Informatica®

Informatica® Cloud Data Integration

Ariba V2 Connector

Informatica Cloud Data Integration Ariba V2 Connector
October 2023

© Copyright Informatica LLC 2019, 2024

This software and documentation are provided only under a separate license agreement containing restrictions on use and disclosure. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC.

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation is subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License.

Informatica, the Informatica logo, Informatica Cloud, and PowerCenter are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at https://www.informatica.com/trademarks.html. Other company and product names may be trade names or trademarks of their respective owners.

Portions of this software and/or documentation are subject to copyright held by third parties. Required third party notices are included with the product.

See patents at https://www.informatica.com/legal/patents.html.

DISCLAIMER: Informatica LLC provides this documentation "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of noninfringement, merchantability, or use for a particular purpose. Informatica LLC does not warrant that this software or documentation is error free. The information provided in this software or documentation may include technical inaccuracies or typographical errors. The information in this software and documentation is subject to change at any time without notice.

NOTICES

This Informatica product (the "Software") includes certain drivers (the "DataDirect Drivers") from DataDirect Technologies, an operating company of Progress Software Corporation ("DataDirect") which are subject to the following terms and conditions:

1. THE DATADIRECT DRIVERS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.
2. IN NO EVENT WILL DATADIRECT OR ITS THIRD PARTY SUPPLIERS BE LIABLE TO THE END-USER CUSTOMER FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES ARISING OUT OF THE USE OF THE ODBC DRIVERS, WHETHER OR NOT INFORMED OF THE POSSIBILITIES OF DAMAGES IN ADVANCE. THESE LIMITATIONS APPLY TO ALL CAUSES OF ACTION, INCLUDING, WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at infa_documentation@informatica.com.

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Publication Date: 2024-07-15

Table of Contents

Preface 5

Informatica Resources 5

- Informatica Documentation 5
- Informatica Intelligent Cloud Services web site 5
- Informatica Intelligent Cloud Services Communities 5
- Informatica Intelligent Cloud Services Marketplace 6
- Data Integration connector documentation 6
- Informatica Knowledge Base 6
- Informatica Intelligent Cloud Services Trust Center 6
- Informatica Global Customer Support 6

Chapter 1: Introduction to Ariba V2 Connector 7

Ariba V2 Connector assets 7

Ariba V2 objects 7

Introduction to Ariba 8

Administration of Ariba V2 Connector 8

- View supported formats for the tasks 8
- Enable ITK operations 9
- Enable SOAP operations 10
- Get the SSL certificate 11
- Configure the SSL certificate in Ariba 13

Chapter 2: Ariba V2 connections 14

Ariba V2 connection properties 14

Proxy server configuration 15

- Configure proxy server settings on Windows 15
- Configure proxy server settings on Linux 16

Rules and guidelines for Ariba V2 connections 17

Chapter 3: Mappings and mapping tasks with Ariba V2 Connector 18

ITK operations 18

- Ariba V2 sources in mappings and mapping tasks 18
- Ariba V2 targets in mappings and mapping tasks 19

SOAP operations 20

- Ariba V2 targets in mappings and mapping tasks 20
- Ariba V2 Midstream transformation in mappings 20

Rules and guidelines for mappings and mapping tasks 21

Chapter 4: Ariba V2 data type reference 22

Ariba V2 and transformation data types 22

Chapter 5: Troubleshooting 23

Troubleshooting a mapping 23

Index 24

Preface

Use *Ariba V2 Connector* to learn how to read from or write hierarchical data to Ariba by using Cloud Data Integration. Ariba V2 Connector integrates with Ariba using inbound SOAP web services and Ariba ITK support.

Learn to create an Ariba V2 connection, develop and run mappings and mapping tasks in Cloud Data Integration.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Intelligent Cloud Services web site

You can access the Informatica Intelligent Cloud Services web site at http://www.informatica.com/cloud. This site contains information about Informatica Cloud integration services.

Informatica Intelligent Cloud Services Communities

Use the Informatica Intelligent Cloud Services Community to discuss and resolve technical issues. You can also find technical tips, documentation updates, and answers to frequently asked questions.

Access the Informatica Intelligent Cloud Services Community at:

https://network.informatica.com/community/informatica-network/products/cloud-integration

Developers can learn more and share tips at the Cloud Developer community:

https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers

Informatica Intelligent Cloud Services Marketplace

Visit the Informatica Marketplace to try and buy Data Integration Connectors, templates, and mapplets:

https://marketplace.informatica.com/

Data Integration connector documentation

You can access documentation for Data Integration Connectors at the Documentation Portal. To explore the Documentation Portal, visit https://docs.informatica.com.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Intelligent Cloud Services Trust Center

The Informatica Intelligent Cloud Services Trust Center provides information about Informatica security policies and real-time system availability.

You can access the trust center at https://www.informatica.com/trust-center.html.

Subscribe to the Informatica Intelligent Cloud Services Trust Center to receive upgrade, maintenance, and incident notifications. The Informatica Intelligent Cloud Services Status page displays the production status of all the Informatica cloud products. All maintenance updates are posted to this page, and during an outage, it will have the most current information. To ensure you are notified of updates and outages, you can subscribe to receive updates for a single component or all Informatica Intelligent Cloud Services components. Subscribing to all components is the best way to be certain you never miss an update.

To subscribe, on the Informatica Intelligent Cloud Services Status page, click **SUBSCRIBE TO UPDATES**. You can choose to receive notifications sent as emails, SMS text messages, webhooks, RSS feeds, or any combination of the four.

Informatica Global Customer Support

You can contact a Global Support Center through the Informatica Network or by telephone.

To find online support resources on the Informatica Network, click **Contact Support** in the Informatica Intelligent Cloud Services Help menu to go to the **Cloud Support** page. The **Cloud Support** page includes system status information and community discussions. Log in to Informatica Network and click **Need Help** to find additional resources and to contact Informatica Global Customer Support through email.

The telephone numbers for Informatica Global Customer Support are available from the Informatica web site at https://www.informatica.com/services-and-training/support-services/contact-us.html.

CHAPTER 1

Introduction to Ariba V2 Connector

You can use Ariba V2 Connector to securely connect to Ariba from Data Integration and read from or write hierarchical data to Ariba.

You can use Ariba V2 Connector to read data from Ariba and integrate the data with other applications, databases, or flat file. You can also use Ariba V2 Connector to read data from a flat file or other applications and write data to Ariba.

You can use Ariba V2 objects as sources and targets in mapping tasks.

You can switch mappings to advanced mode to include transformations and functions that enable advanced functionality.

Ariba V2 Connector integrates with Ariba using inbound SOAP web services and Ariba ITK support. You can use Ariba V2 Connector on Windows and Linux operating systems. You can configure the proxy server settings for the Secure Agent to connect to Ariba.

Note: Ariba V2 Connector does not support the Hosted Agent.

Ariba V2 Connector assets

When you use Ariba V2 Connector, you can include the following Data Integration assets:

- Mapping
- Mapping task

For more information about configuring assets and transformations, see *Mappings*, *Transformations*, and *Tasks* in the Data Integration documentation.

Ariba V2 objects

Use Ariba V2 Connector to read data from or write data to Ariba using SOAP web services and ITK operations.

Ariba V2 Connector supports all ITK operations. Ariba V2 Connector supports export ITK operations as source objects and import ITK operations as target objects. Use the export ITK operations to read data from

Ariba and use the import ITK operations to insert, update, or upsert data in Ariba. Ariba V2 Connector does not support the delete operation.

Ariba V2 Connector supports all SOAP operations. The following table lists the default SOAP operations:

Objects	Read	Insert	Upsert	Update	Delete
Import Requisition	No	Yes	Yes	Yes	No
Import Suppliers	No	Yes	Yes	Yes	No
Import Company Codes	No	Yes	Yes	Yes	No
Import Purchase Organization	No	Yes	Yes	Yes	No
Search Catalog	Yes	No	No	No	No

Introduction to Ariba

Ariba is a cloud-based B2B application that is used to connect buyers and sellers. It allows sellers to manage their catalogs, bids, purchases, and invoices and enables buyers with the ability to search for suppliers, negotiate savings, procure goods and services, and track spending.

Administration of Ariba V2 Connector

As a user, you can use Ariba V2 Connector after the organization administrator performs the following tasks:

- View supported formats for the tasks.
- Configure the ITK and SOAP operations.
- Get the SSL certificate from a Certificate Authority.
- Configure the SSL certificate in Ariba.

View supported formats for the tasks

Before you enable an operation, you can check the supported format for the tasks. A file based format indicates that the task is an ITK task and a web service format indicates that the task is a SOAP or web service task.

Perform the following steps to view the supported formats for the tasks:

1. Log in to your Ariba account.
2. Go to **Manage** > **Core Administration**.
3. Under **Integration Manager**, click **Integration Configuration**.
4. In **Search Filters**, search the task by **Task Name** or click **List All** to view all tasks.
   The list of tasks and supported formats is displayed under **Configuration**.

The enabled or disabled tasks might vary based on the Ariba instance. For more details about enabled or disabled tasks, contact the Ariba administrator.

Enable ITK operations

Ariba V2 Connector supports all ITK based operations. To use ITK operations as Ariba V2 objects you need to create an ITK connection.

An ITK connection requires you to specify the location of the data dictionary file which is an Excel file. The operations listed in the Excel sheet are enabled in Ariba V2 Connector. The name of the operations in Ariba matches with the Task Name in the Excel sheet.

As task names and ITK names can vary based on the type of Ariba realm and integration configuration in Ariba respectively, you must use the Excel sheet to configure Ariba V2 Connector.

The organization administrator must perform the following tasks to enable ITK operations:

1. Get the user name and password for the Ariba account.
2. Get the Service URL and Realm name of the Ariba instance.
3. Get the certificate for SSL authentication.
4. Get the Shared Secret from the Integration Manager in Ariba for non-SSL authentication.
5. Enable the ITK operations as file-based in Ariba.
6. Download the data dictionary file from the Integration Manager in Ariba and perform the following steps:
    a. Open the data dictionary file and add a sheet with the name **AribaConnector_ITK_Names**.
    b. In the sheet, add the following column headers:
        - Task Name - Name of the operation in the data dictionary.
        - ITK Name - Name of the ITK operation enabled in Ariba.
    c. Enter the Task Name and ITK Name for the operations that you want to use and save the data dictionary file on your local machine.

Task Name	ITK Name
Export Purchase Orders	Export Purchase Orders
Export Purchase Order to ERP	Export Purchase Order
Export Receipts	Export Receipts
Export Receipt Status	Export Receipt Status
Export Supplier Organizations	Export Supplier Organizations
Export Payment Requests	Export Payment Requests
Export Financial Extract	Export Financial Extract
Import Purchase Order ID	Import Purchase Order Status
Import Receipt ID	Import Receipt Status

After the administrator enables the ITK operations, you can create an ITK connection to use ITK operations as Ariba V2 objects.

Note: You can use only ITK operations (downstream) available in the data dictionary, under Core Administration. You cannot use the ITK operations (upstream) available in the Administration data dictionary.

View task names and ITK names

Perform the following steps to view the task names and ITK names:

1. Log in to your Ariba account.
2. Go to **Manage** > **Core Administration**.
3. Under **Site Manager**, click **Data Import/Export**.
4. In **Search Filters**, search the task by **Task Name** or click **List All** to view all tasks.
   The **Import** tab and **Export** tab displays the list of task names and ITK names.

The enabled or disabled tasks might vary based on the Ariba instance. For more details about enabled or disabled tasks, contact the Ariba administrator.

If there is no ITK name for the task, the task might be a batch data import task. However, every task that does not have an ITK name might not be a batch data import task. You must check the task and the supported files. For a batch data import task, the file name is **Import Data Batch.**

Perform the following steps to view the file name:

1. In **Search Filters**, search **Import Batch Data**.
2. Click **Import**.
3. Select **Incremental Load** and then click **View Supported Files** to view the file names.

Note: Ariba V2 Connector supports only incremental load. Ariba V2 Connector uses the values in the source file to create and modify objects. If an object in the source file does not exist in the database, the object is created. If an object in the source file already exists in the database, it is updated with the values in the source file. For more details about incremental load, contact the Ariba administrator.

Enable SOAP operations

Ariba V2 Connector supports SOAP web services. To use SOAP operations as Ariba V2 objects, you need to create a SOAP connection.

The organization administrator must perform the following tasks to enable the SOAP operations other than the default SOAP operations in Ariba:

1. Configure the Ariba Endpoint URL.
2. Get the user name and password for the Ariba account.
3. Get the Service URL and Realm name of the Ariba instance
4. Enable the required operations as web service based in Ariba.
5. Create a properties file with the name `ARIBAV2_SOAP_OPERATIONS.txt` in the following location:
   `<Informatica Cloud Secure Agent installation directory>\apps\agentcore\conf\`

   In the properties file, add the list of SOAP operations that you want to use. To add the SOAP operation, enter the Task Name and Operation Name using a comma delimiter.

   - Task Name - Name of the SOAP operation in Ariba V2 Connector.
   - Operation Name - Name of the web service in Ariba.

Example

Let us assume that following is the service URL for Import Requisition in Ariba:

```
https://s1.ariba.com/Buyer/soap/yourdemoinabox/RequisitionImportPull?wsdl&validate=false
```

To enable the Import Requisition operation in Ariba V2 Connector, you must enter `Import Requisition, RequisitionImportPull` in the properties file, where Import Requisition is the name of the SOAP operation in Ariba V2 Connector and RequisitionImportPull is the name of the web service in Ariba.

The following list displays the task names and corresponding operation names:

- Search Catalog,WSCatalogItemSearch
- Export Contract ,WSExternalContractPull
- Import Receipt,ExternalReceiptImport
- Export Process,ProcessInvoiceExternallyExport
- Import Supplier,SupplierPull

View task names and SOAP operation names

Perform the following steps to view the task names and ITK names:

1. Log in to your Ariba account.
2. Go to **Manage** > **Core Administration**.
3. Under **Integration Manager**, click **Integration Configuration**.
4. In **Search Filters**, select the **Format** as **Web Service**, and then click **Search**.
   The list of web service tasks is displayed under **Configuration**.
5. Click the web service task name.
6. Click **View WSDL**.
   The SOAP operation name is displayed as the service name in the WSDL.

   For example, `<wsdl:service name="RequisitionImportPull">`

The enabled or disabled tasks might vary based on the Ariba instance. For more details about enabled or disabled tasks, contact the Ariba administrator.

Get the SSL certificate

You can create an ITK connection using an SSL certificate. When you use an SSL certificate, the Secure Agent establishes an encrypted connection to Ariba.

You can get an SSL certificate signed by a Certificate Authority using an SSL certificate tool of your choice.

Perform the following steps to generate an SSL certificate using the KeyStore Explorer:

Step 1: Create a new keystore

1. Download and install the KeyStore Explorer from the following link: http://keystore-explorer.org/.
2. Open the KeyStore Explorer.
3. Click **Create a new KeyStore**.
4. In the **New KeyStore Type** window, select **JKS**.

   Note: You need to provide the path to this KeyStore in the **Client Keystore** field in the connection properties while creating an SSL-based ITK connection.
5. Click **OK**

Step 2: Generate a key pair

1. Click **Tools** > **Generate Key Pair**.
2. In the **Generate Key Pair** window, select **RSA** as the algorithm and set the **Key Size** to **4096**.
3. Click **OK**.

4. In the **Generate Key Pair Certificate** window, click **Edit name** and configure the following fields:

Field name	Description
Common Name (CN)	The Fully Qualified Domain Name (FQDN) of the server.
Organization Unit (OU)	Name of the organization unit.
Organization Name (O)	Name of the organization.
Locality Name (L)	Name of the locality.
State Name (ST)	Name of the state.
Country (C)	Name of the Country.
Email (E)	Email address.

5. Click **OK**.
6. Enter the domain name of your server.
7. Click **Add Extensions**, click the + icon, and select **Subject Alternative Name**.
8. In the **Subject Alternative Name Extension** window, click the + icon.
9. Select **DNS Name** and in **General Name Value** field specify the domain name of your server.
10. Click **OK** until you return to the **Generate Key Pair Certificate** window.
11. In the **Generate Key Pair Certificate** window, click **OK**.
12. In the **New Key Pair Entry Alias** field, enter an alias for the key pair.
13. Click **OK**.
14. In the **New Key Pair Entry Password** field, enter a password, and click **OK**.

    Note: You need to provide this password in the **Client Key Password** field in the connection properties while creating an SSL-based ITK connection.

    The Generate Key Pair window displays a success message.
15. Click **OK** to save the KeyStore.
    The key pair is displayed in the KeyStore Explorer window.
16. In the KeyStore Explorer menu bar, click **File** > **Save**.
    The Set KeyStore Password window appears.
17. Enter a password for the KeyStore.

    Note: You need to provide this password in the **Client Keystore Password** field in the connection properties while creating an SSL-based ITK connection.
18. Click **OK**.
    The Save KeyStore As window appears.
19. Enter the name of the KeyStore.
    Consider the following format for your KeyStore for easy identification: `fqdn_domain_com.jks`
20. Click **Save**.
    Your KeyStore file is saved to your computer.

Step 3: Generate and send certificate signature request

1. In the KeyStore Explorer, right-click the key pair and select **Generate CSR**.

2. In the Generate CSR window, configure the required fields.
3. Click **OK**.
   The Generate CSR window appears with a success message.
4. Click **OK**.
5. Send the generated CSR file to the certificate authority.

Step 4: Import the signed certificate to the keystore

1. When the certificate authority returns the signed certificate and key, place them in a directory accessible by KeyStore Explorer.
2. In KeyStore Explorer, right-click the same key pair used to generate the CSR and select **Import CA Reply** > **From File**.
3. Select the signed certificate from the certificate authority, and click **Import**.
   The signed certificate is added to the key pair as the server-level certificate.
4. To verify the certificate chain, right-click the key pair entry, and select **View Details** > **Certificate Chain Details**.
5. To import intermediate and root-level certificates, right-click the key pair entry and select **Edit Certificate Chain** > **Append Certificate** to append the intermediate and root-level certificates.
6. In the menu bar, click **File** > **Save** to save the imported certificate to your keystore.

Configure the SSL certificate in Ariba

You need to configure the SSL certificate in Ariba to use the certificate in an ITK connection.

Perform the following steps to configure the SSL certificate in Ariba:

1. Log in to the Ariba account.
2. Go to **Manage** > **Core Administration** > **Integration Manager** > **Integration Toolkit Security**.
3. Select Certificate as the Authentication Type and paste the content of the certificate in the certificate content field.

CHAPTER 2

Ariba V2 connections

Create an Ariba V2 connection to access Ariba master and transactional data from Data Integration. You can create a connection on the Connections page or when you create a task. After you create a connection, it becomes available to all users who have access to the organization.

Ariba V2 connection properties

When you set up an Ariba V2 connection, you must configure the connection properties.

You can create an ITK or SOAP connection. When you create an ITK connection, Ariba allows authentication using shared secret or SSL certificate.

The following table describes the Ariba V2 connection properties:

Connection Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Connection Type	Type of Connection. You can select SOAP or ITK.
Service URL	URL for the Ariba service.
Realm/Site	Realm of the Ariba instance.
Data Dictionary File Location	Location of the data dictionary file on your local machine.
Use SSL Certificate	Applicable for ITK connection. Determines whether the Secure Agent establishes a secure connection to Ariba. When you select this option, the Secure Agent establishes an encrypted connection. SSL authentication requires Client Keystore, Client Keystore Password, and Client Key Password.

Connection Property	Description
Shared Secret	Shared Secret for the ITK connection. Leave the Shared Secret blank if you authenticate using SSL certificate on Ariba Network.
Client Keystore	The location of the client keystore file.
Client Keystore Password	The password for the client keystore file required for secure communication.
Client Key Password	The password for the client key.
User Name	Required for a SOAP connection. User name for the Ariba account.
Password	Required for a SOAP connection. Password for the Ariba account.

Proxy server configuration

If your organization uses an outgoing proxy server to connect to the internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux.

1. Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux.
2. Configure the JVM options of the DTM or the Secure Agent to use the proxy server at run time.

Contact your network administrator for the correct proxy settings.

Configure proxy server settings on Windows

You can configure the proxy server for both on-premises and cloud applications. When you configure the proxy server on a Windows machine, you must configure both the Secure Agent and the JVM options in DTM.

Configure proxy server settings through the Secure Agent Manager

Use the Secure Agent Manager to configure the Secure Agent to use the proxy server on Windows.

1. In the Secure Agent Manager, click **Proxy**.
2. To enter proxy server settings, click **Use a proxy server**.
3. Configure the following fields:

Field	Description
Proxy Host	Required. Host name of the outgoing proxy server that the Secure Agent uses.
Proxy Port	Required. Port number of the outgoing proxy server.

Field	Description
User Name	User name to connect to the outgoing proxy server.
Password	Password to connect to the outgoing proxy server.

4. Click **OK**.
   The Secure Agent Manager restarts the Secure Agent to apply the settings.

Configure proxy server settings through the JVM options in DTM

You can configure the JVM options of the DTM or the Secure Agent to use the proxy server at run time.

1. Log in to Informatica Intelligent Cloud Services.
2. Open Administrator and select **Runtime Environments**.
3. Select the Secure Agent for which you want to configure a proxy server.
4. On the upper-right corner of the page, click **Edit**.
5. In the **System Configuration Details** section, select the **Type** as **DTM** for the Data Integration Server.
6. Add the following parameters in any **JVMOption** field and specify appropriate values for each parameter:

```
JVMOption1= -Dhttps.proxySet=True
JVMOption2= -Dhttps.proxyHost=<proxy_server_hostname>
JVMOption3= -Dhttps.proxyPort=<proxy_server_portnumber>
JVMOption4= -Dhttps.proxyUser=<user name>
JVMOption5= -Dhttps.proxyPassword=<password>
```

7. Click **Save**.
   The Data Integration Server restarts to apply the settings.

Configure proxy server settings on Linux

You can configure the proxy server for both on-premises and cloud applications. You must configure the proxy server on a Linux machine using both the shell command and the JVM options in DTM.

Configure proxy server settings through the shell command

Use the shell command to configure proxy server settings for the Secure Agent on a Linux machine.

1. Navigate to the following directory:
   `<Secure Agent installation directory>/apps/agentcore/`
2. Run the following command:
   `./consoleAgentManager.sh configureProxy <proxy host> <proxy port> <user name> <password>`
3. Restart the Secure Agent.

Configure proxy server settings through the JVM options in DTM

You can configure the JVM options of the DTM or the Secure Agent to use the proxy server at run time.

1. Log in to Informatica Intelligent Cloud Services.
2. Open Administrator and select **Runtime Environments**.
3. Select the Secure Agent for which you want to configure the proxy server.

4. On the upper-right corner of the page, click **Edit**.
5. In the **System Configuration Details** section, select the **Type** as **DTM** for the Data Integration Server.
6. Add the following parameters in any **JVMOption** field and specify appropriate values for each parameter:
   ```
   JVMOption1= -Dhttps.proxySet=True
   JVMOption2= -Dhttps.proxyHost= <proxy_server_hostname>
   JVMOption3= -Dhttps.proxyPort=<proxy_server_portnumber>
   JVMOption4= -Dhttps.proxyUser=<user name>
   JVMOption5= -Dhttps.proxyPassword=<password>
   ```
7. Click **Save**.
   The Data Integration Server restarts to apply the settings.

Rules and guidelines for Ariba V2 connections

Consider the following rules and guidelines for Ariba V2 connections:

- You can create an ITK connection using the Shared Secret or SSL certificate.
- The service URL for an ITK connection is based on the authentication type.
  For example, if the service URL for connection based on the shared secret is `https://s1.ariba.com/Buyer`, then the service URL for SSL-based connection is `https://certs1.ariba.com/Buyer`

  You can get these URLs from the Ariba Administrator.
- The service URL for a SOAP connection is based on the WSDL or Ariba endpoint that is exposed.
  For example, if the WSDL URL for import requisition is `https://s1.ariba.com/Buyer/soap/bconedemoinabox/WSCatalogItemSearch?wsdl&validate=false`, you must specify the service URL as `https://s1.ariba.com/Buyer`
- When you create an ITK connection using SSL certificate, you must provide the Client Keystore, Client Keystore Password, and Client Key Password.
- For an ITK connection, Ariba V2 Connector uses the Export Purchase Orders operation to test the connection. You must enable the Export Purchase Orders operation as a File-based operation in Ariba for a successful connection.
- For a SOAP connection, Ariba V2 Connector uses the Catalog Item Search operation to test the connection. You must enable the Catalog Item Search operation as a Web Service based operation in Ariba and configure the endpoint for a successful connection.

CHAPTER 3

Mappings and mapping tasks with Ariba V2 Connector

Use the Data Integration Mapping Designer to create a mapping. When you create a mapping, you configure a source or target to represent Ariba V2 object.

In advanced mode, the Mapping Designer updates the mapping canvas to include transformations and functions that enable advanced functionality.

ITK operations

Ariba V2 Connector supports export ITK operations as source objects and import ITK operations as target objects.

For more information about how to enable ITK operations, see "Enable ITK operations" on page 9.

Ariba V2 sources in mappings and mapping tasks

To read data from Ariba, configure an Ariba V2 object as a Source transformation in a mapping task. Ariba V2 Connector supports all export ITK operations as source objects in a mapping task.

The following table describes the Ariba V2 source properties that you can configure in a Source transformation:

Property	Description
Connection	Name of the source connection.
Operation	The export ITK operation that you want to use as a source object.

The following table describes the advanced source properties that you can configure in a Source transformation:

Property	Description
Cache Size for Web Service Response (KB)	Not applicable. **Note:** Do not change the value of this property unless Informatica Global Customer Support instructs you to do so.

The following table describes the Request Options that you can configure in a Source transformation:

Property	Description
Request Message	Request message for the operation that you want to perform in Ariba. The request message is in XML format. You can copy and paste the request message from the Request Message Template.

Date filter

You can use the date filter for export ITK operations to read transactional data. You must specify the `fromDate` and `toDate` in the date filter for transactional data in one of the following formats:

- `MM/DD/YYYY`
- `MM/DD/YYYY HH:mm:ss`
- `MM/DD/YYYY HH:mm:ss z`
  Where `z` represents the time zone.
- `yyyy-MM-dd`
- `yyyy-MM-dd HH:mm:ss`
- `yyyy-MM-dd HH:mm:ss z`
  Where `z` represents the time zone.

Note: Informatica recommends not to specify the time zone. The time zone is automatically updated based on the time zone of the machine where the Secure Agent is installed.

Ariba does not support date filter for master data.

Field mapping in a Source transformation

On the Response Mapping tab, you can view the metadata hierarchy in response structure. The Secure Agent fetches the metadata from the sheet corresponding to the operation in the data dictionary. Each CSV file is added as a separate hierarchical group of fields based on the hierarchy in the data dictionary.

Ariba V2 Connector uses a heuristic approach to identify the primary key (_PK) for the parent CSV file and the foreign key (_FK) for each child CSV that helps you handle the data for all the downstream operations. When you map the elements from the response structure to the output fields, the Secure Agent creates the output groups, along with the primary and foreign keys for the field names.

Ariba V2 targets in mappings and mapping tasks

To write data to Ariba, configure an Ariba V2 object as a Target transformation in a mapping task. Ariba V2 Connector supports all import ITK operations as target objects in a mapping task.

The following table describes the Ariba V2 target properties that you can configure in a Target transformation:

Property	Description
Connection	Name of the target connection.
Operation	The import ITK operation that you want to use as a target object.

The following table describes the advanced target properties that you can configure in a Target transformation:

Property	Description
Cache Size for Web Service Request (KB)	Memory available for the web service request. If the web service request contains large volume of hierarchical data, you might want to increase the cache size. Default and minimum value is 1024 KB. Maximum value is 10239 KB.

SOAP operations

Ariba V2 Connector supports SOAP operations as target objects.

For more information about how to enable SOAP operations, see "Enable SOAP operations" on page 10.

Ariba V2 targets in mappings and mapping tasks

Ariba V2 Connector supports inbound operations as target objects.

Ariba V2 Connector supports all import operations as target objects in a mapping task.

The following table describes the Ariba V2 target properties that you can configure in a Target transformation:

Property	Description
Connection	Name of the target connection.
Operation	The SOAP operation that you want to use as a target object.

The following table describes the Ariba V2 advanced target properties:

Property	Description
Cache Size for Web Service Request (KB)	Not applicable. **Note:** Do not change the value of this property unless Informatica Global Customer Support instructs you to do so.

Ariba V2 Midstream transformation in mappings

Use Ariba V2 Connector to interact with web service applications that support SOAP API. Ariba V2 Connector supports Midstream transformation for a SOAP web service that has both request and response associated with it. You can use Ariba V2 Connector Midstream in a mapping to pass a single request to a web service application and process the response data.

Ariba V2 Connector does not support multiple source objects in a midstream transformation.

Before you configure a midstream transformation, you must create a business service from the **Configure** tab. You must select an Ariba V2 connection and a SOAP operation when you create a business service.

Perform the following steps to configure Midstream transformation:

1. On the **Web Service** tab, select the business service and the operation
2. On the **Request Mapping** tab, map the incoming fields from the source to the elements of Request Structure to form a web service request.
3. On the **Response Mapping** tab, map the selected elements from the response structure with the output fields.
   You can view the response structure on the Response Mapping tab. When you map the elements from the response structure to the output fields, the Secure Agent creates the output groups, along with the primary and foreign keys for the field names.
4. On the **Advanced** tab, you can specify the cache size details. The fields that you select from the Response Structure of the Web Service transformation appear as incoming fields for the target object.
5. On the **Field Mapping** tab, map the incoming fields to the target fields.
6. Click **Task Wizards** > **Mapping Task**, and select the mapping for the task.

Rules and guidelines for mappings and mapping tasks

Consider the following guideline for mappings and mapping tasks.

- Ensure that you configure the prerequisite operations or objects in Ariba before using specific operations. For example, if you want to export the payment request for a purchase order using the Export Payment Request operation, you must first create an invoice for the purchase order and it must be in Reconciled state.
- The field mapping might display an incorrect value for the total number of input fields mapped. For example, the total number of fields mapped appear as **3 of 7 mapped** instead of **3 of 3 mapped**.
- When you read data from Ariba, ensure that the export operation has a primary key or columns that qualify as a primary key, else the first column with no null values in considered as the primary key. This might lead to missing data in the target.
  You might encounter this issue with the Export Receipt Status operation.

CHAPTER 4

Ariba V2 data type reference

Data Integration uses the following data types in synchronization tasks and mapping tasks with Ariba V2:

Ariba V2 native data types

Ariba V2 data types appear in the Target transformations when you choose to edit metadata for the fields.

Transformation data types

Set of data types that appear in the transformations. They are internal data types based on ANSI SQL-92 generic data types, which the Secure Agent uses to move data across platforms. Transformation data types appear in all transformations in a mapping.

When Data Integration reads source data, it converts the native data types to the comparable transformation data types before transforming the data. When Data Integration writes to a target, it converts the transformation data types to the comparable native data types.

Ariba V2 and transformation data types

The following table lists the Ariba data types that Data Integration supports and the corresponding transformation data types:

Ariba data type	Transformation data type	Range and description
DOUBLE	Double	0 to 15
STRING	String	0 to 255 characters

CHAPTER 5

Troubleshooting

Use the following sections to troubleshoot errors in Ariba V2 Connector.

Troubleshooting a mapping

When I run a mapping, the mapping fails with the following message:

```
Output precision is less than Output length
```

To resolve the issue, increase the cache size for the web service request in the advanced target properties.

The mapping task is successful but data is not loaded to Ariba

When you monitor a job in Cloud Data Integration, the status of a task indicates the success or failure of the initiation of a job to import data into Ariba.

To know the correct status of the initiated job at the Ariba endpoint, perform the following steps:

1. Log in to your Ariba account.
2. Go to **Manage** > **Core Administration**.
3. Under **Integration Manager**, click **Data Import/Export**.
4. In **Search Filters**, search the ITK operation by the task name that you want to write to Ariba.
   If the ITK operation is written to Ariba, the status shows **Completed**.
5. Click **Completed**.
6. In the **History** tab, you can verify the status and the number of records created or updated in Ariba.
   The status **Completed** indicates that the task is successful.

INDEX

A

Ariba V2
  connection properties 14
Ariba V2 Connector
  assets 7
  objects 7
  overview 7

C

Cloud Application Integration community
  URL 5
Cloud Developer community
  URL 5
connections
  Ariba V2 14

D

Data Integration community
  URL 5
data type reference
  transformation data type 22

E

enable
  ITK operations 9
  SOAP operations 10

I

Informatica Global Customer Support
  contact information 6
Informatica Intelligent Cloud Services
  web site 5
ITK operations
  enable 9
  objects 7
  sources 18
ITK operations *(continued)*
  targets 19

M

maintenance outages 6
mapping
  ITK operations 18
  rules and guidelines 21
  SOAP operations 20

O

overview
  Ariba V2 Connector 7

S

SOAP operations
  enable 10
  objects 7
  targets 20
  web services 20
status
  Informatica Intelligent Cloud Services 6
system status 6

T

trust site
  description 6

U

upgrade notifications 6

W

web site 5