ariba Network Integration for SAP SNC Framework Settings Direct Connectivity Settings.

Configuration of the Outbound Service CO_ARBFND_PRX_GPDQ_OUT

Proceed as follows:

1. Choose the outbound service CO_ARBFND_PRX_GPDQ_OUT and choose Apply Selection.
2. Navigate to the Configurations tab page and choose Create Logical Port. The SOA Management dialog box appears.
3. Choose Manual Configuration as the configuration type and select the Logical Port is Default checkbox.
4. Fill the required fields and choose Apply Settings. The following table contains an example of the values you can enter:

<table>
<thead>
<tr>
<th>Logical Port Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET_PENDING_DATA</td>
<td>ARIBA Polling Agent</td>
</tr>
</tbody>
</table>

5. On the Transport settings tab page, check or fill the fields. The following table contains a set of values you can check or enter:

<table>
<thead>
<tr>
<th>URL Access Path</th>
<th>/ANSapGateway.aw/ad/cxml</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Protocol Information</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Computer Name of Access URL</td>
<td>service.ariba.com</td>
</tr>
<tr>
<td>Port Number of Access URL</td>
<td>443</td>
</tr>
<tr>
<td>Name of Proxy Host</td>
<td>&lt;Enter the name of your Proxy Host&gt;</td>
</tr>
<tr>
<td>Port Number of Proxy Host</td>
<td>&lt;Enter the Port Number of your Proxy Host&gt;</td>
</tr>
<tr>
<td>Make Local Call</td>
<td>No Call in Local System</td>
</tr>
<tr>
<td>Compress Response</td>
<td>False</td>
</tr>
</tbody>
</table>

Note

You will receive the URL information from Ariba.

6. On the Consumer Security tab page, select the User ID/Password checkbox.
7. Save your configuration. The system displays a success message such as Logical Port GET_PENDING_DATA successfully activated. Alternatively, check the error messages and other messages at the top of the screen.
Repeat the steps above to configure the settings for the outbound service `CO_ARBFND_PRX_QADP_OUT`. You can use `SYNC_OUTB_ARIBA_CONNECT` as the logical port name.

### Note

You can test the ping Web service for every consumer proxy. To perform the test, click the Ping Web Service icon on the Configurations tab page in the Details page of each outbound consumer proxy. If successful, the system displays a successful message such as Web service ping successful for LP ‘GET_PENDING_DATA’, proxy ‘CO_ARBFND_PRX_STAT_OUT’.

You can now find your generated Web services in your SAP SNC system in the Maintain Services tool (transaction `SICF`). Make sure the services are active, and activate them if necessary. To find the services, double-click the default_host node, choose sap > bc > srt > xip > sap.

### 6.2 Extrinsic Elements (Extensibility)

Extensibility in the communication with Ariba Network is enabled by extrinsic elements in cXML messages. For more information, see the cXML User’s guide that is available at [http://cxml.org](http://cxml.org).

Ariba Network Integration 1.0 for SAP Business Suite supports enhancements for all types of outgoing messages with additional fields (extrinsics), as well as the processing of extrinsics in all types of incoming messages.

#### 6.2.1 Extrinsics in Outbound cXML Messages

To enhance a cXML message that you send to Ariba Network you have to add it in the outbound message mapping. To do this, use the enhancement spot `ARBERP_OUTBOUND` with the BAdI Definition `ARBERP_OUTBOUND_MAPPING`. This BAdI is available in Customizing for SAP Business Suite Integration Component for Ariba under Application-Specific Settings SAP ERP Integration Component for Ariba Business Add-Ins (BAdIs) BAdI: Outbound Mapping. See the Customizing documentation and the BAdI definition for the methods you can implement.

#### 6.2.2 Extrinsics in Inbound cXML messages

A cXML message that comes in from Ariba Network can hold additional data that you would like to process and store in SAP ERP. Therefore you must enhance the inbound message mapping. To do this, use the enhancement spot `ARBERP_INBOUND` with the BAdI Definition `ARBERP_INBOUND_MAPPING`. See the Customizing documentation and the BAdI definition for the methods you can implement.
6.3 Endpoints

The endpoints in Ariba Network manage and control the flow of data from Ariba Network to the various systems that are connected. An endpoint on Ariba Network acts as a document routing placeholder that ensures that documents from Ariba Network are sent to the intended target system. You can create endpoints on Ariba Network according to your business requirements.

Example Scenario

In your system landscape, you have an SAP SNC (system ID: SNC) system and two ERP systems (system IDs: ERP1 and ERP2). Both ERP systems are integrated with the SAP SNC system. SNC and ERP2 are integrated with Ariba Network.

In this case, purchase orders can reach Ariba Network both from SNC and from ERP2. In such a scenario, you create the endpoints in a way that allows Ariba Network to send, for example, the confirmations to the correct system.

1. On Ariba Network, define 3 business systems (logical system in SAP terminology): ERP1, ERP2, and SNC.
2. Under the business system ERP2, which is connected to both SNC and to Ariba Network, define two endpoints, for example: ENDP_ERP2, and ENDP_SNC.
   Generally speaking, create two endpoints for all business systems that are integrated with SAP SNC: one endpoint for the SNC connection, one endpoint for the direct connection between Ariba Network and the ERP system itself.
3. Assign the endpoint IDs to an ANID you use when you make the settings in the Endpoints for Ariba Network Customizing activity.
4. Assign the business system (logical system) and endpoint pairs to an ANID you use in the settings for the polling agent.

Customizing Settings for Endpoints

You have received one or several IDs, known as Ariba Network IDs (ANID). You use either a password (SharedSecret) or a client certificate with each ANID. Each credential represents a unique entity on Ariba Network, that is, your appearance to the vendors on the network. Maintain this information in Customizing for Ariba Network Integration for SAP SNC under Framework Settings > Define Credentials and End Points for Ariba Network. Proceed as follows:

1. Enter the ANID in the Ariba Network ID column.
2. Do not enter SharedSecret if you use endpoints. Use one of the following options:
   ○ If you want to use endpoints only for authentication, select Enable end points for authentication.
   ○ If you use direct connectivity, that is, you integrate with Ariba Network without a middleware, you use endpoints also to poll messages. In this case, select Enable end points for authentication and polling. As a result, the end point is available in the Customizing activity Define Settings for Polling Agent and is used for polling cXML messages from Ariba Network.
3. Select the above specified ANID, and select the *End points for Ariba Network* view in the left-hand pane.

4. Maintain the required data for each endpoint on the screen *End points for Ariba Network: Overview*.

   The SAP-internal key can be freely defined; it is used to reference the Ariba endpoint ID in the SAP system.

   **Caution**

   Make sure the ID of the endpoints and their settings, such as user and passwords, are the same on Ariba Network and in Ariba Network Integration for SAP SNC.
Important Disclaimers and Legal Information

Coding Samples

Any software coding and/or code lines / strings (“Code”) included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP’s gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP’s current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with “you”, or a gender-neutral noun (such as “sales person” or “working days”) is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP’s gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).