



Informatica® Cloud Data Integration

SAP Connector

© Copyright Informatica LLC 2015, 2021

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: 2021-06-21

Table of Contents

Preface	9
Informatica Resources.	9
Informatica Documentation.	9
Informatica Intelligent Cloud Services web site.	9
Informatica Intelligent Cloud Services Communities.	9
Informatica Intelligent Cloud Services Marketplace.	9
Data Integration connector documentation.	10
Informatica Knowledge Base.	10
Informatica Intelligent Cloud Services Trust Center.	10
Informatica Global Customer Support.	10
 Part I: Introduction to SAP Connector.....	 11
 Chapter 1: Introduction to SAP Connector.	 12
SAP Connector overview.	12
Data Integration and SAP integration methods.	12
Data Integration using SAP tables.	13
Data Integration using BAPI/RFC functions.	13
Data Integration using IDocs.	13
Data Integration using SAP ADSO Writer.	14
Data Integration using SAP ODP Extractor.	14
Communication interfaces.	15
SAP Metadata utility.	15
 Part II: SAP Connector Administration.....	 16
 Chapter 2: SAP Connector administration.	 17
SAP Connector administration overview.	17
SAP Table Connector administration.	17
Step 1. Verifying if the required licences are available for SAP Table Connector.	18
Step 2. Downloading and installing the Microsoft Visual C++ Redistributable.	18
Step 3. Downloading and configuring the libraries for table read and write.	18
Step 4. Configuring sapnwrfc.ini.	21
Step 5. Configuring SAP user authorization.	24
Step 6. Installing SAP Table connection transport files.	25
Step 7: Configuring HTTPS.	26
Step 8: Configuring the Secure Agent as a whitelisted host in SAP (optional).	29
SAP IDocs and RFCs/BAPI Connector administration.	30
Step 1. Verifying if the required licences are available for SAP IDocs and RFCs/BAPI Connector.	30

Step 2. Downloading and installing the Microsoft Visual C++ Redistributable.	31
Step 3. Downloading and configuring SAP libraries for IDoc and BAPI/RFC.	31
Step 4. Configuring sapnwrfc.ini.	33
Step 5. Defining SAP Connector as a logical system in SAP.	35
Step 6. Configuring SAP user authorizations.	38
Step 7. Installing and configuring the SAP IDocs Metadata utility.	39
SAP BW Connector administration.	40
Step 1. Verifying if the required licences are available for SAP BW Connector.	40
Step 2. Downloading and configuring the libraries for SAP BW data extraction.	40
Step 3. Installing SAP BW Reader transport files.	41
Step 4: Configuring HTTPS.	42
Step 5. Configuring SAP user authorizations.	43
SAP ODP Extractor Connector administration.	43
Step 1. Verifying if the required licenses are available for SAP ODP Extractor Connector.	43
Step 2. Verifying and installing prerequisite SAP Notes in the SAP server	44
Step 3. Installing SAP ODP Extractor Connector transport files.	44
Step 4. Configure SAP user authorization.	45
Step 5. Download and configure the SAP libraries.	47
SAP ADSO Writer Connector administration.	48
Step 1. Verifying if the required licenses are available for SAP ADSO Writer.	48
Step 2. Verifying the prerequisites for SAP server.	48
Step 3. Installing SAP ADSO Writer Connector transport files.	49
Step 4. Configure SAP user authorization.	50
Step 5. Download and configure the SAP libraries.	51

Part III: Connections. 53

Chapter 3: SAP connections. 54

SAP connections overview.	54
SAP Table connections.	55
SAP Table connection properties	55
SAP connection rules and guidelines.	56
SAP IDoc and BAPI/RFC connections.	57
SAP RFC/BAPI interface connection properties.	57
SAP IDoc Reader connection properties.	58
SAP IDoc Writer connection properties.	58
SAP BW Reader connections.	59
SAP BW Reader connection properties.	59
SAP ADSO Writer connections.	61
SAP ADSO Writer connection properties.	62
SAP ODP Extractor connections.	66
SAP ODP Extractor connection properties.	66
Creating an SAP Table connection.	70

Creating an SAP IDoc Reader connection.	71
Creating an SAP IDoc Writer or SAP RFC/BAPI interface connection	72
Creating an SAP BW Reader connection.	73
Creating an SAP ADSO Writer connection.	74
Creating an SAP ODP Extractor connection.	76
Chapter 4: Troubleshooting.	78
Troubleshooting.	78
SAP Table connection errors.	79
Part IV: Data Integration using SAP Table.	80
Chapter 5: SAP Table	81
SAP objects.	81
ABAP CDS views.	81
Rules and guidelines for SAP sources and targets.	82
Chapter 6: Synchronization tasks with SAP Table.	84
Synchronization tasks with SAP Table overview.	84
SAP Table sources in synchronization tasks.	84
SAP Table lookups in synchronization tasks.	86
Configuring a synchronization task with a single SAP object as the source.	86
Configuring a synchronization task with multiple SAP objects as the source.	88
Monitoring a synchronization task.	90
Synchronization task example.	90
Step 1: Define the synchronization task.	91
Step 2: Configure the SAP Table source.	91
Step 3: Configure the flat file target.	93
Step 4: Configure the field mapping.	94
Chapter 7: Mappings and mapping tasks with SAP Table.	95
Mapping and mapping tasks with SAP Table overview.	95
SAP Table sources in mappings.	96
Delta extraction for SAP table reader mappings.	97
Delta extraction behavior.	98
Informatica custom table /INFADI/TBLCHNGN.	98
Update modes for delta extraction	99
Configuring a parameter file for delta extraction.	100
Configure a table name override for delta extraction	101
Rules and guidelines for delta extraction.	102
Configuring delta extraction for an SAP table reader mapping.	102
Troubleshooting delta extraction for SAP Table Reader mappings.	103
Key range partitioning for SAP Table sources.	103

Configuring key range partitioning for SAP Table sources.	104
Best practices for key range partitioning.	104
SAP Table lookups in mappings.	104
Configuring a mapping with an SAP Table source.	105
Creating a mapping task.	106
Mapping with an SAP Table source example.	107
Step 1: Define the mapping.	107
Step 2: Configure the SAP Table source.	107
Step 3: Configure the flat file target.	110
Step 4: Save the mapping and create a mapping task.	112
 Part V: Data Integration using BAPI/RFC functions.	113
 Chapter 8: BAPI/RFC mapplets.	114
BAPI/RFC mapplets overview.	114
BAPI/RFC mapplet parameters.	115
BAPI/RFC parameter properties.	115
BAPI/RFC functions with nested structures.	116
System variables.	117
Integration ID in BAPI/RFC mapplet.	117
Target object for BAPI/RFC error output.	118
Rules and guidelines for BAPI/RFC mapplets in mappings.	118
 Chapter 9: Mapping and mapping tasks using BAPI/RFC functions.	119
Mapping and mapping tasks using BAPI/RFC functions overview.	119
Generating a BAPI/RFC mapplet.	120
Configuring a mapping with a BAPI/RFC mapplet.	120
Mappings with BAPI/RFC function example.	121
Step 1: Generating a BAPI/RFC mapplet in Data Integration for the BAPI_SALESORDER_CREATEFROMDAT1 BAPI function.	123
Step 2: Configuring a mapping with the bapi_salesorder_createfromdat1 mapplet.	124
 Part VI: Data Integration Using IDocs.	127
 Chapter 10: IDoc mapplets.	128
IDoc mapplets overview.	128
Segments and groups.	128
Segment and group status.	129
IDocs properties.	130
Outbound mapplet.	131
Outbound mapplet ports.	131
Target object for outbound mapplet error output.	132
Inbound mapplet.	132

Key fields and control record fields.	132
IDoc primary and foreign keys.	133
Importing IDoc metadata.	135
Chapter 11: Mapping and mapping tasks using IDocs.	137
Mapping and mapping tasks using IDocs overview.	137
IDoc reader sources in mappings.	138
Importing an IDoc mapplet to Data Integration.	139
Configuring an outbound mapping to read IDocs from SAP.	139
Configuring an inbound mapping to write IDocs to SAP.	140
Outbound mapping to read IDocs from SAP example.	141
Step 1: Importing MATMAS IDoc metadata.	142
Step 2: Importing the MATMAS04_Interpreter_Mapping mapplet to Data Integration.	144
Step 3: Configuring an outbound mapping with the MATMAS IDoc.	145
Inbound mapping to write IDocs to SAP example.	147
Step 1: Importing MATMAS IDoc metadata.	148
Step 2: Importing the MATMAS03_Prepare_Mapping mapplet to Data Integration.	149
Step 3: Configuring an inbound mapping with the MATMAS IDoc.	149
Part VII: SAP BW Data Extraction	152
Chapter 12: Synchronization tasks with SAP BW.	153
Synchronization tasks with SAP BW overview.	153
SAP BW sources in Synchronization tasks.	154
Configuring a Synchronization task with a single SAP BW object as the source.	155
Monitoring a Synchronization task.	156
Chapter 13: Mappings and Mapping tasks with SAP BW.	157
Mappings and Mapping tasks with SAP BW overview	157
SAP BW sources in mappings.	158
Configuring a mapping with a single SAP BW source.	158
Creating a Mapping task.	160
Monitoring a Mapping task.	161
Rules and guidelines for SAP BW sources.	161
Part VIII: Data Integration using SAP ODP Extractor.	162
Chapter 14: SAP ODP.	163
SAP ODP sources.	163
Rules and guidelines for SAP ODP sources.	164
Chapter 15: Mappings and mapping tasks with SAP ODP Extractor.	165
Mapping and mapping tasks overview.	165

SAP ODP sources in mappings.	166
Delta extraction for SAP ODP Extractor mappings.	168
Fixed partitioning for SAP ODP sources.	168
Configuring a mapping with an SAP ODP source.	169
Creating a mapping task.	170
Part IX: Data Integration for SAP ADSO.....	171
Chapter 16: Data Integration for SAP ADSO sources using SAP Table Reader.....	172
SAP ADSO sources.	172
Importing an SAP ADSO object.	173
Chapter 17: Data Integration for SAP ADSO targets using SAP ADSO Writer	174
SAP ADSO targets.	174
Rules and guidelines for SAP ADSO targets.	174
Chapter 18: Mappings and mapping tasks with SAP ADSO Writer.....	176
Mapping and mapping tasks overview.	176
SAP ADSO Extractor targets in mappings.	177
Activate option mode for SAP ADSO Writer mappings.	178
Fixed partitioning for SAP ADSO targets.	178
Configuring a mapping with an SAP ADSO target.	179
Creating a mapping task.	180
Appendix A: SAP data type reference.....	182
SAP data type reference overview.	182
SAP and transformation data types.	183
Rules and guidelines for SSTRING, STRING, and RAWSTRING data types.	185
SAP BW and transformation data types.	185
Index.....	187

Preface

Use *SAP Connector* to learn how to read from or write to SAP by using Cloud Data Integration. Learn to create an SAP connection, develop and run synchronization tasks, mappings, mapping tasks, and data transfer 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, go to <https://status.informatica.com/> and click **SUBSCRIBE TO UPDATES**. You can then 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 Customer Support Center by telephone or online.

For online support, click **Submit Support Request** in Informatica Intelligent Cloud Services. You can also use Online Support to log a case. Online Support requires a login. You can request a login at <https://network.informatica.com/welcome>.

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>.

Part I: Introduction to SAP Connector

This part contains the following chapter:

- [Introduction to SAP Connector, 12](#)

CHAPTER 1

Introduction to SAP Connector

This chapter includes the following topics:

- [SAP Connector overview, 12](#)
- [Data Integration and SAP integration methods, 12](#)
- [Communication interfaces, 15](#)
- [SAP Metadata utility, 15](#)

SAP Connector overview

You can use SAP Connector to integrate with SAP systems in batch, asynchronous, or synchronous modes based on your requirements.

Data Integration supports ABAP, IDoc read, IDoc write, BAPI/RFC, ODP read, and ADSO write functions to integrate with SAP systems. You can choose an SAP connection type to connect to SAP systems based on the interface requirements.

You can use the SAP connection in synchronization tasks, mappings, and mapping tasks. Create a synchronization task to synchronize data between a source and target. Create a mapping task to process data based on the data flow logic defined in a mapping or integration template.

You can also use the SAP connection in data transfer tasks. For more information about configuring data transfer tasks, see *Tasks* in the Data Integration Help.

Data Integration and SAP integration methods

SAP is an application platform that integrates multiple business applications and solutions, such as Customer Relationship Management (CRM), Advanced Planner and Optimizer (APO), and Bank Analyzer. Developers can add business logic within SAP using Java 2 Enterprise Edition (J2EE) or Advanced Business Application Programming-Fourth Generation (ABAP/4 or ABAP), a language proprietary to SAP.

You can use the SAP Table, BAPI/RFC functions, and IDocs integration methods to extract data from or load data to SAP systems. Use SAP Table for data-level integration, BAPI/RFC functions for object-level integration, and IDocs for message-level integration.

You can use SAP ADSO Writer Connector to load in SAP BW4 HANA. You can also use SAP ODP Extractor Connector to extract data from SAP S4 HANA, ECC, and other Operational Data Provisioning (ODP)-enabled

applications. You can perform delta extraction on any ODP source that is enabled with Operational Delta Queue (ODQ).

Data Integration using SAP tables

You can integrate SAP data dictionary objects by creating an SAP Table connection.

You can use SAP Table connection to read data from SAP and write to any target. You can also write data from any source to custom tables in SAP. Contact Informatica Global Customer Support for information about using SAP Table connection to write data to SAP systems.

You can read data from transparent tables, cluster tables, pool tables, views, and ABAP CDS views. The Secure Agent accesses data through the application layer in SAP using ABAP. Data is streamed to the Secure Agent through HTTP (s) protocol. SAP Table connector supports joins and filters on the source tables.

You can also use the SAP Table Reader connection to read data from an SAP ADSO. To write data to an ADSO, use the SAP ADSO Writer Connector.

To optimize performance when the Secure Agent and the SAP system are in different networks, you can enable data compression when you read data from SAP.

When you create a synchronization task, mapping, or mapping task, Data Integration generates a dynamic ABAP query to read from SAP tables and write to custom SAP tables.

Data Integration using BAPI/RFC functions

Business Application Programming Interfaces (BAPI) provide a way for third-party applications to synchronously integrate with SAP at the object-level. You use BAPIs to read, create, change, or delete data in SAP.

BAPIs allow access to the SAP system objects through methods for the business object types. Together with the business object types, BAPIs define and document the interface standard at the business level.

You define BAPIs in the SAP Business Objects Repository. You can call BAPIs as an ABAP program within SAP or from any external application. SAP Connector uses RFC protocol to call BAPI/RFC functions outside of SAP.

You can import a BAPI/RFC function as a mapplet to Data Integration. You can then use the mapplet in a mapping to read, create, change, or delete data in SAP. When you run the mapping or the mapping task, Data Integration makes the RFC function calls to SAP to process data synchronously.

You can view and test the BAPI interface definitions in SAP using transaction SE37.

Data Integration using IDocs

Intermediate Documents (IDocs) electronically exchange data between SAP applications or between SAP applications and external programs. IDoc is a message-based integration interface that processes data asynchronously.

IDoc is a component of Application Link Enabling (ALE) module within SAP that can send and receive Intermediate Documents (IDocs) over RFC protocol.

ALE Layers

The message-based architecture of ALE comprises three layers:

- Application layer that provides ALE an interface to SAP to send or receive messages from external systems.

- Distribution layer that filters and converts messages to ensure that they are compatible between different SAP releases.
- Communications layer that enables ALE to support synchronous and asynchronous communication. You use IDocs for asynchronous communication.

The architecture of ALE provides a way to send IDocs as text files without connecting to a central database. Applications can communicate with each other without converting between formats to accommodate hardware or platform differences.

IDoc Record Types

IDocs contain three record types:

- Control record, which identifies the message type.
- Data records that contain the IDoc data in segments.
- Status records that describe the status of the IDoc. Status record names are the same for each IDoc type.

ALE Components

ALE has the following components:

Component	Description
Logical System	All systems that need to communicate using ALE/IDoc must be setup as a Logical System within SAP. An SAP administrator can setup logical systems in transaction BD54.
Distribution Model	Defines an agreement between two logical systems on the messages that can be exchanged and identifies the sender and the receiver. An SAP administrator can setup distribution models in transaction BD64.
Partner Profile	Stores the IDoc type and processing logic related to the distribution model. An SAP administrator can setup partner profiles in transaction WE20.
RFC Destination	Defines the protocol and access to the logical system. An SAP administrator can setup RFC destinations in transaction SM59.
Message Type	Representation of a business object.
IDoc Type	Representation of a message type. SAP uses IDoc types to support backward compatibility across various SAP releases.
IDoc	An instance of an IDoc type that contains business data.

Data Integration using SAP ADSO Writer

Advanced DataStore Object (ADSO) is the central object for data storage and consolidation in the SAP BW system. ADSO is the primary data persistency object in BW/4HANA that simplifies data modeling and the support environment. ADSOs are commonly stored in 2-dimensional transparent database tables.

You can use SAP ADSO Writer Connector to load large volumes of data to the target ADSO objects in the SAP BW/4HANA application.

Data Integration using SAP ODP Extractor

Operational Data Provisioning (ODP) is an SAP NetWeaver based framework that unifies the data transfer between the source and target systems. The ODP installed as a source in the SAP system maintains the

Operational Delta Queue (ODQ) that allows delta data extraction from ODP-enabled data sources. ODP is the key infrastructure used for the data extraction from ABAP-based SAP systems to an SAP S/4HANA system.

SAP providers vary based on the source object through which you can extract data. The SAP providers define the context for the ODP extraction mechanism.

SAP ODP Extractor Connector supports the following ODP providers or contexts:

Providers/Context	Source SAP System and ODPs
SAP Service Application Programming Interface (S-API)	SAP Data Sources/Extractors without Enterprise Search (ESH)
HANA	SAP HANA Information View
BW	SAP NetWeaver Business Warehouse
ABAP_CDS	ABAP Core Data Services

ODQ is maintained for contexts SAPI and BW. You can use the SAP ODP Extractor connection to extract the historical and delta data wherever applicable through the ODP-enabled source objects.

Communication interfaces

SAP uses TCP/IP as the native communication interface to communicate with Data Integration.

SAP also uses the Remote Function Call (RFC) communication protocol to communicate with Data Integration. To execute remote calls from Data Integration, SAP requires connection information, and the service name and gateway on the application server. The service and gateway parameters, and connection information is stored in a configuration file named `sapnwrfc.ini` on the Secure Agent machine.

SAP Metadata utility

You can use the SAP Metadata utility on the Windows operating system to import metadata from IDoc messages through Data Integration mapplets.

The utility generates a mapplet XML file based on the API functionality that you specify. Import the mapplet to Data Integration and use the mapplet in a mapping.

Use the utility to import one IDoc message at a time. After you import the metadata, you can stay connected to the same SAP system destination to import more than one IDoc in the same session. To import metadata from a different destination, end the session and launch the utility again.

By default, the utility writes the XML file to the `<Utility installation directory>/generatedMappings` folder. However, you can configure the location of the output file.

Note: You do not need to configure SAP or install SAP transports to use the SAP Metadata utility.

Part II: SAP Connector Administration

This part contains the following chapter:

- [SAP Connector administration, 17](#)

CHAPTER 2

SAP Connector administration

This chapter includes the following topics:

- [SAP Connector administration overview, 17](#)
- [SAP Table Connector administration, 17](#)
- [SAP IDocs and RFCs/BAPI Connector administration, 30](#)
- [SAP BW Connector administration, 40](#)
- [SAP ODP Extractor Connector administration, 43](#)
- [SAP ADSO Writer Connector administration, 48](#)

SAP Connector administration overview

SAP Connector requires configuration on the machine that hosts the Secure Agent and also on the SAP systems. The administrators for each of these systems must perform the configuration tasks for their respective systems.

SAP Table Connector administration

Before users can use an SAP table connection to process SAP table data, an SAP Administrator must perform the following tasks:

1. Verify if the required licences are enabled.
2. Download and install the Microsoft Visual C++ redistributable.
3. Download and configure the SAP libraries for SAP Table read and write.
4. Configure the `sapnwrfc.ini` file.
5. Configure SAP user authorization.
6. Install transport files.
7. Configure HTTPS.

After the administrator has performed the configuration, users can set up and use an SAP table connection in synchronization tasks and mapping tasks.

Step 1. Verifying if the required licences are available for SAP Table Connector

You must verify if the required licences for SAP Table Connector are available before you create an SAP table connection and process SAP table data.

1. In the Data Integration home page, click the **Administrator** tab.
2. Under **Licences**, verify if the **SAP Table Connector** licence is enabled.

Step 2. Downloading and installing the Microsoft Visual C++ Redistributable

If you do not have Microsoft Visual C++ (VC++) installed, download and install the Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package on the Windows machine that hosts the Secure Agent. You can then run applications developed with VC++.

Perform the following steps to install the Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package:

1. Click the following URL:
<http://www.microsoft.com/technet/security/bulletin/MS09-035.msp>
2. Scroll down and find the **Affected Software** section.
3. Download and install the package titled **Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package (KB973544)**. Use the following URL to download the package:
<https://www.microsoft.com/en-us/download/details.aspx?id=14431>

For more information, see the following SAP Notes: 1375494 and 1025361

Step 3. Downloading and configuring the libraries for table read and write

Before you can use an SAP Table connection, download and configure the SAP libraries. Install and configure the SAP libraries on the Secure Agent machine.

The libraries that you use are based on whether you want to read from SAP tables or write to SAP tables.

Downloading and configuring libraries to read from SAP tables

To read data from SAP tables, you must download the SAP JCo libraries and configure them on the machine where the Secure Agent runs. Contact SAP Customer Support if you encounter any issues with downloading the libraries.

1. Go to the SAP Service Marketplace: <http://service.sap.com/connectors>

Note: You will need SAP credentials to access the Service Marketplace.

2. Download the 64-bit SAP JCo libraries based on the operating system on which the Secure Agent runs:

Secure Agent System	SAP File Name
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

Verify that you download the most recent version of the libraries.

3. Copy the JCo libraries to the following directory:

<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext
\deploy_to_main\bin\rdtm-extra\tpl\sap

Create the deploy_to_main\bin\rdtm-extra\tpl\sap directory if it does not already exist.

4. Configure the JAVA_LIBS property in Data Integration.

1. Log in to Data Integration.
2. Click **Runtime Environments** to access the **Runtime Environments** page.
3. To the left of the agent name, click **Edit Secure Agent**.
4. From the **Service** list, select **Data Integration Server**.
5. From the **Type** list, select **Tomcat JRE**.
6. Enter the JAVA_LIBS value based on the operating system on which the Secure Agent runs.

Operating System	Value
Windows	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar.../bin/rdtm/javaliib/sap/sap-adapter-common.jar

Note: Copy the value to a text editor and make sure that the value you copied is not corrupted. If you copy the value directly from the table, the hyphens (-) in the value are incorrectly copied.

7. Click **OK** to save the changes.
8. Repeat steps 2 through 7 on every machine where you installed the Secure Agent.
5. Restart the Secure Agent.

Downloading and configuring libraries to write to SAP tables

Download and configure the SAP NetWeaver RFC SDK 7.50 libraries. Contact SAP Customer Support if you encounter any issues with downloading the libraries.

Note: If you performed this step for an SAP IDoc or RFC/BAPI connection, you do not need to do it again.

1. Go to the SAP Service Marketplace: <http://service.sap.com>

Note: You must have SAP credentials to access the Service Marketplace.

2. Download the SAP NetWeaver RFC SDK 7.50 libraries that are specific to the operating system that hosts the Secure Agent process.

The following table lists the libraries corresponding to the different operating systems:

Operating System	SAP NetWeaver RFC SDK Libraries
Linux 64	<ul style="list-style-type: none">- libicudata.so.50- libicudecnumber.so- libicui18n.so.50- libicuuc.so.50- libsapnwrfc.so- libsapucum.so
Windows 64	<ul style="list-style-type: none">- icudt50.dll- icuin50.dll- icuuc50.dll- libicudecnumber.dll- libsapucum.dll- sapnwrfc.dll

3. Copy the SAP NetWeaver RFC SDK 7.50 libraries to the following directory:

```
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext  
\deploy_to_main\bin\rdtm
```

Create the `deploy_to_main\bin\rdtm` directory if it does not already exist.

Note: If you upgrade from a 32-bit operating system, the Secure Agent copies the 32-bit SAP NetWeaver RFC SDK 7.50 libraries to the directory. You must replace the 32-bit libraries with 64-bit libraries. If you upgrade from a 64-bit operating system, you do not need to perform this step. The Secure Agent copies the 64-bit SAP NetWeaver RFC SDK 7.50 libraries to the directory.

4. Set the following permissions for each NetWeaver RFC SDK library:
 - Read, write, and execute permissions for the current user.
 - Read and execute permissions for all other users.
5. Download the 64-bit SAP JCo libraries based on the operating system on which the Secure Agent runs:

Secure Agent System	SAP File Name
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

Verify that you download the most recent version of the libraries.

6. Copy the JCo libraries to the following directory:

```
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext  
\deploy_to_main\bin\rdtm-extra\tpl\sap
```

Create the `deploy_to_main\bin\rdtm-extra\tpl\sap` directory if it does not already exist.

Note: If you upgrade from a 32-bit operating system, the Secure Agent copies the 32-bit SAP JCo libraries to the directory. You must replace the 32-bit JCo libraries with 64-bit JCo libraries. If you upgrade from a 64-bit operating system, you do not need to perform this step. The Secure Agent copies the 64-bit SAP JCo libraries to the directory.

7. Configure the JAVA_LIBS property in Data Integration.
 1. Log in to Data Integration.
 2. Click **Runtime Environments** to access the **Runtime Environments** page.
 3. To the left of the agent name, click **Edit Secure Agent**.
 4. From the **Service** list, select **Data Integration Server**.
 5. From the **Type** list, select **Tomcat JRE**.
 6. Enter the JAVA_LIBS value based on the operating system on which the Secure Agent runs.

Operating System	Value
Windows	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar../bin/rdtm/javaliib/sap/sap-adapter-common.jar

Note: Copy the value to a text editor and make sure that the value you copied is not corrupted. If you copy the value directly from the table, the hyphens (-) in the value are incorrectly copied.

7. Click **OK** to save the changes.
 8. Repeat steps 2 through 7 on every machine where you installed the Secure Agent.
8. Restart the Secure Agent.

Step 4. Configuring sapnwrfc.ini

SAP uses the communications protocol, Remote Function Call (RFC), to communicate with other systems. SAP stores RFC-specific parameters and connection information in a file named `sapnwrfc.ini`. To enable the Secure Agent to connect to the SAP system as an RFC client, create and configure the `sapnwrfc.ini` file on the machines that host the Secure Agent.

When you read data from SAP tables, if you define the path and file name of the `sapnwrfc.ini` file in the SAP connection, the Secure Agent uses the `sapnwrfc.ini` file. However, if you define only the path of the `sapnwrfc.ini` file in the connection, the Secure Agent first verifies if an `sapnwrfc.ini` file exists in the specified path. If the `sapnwrfc.ini` file exists, the Secure Agent uses the `sapnwrfc.ini` file. Else, an exception occurs.

To process data through RFC/BAPIs, read IDocs, write IDocs, and write data to SAP tables, you cannot use the `sapnwrfc.ini` file.

Use a DOS editor or WordPad to configure the `sapnwrfc.ini` file. Notepad can introduce errors to the `sapnwrfc.ini` file.

After you create the `sapnwrfc.ini` file, copy the file to the following directory and restart the Secure Agent:

```
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext  
\deploy_to_main\bin\rdtm\
```

Create the `deploy_to_main\bin\rdtm` directory if it does not already exist.

Note: If you are upgrading from an earlier version, you do not need to perform this step. The Secure Agent copies the `sapnwrfc.ini` file to the directory.

Configure the connection entries in the `sapnwrfc.ini` file

Use the `sapnwrfc.ini` file to configure the connections that you want to use.

You can configure the following types of connections in the `sapnwrfc.ini` file:

Connection to a specific SAP application server

Create this connection to enable communication between an RFC client and an SAP system. Each connection entry specifies one application server and one SAP system.

The following sample shows a connection entry for a specific SAP application server in the `sapnwrfc.ini` file:

```
DEST=sapr3
ASHOST=sapr3
SYSNR=00
```

Connection to use SAP load balancing

Create this connection to enable SAP to create an RFC connection to the application server with the least load at run time. Use this connection when you want to use SAP load balancing.

The following sample shows a connection entry for SAP load balancing in the `sapnwrfc.ini` file:

```
DEST=sapr3
R3NAME=ABV
MSHOST=infamessageserver.informatica.com
GROUP=INFADDEV
```

Connection to an RFC server program registered at an SAP gateway

Create this connection to connect to an SAP system from which you want to receive outbound IDocs.

The following sample shows a connection entry for an RFC server program registered at an SAP gateway in the `sapnwrfc.ini` file:

```
DEST=sapr346CLSQA
PROGRAM_ID=PID_LSRECEIVE
GWHOST=sapr346c
GWSERV=sapgw00
```

sapnwrfc.ini parameters

The following table describes the parameters that you can define for various connection types in the `sapnwrfc.ini` file.

sapnwrfc.ini Parameter	Description	Applicable Connection Types
DEST	Logical name of the SAP system for the connection. All DEST entries must be unique. You must have only one DEST entry for each SAP system. For SAP versions 4.6C and later, use up to 32 characters. For earlier versions, use up to eight characters.	Use this parameter for the following types of connections: <ul style="list-style-type: none">- Connection to a specific SAP application server- Connection to use load balancing- Connection to an RFC server program registered at an SAP gateway
ASHOST	Host name or IP address of the SAP application. The Secure Agent uses this entry to attach to the application server.	Use this parameter to create a connection to a specific SAP application server.
SYSNR	SAP system number.	Use this parameter to create a connection to a specific SAP application server.
R3NAME	Name of the SAP system.	Use this parameter to create a connection to use SAP load balancing.
MSHOST	Host name of the SAP message server.	Use this parameter to create a connection to use SAP load balancing.
GROUP	Group name of the SAP application server.	Use this parameter to create a connection to use SAP load balancing.
PROGRAM_ID	Program ID. The Program ID must be the same as the Program ID for the logical system that you define in the SAP system to send or receive IDocs.	Use this parameter to create a connection to an RFC server program registered at an SAP gateway.
GWHOST	Host name of the SAP gateway.	Use this parameter to create a connection to an RFC server program registered at an SAP gateway.
GWSERV	Server name of the SAP gateway.	Use this parameter to create a connection to an RFC server program registered at an SAP gateway.
TRACE	Debugs RFC connection-related problems. Set one of the following values based on the level of detail that you want in the trace: <ul style="list-style-type: none">- 0. Off- 1. Brief- 2. Verbose- 3. Full	Use this parameter for the following types of connections: <ul style="list-style-type: none">- Connection to a specific SAP application server- Connection to use load balancing- Connection to an RFC server program registered at an SAP gateway

Sample sapnwrfc.ini file

The following snippet shows a sample `sapnwrfc.ini` file:

```
/*=====*/  
/* Connection to an RFC server program registered at an SAP gateway */  
/*=====*/
```

```

DEST=<destination in RfcRegisterServer>
PROGRAM_ID=<program-ID, optional; default: destination>
GWHOST=<host name of the SAP gateway>
GWSERV=<service name of the SAP gateway>
*=====*/
/* Connection to a specific SAP application server */
/*=====*/
DEST=<destination in RfcOpenConnection>
ASHOST=<Host name of the application server.>
SYSNR=<The back-end system number.>
*=====*/
/* Connection to use SAP load balancing */
/* The application server will be determined at run time. */
/*=====*/
DEST=<destination in RfcOpenConnection>
R3NAME=<name of SAP system, optional; default: destination>
MSHOST=<host name of the message server>
GROUP=<group name of the application servers, optional; default: PUBLIC>

```

Step 5. Configuring SAP user authorization

Configure the SAP user account to process SAP table data.

The following table describes the required authorization to read from SAP tables:

Read Object Name	Required Authorization
S_BTCH_JOB	DELE, LIST, PLAN, SHOW. Set Job Operation to RELE.
S_PROGRAM	BTCSUBMIT, SUBMIT
S_RFC	SYST, SDTX, SDIFRUNTIME, /INFADI/TBLRDR
S_TABU_DIS	&_SAP_ALL

The following table describes the required authorization to write to SAP tables:

Write Object Name	Required Authorization
S_RFC	/INFATRAN/ZPMW
S_TABU_DIS	&_SAP_ALL

Step 6. Installing SAP Table connection transport files

Install the SAP Table connection transport files on the SAP machines that you want to access. Before you install the transports on your production system, install and test the transports in a development system.

Install the transports on the SAP development system in the same order as listed in the table.

Data and Cofile Names	Required/Optional	Transport Request	Functionality
- TABLE_READER_R900090.EP6 - TABLE_READER_K900090.EP6	Required	- EP6900090	Install the TABLE_READER transports to read from SAP transparent tables, cluster tables, pool tables, and views.
- TABLE_READER_Addon_R900027.D75 - TABLE_READER_Addon_K900027.D75	Optional	- D75900027	Install the TABLE_READER_Addon transports only if you want to read data from ABAP CDS views.

Before you install the TABLE_READER_Addon transports, complete the following prerequisite tasks:

- Install the TABLE_READER transports and only then install the TABLE_READER_Addon transports.
- Use the TABLE_READER_Addon transports for SAP NetWeaver 7.50 SP4 version and later.
- Verify that the RSODPABAPCDSVIEW table is available in SAP before you install the TABLE_READER_Addon transport files. If the RSODPABAPCDSVIEW table is not available, the TABLE_READER_Addon transport installation fails.

Installing transport files

Install transport files from a Secure Agent directory to read from a Unicode SAP system. The transport files are for SAP version ECC 5.0 or later. To install transport files to write to an SAP system, contact Informatica Global Customer Support.

1. Find the transport files in the following directory on the Secure Agent machine:

```
<Informatica Secure Agent installation directory>\downloads\package-SAPConnector.  
32\package\rdtm\sap-transport\SAPTableReader
```

2. Copy the cofile transport file to the **Cofile** directory in the SAP transport management directory on each SAP machine that you want to access.

The cofile transport file uses the following naming convention: `TABLE_READER_K<number>.EP6`.

3. Remove "TABLE_READER_" from the file name to rename the cofile.

For example, for a cofile transport file named `TABLE_READER_K900090.EP6`, rename the file to `K900090.EP6`.

4. Copy the data transport file to the **Data** directory in the SAP transport management directory on each SAP machine that you want to access.

The data transport file uses the following naming convention: `TABLE_READER_K<number>.EP6`.

5. Remove "TABLE_READER_" from the file name to rename the file.

6. To import the transports to SAP, in the STMS, click **Extras > Other Requests > Add** and add the transport request to the system queue.

7. In the **Add Transport Request to Import Queue** dialog box, enter the request number for the cofile transport.
The request number inverts the order of the renamed cofile as follows: EP6K<number>.
For example, for a cofile transport file renamed as K900090.EP6, enter the request number as EP6900090.
8. In the Request area of the import queue, select the transport request number that you added, and click **Import**.
9. If you are upgrading from a previous version of the Informatica Transports, select the **Overwrite Originals** option.

Step 7: Configuring HTTPS

To connect to SAP through HTTPS and read SAP table sources, you must configure the machine that hosts the Secure Agent and the machine that hosts the SAP system. You must also enable HTTPS when you configure an SAP Table connection in Data Integration.

Perform the following configuration tasks on the Secure agent and SAP systems:

HTTPS Configuration on the Secure Agent System

To configure HTTPS on the machine that hosts the Secure Agent, perform the following tasks:

1. Create a certificate using OpenSSL and JAVA KeyTool.
2. Convert the OpenSSL certificate (PKCS#12 certificate) to SAP specific format (PSE) using the SAPGENPSE tool.

Currently, self-signed certificates are supported

HTTPS Configuration on the SAP System

To configure HTTPS on the machine that hosts the SAP system, perform the following tasks:

1. Enable the HTTPS service on the SAP system.
2. Import the certificate in PSE format to the SAP system trust store.

Prerequisites

Before you create an OpenSSL certificate, verify the following prerequisites:

- Download and install OpenSSL on the Secure Agent machine.
- Based on the operating system of the machine that hosts the Secure Agent and the SAP system, download the latest available patch of the SAPGENPSE Cryptography tool from the SAP Service Marketplace.
Typically, the SAPGENPSE files are extracted to the `nt-x86_64` directory.
- Configure the following SAP parameters: `icm/server_port`, `ssl/ssl_lib`, `sec/libsapsecu`, `ssf/ssfapi_lib`, `ssf/name`, `icm/HTTPS/verify_client`, `ssl/client_pse`, and `wdisp/ssl_encrypt`. For more information, see the SAP documentation.

Create an OpenSSL certificate

Create a self-signed certificate using OpenSSL.

1. At the command prompt, set the `OPENSSL_CONF` variable to the absolute path to the `openssl.cfg` file. For example, enter the following command: `set OPENSSL_CONF= C:\OpenSSL-Win64\bin\openssl.cfg`

2. Navigate the `<openssl installation directory>\bin` directory.
3. To generate a 2048-bit RSA private key, enter the following command: `openssl.exe req -new -newkey rsa:2048 -sha1 -keyout <RSAkey File_Name>.key -out <RSAkey File_Name>.csr`.
4. When prompted, enter the following values:
 - Private key password (PEM pass phrase). Enter a phrase that you want to use to encrypt the secret key. Re-enter the password for verification.
Important: Make a note of this PEM password. You need to specify this value in some of the following steps.
 - Two letter code for country name.
 - State or province name.
 - Locality name.
 - Organization name
 - Organization unit name.
 - Common name (CN). Mandatory.
Important: Enter the fully qualified host name of the machine that hosts the Secure Agent.
 - Email address.
5. Enter the following extra attributes you want to send along with the certificate request:
 - Challenge password.
 - Optional company name.

A RSA private key of 2048-bit size is created. The `<RSAkey File_Name>.key` and `<RSAkey File_Name>.csr` files are generated in the current location.
6. To generate a self-signed key using the RSA private key, enter the following command: `openssl x509 -req -days 11499 -in <RSAkey File_Name>.csr -signkey <RSAkey File_Name>.key -out <Certificate File_Name>.crt`
7. When prompted, enter the PEM pass phrase for the RSA private key.
 The `<Certificate File_Name>.crt` file is generated in the current location.
8. Concatenate the contents of the `<Certificate File_Name>.crt` file and the `<RSAkey File_Name>.key` file to a `.pem` file.
 - a. Open the `<Certificate File_Name>.crt` file and the `<RSAkey File_Name>.key` files in a Text editor.
 - b. Create a file and save it as `<PEM File_Name>.pem`.
 - c. Copy the contents of the `<Certificate File_Name>.crt` file and paste it in the `.pem` file.
 - d. Copy the contents of the `<RSAkey File_Name>.key` file and append it to the existing contents of the `.pem` file.
 - e. Save the `<PEM file name>.pem` file.
9. To create a PKCS#12 certificate, enter the following command at the command prompt: `openssl pkcs12 -export -in <PEM File_Name>.pem -out <P12 File_Name>.p12 -name "domain name"`.
10. When prompted, enter the following details:
 - The PEM pass phrase for the `.pem` file.
 - An export password for the P12 file. Re-enter the password for verification.
Important: Make a note of this export password for the P12 file. You need to specify this value in some of the following steps and while creating the SAP Table connection in Data Integration.

The <P12 File_Name>.p12 file is generated in the current location.

11. To create a Java keystore file, enter the following command: `keytool -v -importkeystore -srckeystore <P12 File_Name>.p12 -srcstoretype PKCS12 -destkeystore <JKS File_Name>.jks -deststoretype JKS -srcalias "source alias" -destalias "destination alias"`.

12. When prompted, enter the following details:

- Password for the destination keystore, the JKS file.

Important: Make a note of this password. You need to specify this password while creating the SAP Table connection in Data Integration.

- Password for the source keystore, the P12 file. Enter the Export password for the P12 file.

The <JKS File_Name>.jks file is generated in the current location.

Important: While enabling HTTPS in an SAP Table connection, you must specify the name and location of this keystore file. You must also specify the destination keystore password as the Keystore Password and the source keystore password as the Private Key Password.

Convert an OpenSSL certificate to PSE format

You can convert an OpenSSL certificate to PSE format using the SAPGENPSE tool.

1. At the command prompt, navigate to the <SAPGENPSE Extraction Directory>.
2. To generate a PSE file, enter the following command: `sapgenpse import_p12 -p <PSE_Directory> \<PSE File_Name>.pse <P12 Certificate_Directory>\<P12 File_Name>.p12`

3. When prompted, enter the following details:

- Password for the P12 file. Enter the Export password for the P12 file.
- Personal identification number (PIN) to protect the PSE file. Re-enter the PIN for verification.

The <PSE File_Name>.pse file is generated in the specified directory.

4. To generate the certificate based on the PSE format, enter the following command: `sapgenpse export_own_cert -p <PSE File_Directory>\<PSE File_Name>.pse -o <Certificate_Name>.cert`

5. When prompted, enter the PSE PIN number.

The <Certificate_Name>.cert file is generated in the current location. Import this certificate file to the SAP system trust store.

Enable the HTTPS service on SAP system

Enable the HTTPS service from the SMICM transaction.

Import a certificate to SAP system trust store

1. Login to SAP and go to the STRUST transaction.
2. Select SSL Client (Standard) and specify the password. In the **Import Certificate** dialog, you may need to select Base64 format as the certificate file format.
3. Click the **Import** icon and select the <Certificate_Name>.cert file in PSE format.

Note: You may need to add a DNS entry of the agent host on the SAP app server if a user is on a different network.

4. Click **Add to Certificate List**.
5. Restart the ICM.

Step 8: Configuring the Secure Agent as a whitelisted host in SAP (optional)

When you read SAP table data, you can configure the Secure Agent as a whitelisted host in the SAP system.

Perform the following steps to configure the Secure Agent as a whitelisted host in SAP:

1. Install the `TABLE_READER_R900544.EC5` and `TABLE_READER_K900544.EC5` transport files. For more information about installing the SAP Table Connector transport files, see [“Installing transport files” on page 25](#).
2. In Data Integration, configure the **JVMOption** property for the Secure Agent that you want to define as a whitelisted host in SAP. Set the value of the property to **-Dsap_whitelist_check=1** if you want SAP to validate the Secure Agent. You can specify the value in any **JVMOption** field.
3. In SAP, use transaction SE16 to create an entry for the Secure Agent in the SAP HTTP_Whitelist table. SAP stores whitelist information in the HTTP_Whitelist table.

If you set the value of the **JVMOption** property to **-Dsap_whitelist_check=1**, when the Secure Agent runs a task or mapping to read SAP table data, SAP validates that a corresponding entry exists for the Secure Agent in the SAP HTTP_Whitelist table. If the entry exists, the task or mapping runs successfully. Otherwise, the task or mapping fails.

Configuring the JVMOption property in Data Integration

Configure the **JVMOption** property in Data Integration to define the Secure Agent as a whitelisted host in the SAP system. You can specify the value in any **JVMOption** field.

1. Log in to Data Integration.
2. Click **Runtime Environments** to access the **Runtime Environments** page.
3. To the left of the agent name, click **Edit Secure Agent**.
4. In the **System Configuration Details** section, from the **Service** list, select **Data Integration Server**.
5. Edit any **JVMOption** field to add the following value: **-Dsap_whitelist_check=1**
6. Repeat steps 2 through 5 for every Secure Agent that you want to define as a whitelisted host in SAP.

Creating an entry for the Secure Agent in the SAP HTTP_Whitelist table

SAP stores whitelist information in the HTTP_Whitelist table. Use transaction SE16 to create an entry for the Secure Agent in the SAP HTTP_Whitelist table and configure the Secure Agent as a whitelisted host in the SAP system.

1. Go to transaction SE16.
2. Configure properties to define the Secure Agent as a whitelisted host in SAP.

The following table describes the properties that you must configure:

Property	Description
MANDT	Required. SAP client number.
ENTRY TYPE	Required. URL type to be compared with this entry. Enter 01 to indicate that the URL is a CSS theme URL.

Property	Description
SORT KEY	Required. Unique value to be used as the primary key. You can enter numbers and alphabets.
PROTOCOL	Protocol that SAP must validate. Enter HTTP or HTTPS . If you do not enter a value, SAP does not validate the protocol.
HOST	Host machine that SAP must validate. Enter the IP address of the machine that hosts the Secure Agent.
PORT	Port number that SAP must validate. Leave the Port field blank to indicate that SAP does not need to validate the port.
URL	URL that SAP must validate. Enter * to indicate that SAP does not need to validate the URL.

3. Repeat steps 1 and 2 for every Secure Agent that you want to configure as a whitelisted host in SAP.

SAP IDocs and RFCs/BAPI Connector administration

Before you can use an SAP connection to process data through IDocs or RFCs/BAPIs, an SAP administrator must perform the following tasks:

1. Verify if the required licences are enabled.
2. Download and install the Microsoft Visual C++ Redistributable.
3. Download and configure the SAP libraries.
4. Configure the `sapnwrfc.ini` file.
5. Define SAP Connector as an external logical system in SAP.
6. Configure SAP user authorization.
7. To process data through IDocs, install and configure the SAP Metadata utility.

After the administrator has performed the configuration, you can create and use SAP RFC/BAPI, IDoc Reader, and IDoc Writer connections in mappings.

Step 1. Verifying if the required licences are available for SAP IDocs and RFCs/BAPI Connector

You must verify if the required licences for SAP IDocs and RFCs/BAPI Connector are available before you create an SAP connection and process data through IDocs or RFCs/BAPIs.

1. In the Data Integration home page, click the **Administrator** tab.
2. Under **Licences**, verify if the **SAP Table Connector** licence is enabled.

Step 2. Downloading and installing the Microsoft Visual C++ Redistributable

If you do not have Microsoft Visual C++ (VC++) installed, download and install the Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package on the Windows machine that hosts the Secure Agent. You can then run applications developed with VC++.

Perform the following steps to install the Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package:

1. Click the following URL:
<http://www.microsoft.com/technet/security/bulletin/MS09-035.msp>
2. Scroll down and find the **Affected Software** section.
3. Download and install the package titled **Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package (KB973544)**. Use the following URL to download the package:

<https://www.microsoft.com/en-us/download/details.aspx?id=14431>

For more information, see the following SAP Notes: 1375494 and 1025361

Step 3. Downloading and configuring SAP libraries for IDoc and BAPI/RFC

Download and configure the SAP NetWeaver RFC SDK libraries. Contact SAP Customer Support if you encounter any issues when you download the libraries.

Note: If you performed this step for an SAP table connection, you do not need to do it again.

1. Go to the SAP Service Marketplace: <http://service.sap.com>

Note: You must have SAP credentials to access the Service Marketplace.

2. Download the SAP NetWeaver RFC SDK 7.50 libraries that are specific to the operating system that hosts the Secure Agent process.

The following table lists the libraries corresponding to the different operating systems:

Operating System	SAP NetWeaver RFC SDK Libraries
Linux 64	<ul style="list-style-type: none">- libicudata.so.50- libcudecnumber.so- libcui18n.so.50- libicuuc.so.50- libsapnwrfc.so- libsapucum.so
Windows 64	<ul style="list-style-type: none">- icudt50.dll- icuin50.dll- icuuc50.dll- libcudecnumber.dll- libsapucum.dll- sapnwrfc.dll

3. Copy the SAP NetWeaver RFC SDK 7.50 libraries to the following directory:

<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext
\deploy_to_main\bin\rdtm\

Create the `deploy_to_main\bin\rdtm` directory if it does not already exist.

Note: If you upgrade from a 32-bit operating system, the Secure Agent copies the 32-bit SAP NetWeaver RFC SDK 7.50 libraries to the directory. You must replace the 32-bit libraries with 64-bit libraries. If you upgrade from a 64-bit operating system, you do not need to perform this step. The Secure Agent copies the 64-bit SAP NetWeaver RFC SDK 7.50 libraries to the directory.

4. Set the following permissions for each NetWeaver RFC SDK library:
 - Read, write, and execute permissions for the current user.
 - Read and execute permissions for all other users.
5. Download the 64-bit SAP JCo libraries based on the operating system on which the Secure Agent runs:

Secure Agent System	SAP File Name
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

Verify that you download the most recent version of the libraries.

6. Copy the JCo libraries to the following directory:

```
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext
\deploy_to_main\bin\rdtm-extra\tpl\sap
```

Create the `deploy_to_main\bin\rdtm-extra\tpl\sap` directory if it does not already exist.

Note: If you upgrade from a 32-bit operating system, the Secure Agent copies the 32-bit SAP JCo libraries to the directory. You must replace the 32-bit JCo libraries with 64-bit JCo libraries. If you upgrade from a 64-bit operating system, you do not need to perform this step. The Secure Agent copies the 64-bit SAP JCo libraries to the directory.

7. Configure the JAVA_LIBS property in Data Integration.
 1. Log in to Data Integration.
 2. Click **Runtime Environments** to access the **Runtime Environments** page.
 3. To the left of the agent name, click **Edit Secure Agent**.
 4. From the **Service** list, select **Data Integration Server**.
 5. From the **Type** list, select **Tomcat JRE**.
 6. Enter the JAVA_LIBS value based on the operating system on which the Secure Agent runs.

Operating System	Value
Windows	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar

Note: Copy the value to a text editor and make sure that the value you copied is not corrupted. If you copy the value directly from the table, the hyphens (-) in the value are incorrectly copied.

7. Click **OK** to save the changes.

8. Repeat steps 2 through 7 on every machine where you installed the Secure Agent.
8. Restart the Secure Agent.

Step 4. Configuring sapnwrfc.ini

SAP uses the communications protocol, Remote Function Call (RFC), to communicate with other systems. SAP stores RFC-specific parameters and connection information in a file named `sapnwrfc.ini`. To enable the Secure Agent to connect to the SAP system as an RFC client, create and configure the `sapnwrfc.ini` file on the machines that host the Secure Agent.

When you read data from SAP tables, if you define the path and file name of the `sapnwrfc.ini` file in the SAP connection, the Secure Agent uses the `sapnwrfc.ini` file. However, if you define only the path of the `sapnwrfc.ini` file in the connection, the Secure Agent first verifies if an `sapnwrfc.ini` file exists in the specified path. If the `sapnwrfc.ini` file exists, the Secure Agent uses the `sapnwrfc.ini` file. Else, an exception occurs.

To process data through RFC/BAPIs, read IDocs, write IDocs, and write data to SAP tables, you cannot use the `sapnwrfc.ini` file.

Use a DOS editor or WordPad to configure the `sapnwrfc.ini` file. Notepad can introduce errors to the `sapnwrfc.ini` file.

After you create the `sapnwrfc.ini` file, copy the file to the following directory and restart the Secure Agent:

```
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext  
\deploy_to_main\bin\rdtm\
```

Create the `deploy_to_main\bin\rdtm` directory if it does not already exist.

Note: If you are upgrading from an earlier version, you do not need to perform this step. The Secure Agent copies the `sapnwrfc.ini` file to the directory.

Configure the connection entries in the sapnwrfc.ini file

Use the `sapnwrfc.ini` file to configure the connections that you want to use.

You can configure the following types of connections in the `sapnwrfc.ini` file:

Connection to a specific SAP application server

Create this connection to enable communication between an RFC client and an SAP system. Each connection entry specifies one application server and one SAP system.

The following sample shows a connection entry for a specific SAP application server in the `sapnwrfc.ini` file:

```
DEST=sapr3  
ASHOST=sapr3  
SYSNR=00
```

Connection to use SAP load balancing

Create this connection to enable SAP to create an RFC connection to the application server with the least load at run time. Use this connection when you want to use SAP load balancing.

The following sample shows a connection entry for SAP load balancing in the `sapnwrfc.ini` file:

```
DEST=sapr3  
R3NAME=ABV  
MSHOST=infamessageserver.informatica.com  
GROUP=INFADDEV
```

Connection to an RFC server program registered at an SAP gateway

Create this connection to connect to an SAP system from which you want to receive outbound IDocs.

The following sample shows a connection entry for an RFC server program registered at an SAP gateway in the `sapnwrfc.ini` file:

```
DEST=sapr346CLSQA
PROGRAM_ID=PID_LSRECEIVE
GWHOST=sapr346c
GWSErv=sapgw00
```

sapnwrfc.ini parameters

The following table describes the parameters that you can define for various connection types in the `sapnwrfc.ini` file.

sapnwrfc.ini Parameter	Description	Applicable Connection Types
DEST	Logical name of the SAP system for the connection. All DEST entries must be unique. You must have only one DEST entry for each SAP system. For SAP versions 4.6C and later, use up to 32 characters. For earlier versions, use up to eight characters.	Use this parameter for the following types of connections: <ul style="list-style-type: none">- Connection to a specific SAP application server- Connection to use load balancing- Connection to an RFC server program registered at an SAP gateway
ASHOST	Host name or IP address of the SAP application. The Secure Agent uses this entry to attach to the application server.	Use this parameter to create a connection to a specific SAP application server.
SYSNR	SAP system number.	Use this parameter to create a connection to a specific SAP application server.
R3NAME	Name of the SAP system.	Use this parameter to create a connection to use SAP load balancing.
MSHOST	Host name of the SAP message server.	Use this parameter to create a connection to use SAP load balancing.
GROUP	Group name of the SAP application server.	Use this parameter to create a connection to use SAP load balancing.
PROGRAM_ID	Program ID. The Program ID must be the same as the Program ID for the logical system that you define in the SAP system to send or receive IDocs.	Use this parameter to create a connection to an RFC server program registered at an SAP gateway.
GWHOST	Host name of the SAP gateway.	Use this parameter to create a connection to an RFC server program registered at an SAP gateway.

sapnwrfc.ini Parameter	Description	Applicable Connection Types
GWSESV	Server name of the SAP gateway.	Use this parameter to create a connection to an RFC server program registered at an SAP gateway.
TRACE	Debugs RFC connection-related problems. Set one of the following values based on the level of detail that you want in the trace: <ul style="list-style-type: none"> - 0. Off - 1. Brief - 2. Verbose - 3. Full 	Use this parameter for the following types of connections: <ul style="list-style-type: none"> - Connection to a specific SAP application server - Connection to use load balancing - Connection to an RFC server program registered at an SAP gateway

Sample sapnwrfc.ini file

The following snippet shows a sample sapnwrfc.ini file:

```

/*=====*/
/* Connection to an RFC server program registered at an SAP gateway */
/*=====*/
DEST=<destination in RfcRegisterServer>
PROGRAM_ID=<program-ID, optional; default: destination>
GWHOST=<host name of the SAP gateway>
GWSESV=<service name of the SAP gateway>
/*=====*/
/* Connection to a specific SAP application server */
/*=====*/
DEST=<destination in RfcOpenConnection>
ASHOST=<Host name of the application server.>
SYSNR=<The back-end system number.>
/*=====*/
/* Connection to use SAP load balancing */
/* The application server will be determined at run time. */
/*=====*/
DEST=<destination in RfcOpenConnection>
R3NAME=<name of SAP system, optional; default: destination>
MSHOST=<host name of the message server>
GROUP=<group name of the application servers, optional; default: PUBLIC>

```

Step 5. Defining SAP Connector as a logical system in SAP

To use SAP Connector to send and receive IDocs from SAP, you must define SAP Connector as an external logical system in SAP.

Create a single logical system in SAP for IDoc ALE integration with SAP Connector. When you define SAP Connector as a logical system, SAP acknowledges SAP Connector as an external system that can receive outbound IDocs from SAP and send inbound IDocs to SAP.

Perform the following steps to define SAP Connector as a logical system:

1. Create a logical system in SAP for SAP Connector.
2. Create an RFC destination for SAP Connector.
3. Create a tRFC port for the RFC destination.
4. Create a partner profile for SAP Connector.
5. Create outbound and inbound parameters for the partner profile.

Note: These steps are based on SAP version 4.6C. The steps may differ if you use a different version. For complete instructions on creating a logical system in SAP, see the SAP documentation.

Step 1. Create a logical system for SAP Connector

To uniquely identify SAP Connector as a client within a network, define SAP Connector as an external logical system in SAP.

1. Go to transaction SALE.
The **Display IMG** window appears.
2. Expand the tree to navigate to the **Application Link Enabling > Sending and Receiving Systems > Logical Systems > Define Logical System** operation.
3. Click the **IMG - Activity** icon to run the Define Logical System operation.
An informational dialog box appears.
4. Click **Enter**.
The **Change View Logical Systems** window appears.
5. Click **New Entries**.
The **New Entries** window appears.
6. Enter a name and description for the logical system entry for SAP Connector.

Step 2. Create an RFC destination

Create an RFC destination and program ID for SAP Connector.

1. Go to transaction SM59.
The **Display and Maintain RFC Destinations** window appears.
2. Click **Create**.
The **RFC Destination** window appears.
3. Enter the name of the logical system you created as the RFC destination.
4. To create a TCP/IP connection, enter T as the connection type.
5. Enter a description for the RFC destination.
6. Click **Save**.
7. For Activation Type, click **Registration**.
8. For Program ID, enter the same name as the RFC destination name.
Use the Program ID as the value for the PROGRAM_ID parameter in the `sapnwrfc.ini` file.

Step 3. Create a tRFC port for the RFC destination

Create a tRFC port for the RFC destination you defined in SAP. SAP uses the tRFC port to communicate with SAP Connector.

1. Go to transaction WE21.
2. Click **Ports > Transactional RFC**.
3. Click **Create**.
The **Ports in IDoc Processing** dialog box appears.
4. Click **Generate Port Name** or **Own Port Name** and enter a name.
5. Click **Enter**.
6. Enter a description for the port.

7. Select the IDoc record version type.
8. Enter the name of the RFC destination you created.

Step 4. Create a partner profile for SAP Connector

Create a partner profile for the logical system you defined for SAP Connector. When SAP communicates with an external system, it uses the partner profile to identify the external system.

1. Go to transaction WE20.
2. Click **Create**.
3. Enter the following properties:

Partner Profile Property	Description
Partner number	Name of the logical system you created for SAP Connector.
Partner type	Partner profile type. Enter LS for logical system for ALE distribution systems.

4. In the **Post-processing** tab, enter the following properties:

Partner Profile Property	Description
Type	User type. Enter US for user.
Agent	The SAP user login name.
Lang	Language code that corresponds to the SAP language. Enter EN for English.

5. In the **Classification** tab, enter the following properties:

Partner Profile Property	Description
Partner class	Enter ALE.
Partner status	Indicates the status of communication with the partner. To communicate with the partner, enter A for active.

Step 5. Create outbound and inbound parameters for the partner profile

Outbound parameters define the IDoc message type, IDoc basic type, and port number for outbound IDocs. Inbound parameters define the IDoc message type for inbound IDocs.

SAP uses outbound parameters when it sends IDocs to SAP Connector. Create an outbound parameter for each IDoc message type that SAP sends to SAP Connector. SAP uses inbound parameters when it receives IDocs from SAP Connector. Create an inbound parameter for each IDoc message type that SAP receives from SAP Connector.

1. From the partner profiles window, click **Create Outbound Parameter**.

The **Partner Profiles: Outbound Parameters** window appears.

2. Enter the following properties:

Outbound Parameter Property	Description
Message Type	The IDoc message type the SAP system sends to SAP Connector.
Receiver Port	The tRFC port number you defined.
IDoc Type	The IDoc basic type of the IDocs the SAP system sends to SAP Connector.

3. Click **Save**.
The **Packet Size** property appears.
4. Enter a value between 10 and 200 IDocs as the packet size.
The packet size determines the number of IDocs that SAP sends in one packet to SAP Connector.
5. Click **Enter**.
6. Repeat steps from 1 to 5 to create an outbound parameter for each IDoc message type that SAP sends to SAP Connector.
7. Click **Create Inbound Parameter**.
The **Partner Profiles: Inbound Parameters** window appears.
8. For each inbound parameter, enter the following properties:

Inbound Parameter Property	Description
Message Type	The IDoc message type the SAP system receives from SAP Connector.
Process Code	The process code. The SAP system uses the process code to call the appropriate function module to process the IDocs it receives.

9. Click **Enter**.
10. Repeat steps 7 through 9 to create an inbound parameter for each IDoc message type that SAP receives from SAP Connector.

Step 6. Configuring SAP user authorizations

An SAP administrator needs to create a profile in the development, test, and production SAP system so that you can use the integration features. This profile name must include authorization for the objects and related activities. The profile on the test system should be the same as the profile on the production system.

The setup of the user and profiles is done within SAP using the SAP GUI. This activity is external to Data Integration.

BAPI/RFC

The following table describes the authorization an SAP user requires to execute tasks using the BAPI/RFC functions:

Authorization Object	Authorization Value
S_RFC	SYST, SDTX, SDIFRUNTIME, RFC1, RFC2

Note: In addition to the above authorization, the user needs access to any BAPI/RFC function that needs to be executed.

IDoc

The following table describes the authorization an SAP user requires to execute tasks with IDoc messages:

Authorization Object	Authorization Value
S_RFC	SYST, SDTX, SDIFRUNTIME, RFC1, RFC2, EDIMEXT

Note: In addition to the above authorization, the user needs access to specific IDoc and underlying transactions that needs to be executed.

Step 7. Installing and configuring the SAP IDocs Metadata utility

To import IDoc metadata from SAP systems and generate mapplets, you need to install and configure the SAP Metadata utility.

Prerequisites

Before you use the SAP Metadata utility to process data through IDocs, verify the following prerequisites:

- Configure the sapnwrfc.ini file to include information about the SAP server with the metadata you want to extract.
- Configure the RFC_INI system environment variable for the path to the sapnwrfc.ini file.
- Download and install the 32-bit SAP JCo libraries for your operating system. You can find the libraries on the SAP Service Marketplace: <http://service.sap.com>. Verify that you have downloaded the most recent version of the libraries. Unzip the contents to a local directory.
- Add the location of the SAP JCo libraries to the PATH system environment variable.
- Verify that an SAP user has the authorization to browse and extract metadata.

Installation and configuration

Install and configure the SAP Metadata utility to process data through IDocs on the machine that hosts the Secure Agent.

1. Download the SAP Metadata utility zip file, SapUtility.zip from the [Informatica Cloud Community](#).
2. Unzip the file to a local directory.

Avoid using spaces in the directory name because spaces can cause imports to fail.

3. Edit the <SAP Metadata utility download directory>/SAPUtil.bat file to define the CLASSPATH and JAVA_HOME variables.
 - a. Enter the SAP JCo libraries directory and the sapjco3.jar file name in the CLASSPATH variable and remove "REM" from the following line:

```
REM SET CLASSPATH=%CLASSPATH%;<Location of sapjco3.jar>\sapjco3.jar
```


For example: SET CLASSPATH=%CLASSPATH%;C:\SAP\JCo\sapjco3.jar
 - b. Enter the JAVA JRE directory in the JAVA_HOME variable and remove "REM" from the following line:

```
REM SET JAVA_HOME=<JRE_LOCATION>
```


For example: SET JAVA_HOME=C:\Program Files (x86)\Informatica Cloud Secure Agent\jre
Use the JAVA JRE included with the Informatica Cloud Secure Agent.
4. Save and close the batch file.

SAP BW Connector administration

Before users can use an SAP BW Reader connection to read SAP BW data, you must perform the following tasks:

1. Verify if the required licences are enabled.
2. Download and configure the SAP libraries to read SAP BW data.
3. Install transport files.
4. Configure HTTPS.
5. Configure SAP user authorizations.

Step 1. Verifying if the required licences are available for SAP BW Connector

You must verify if the required licences for SAP BW Connector are available before you create an SAP BW reader connection and read data from SAP BW objects such as InfoCubes, InfoSets, MultiProviders, and DataStore objects.

1. In the Data Integration home page, click the **Administrator** tab.
2. Under **Licences**, verify if the **SAP BW Connector** licence is enabled.

Step 2. Downloading and configuring the libraries for SAP BW data extraction

Before you can use an SAP BW Reader connection, you must download the SAP JCo libraries from the SAP Service Marketplace and configure them on the machine where the Secure Agent runs.

Contact SAP Customer Support if you encounter any issues with downloading the libraries.

1. Go to the SAP Service Marketplace: <http://service.sap.com/connectors>

Note: You will need SAP credentials to access the Service Marketplace.

2. Download the 64-bit SAP JCo libraries based on the operating system on which the Secure Agent runs:

Secure Agent System	SAP File Name
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

Verify that you download the most recent version of the libraries.

3. Copy the JCo libraries to the following directory:

```
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext  
\deploy_to_main\bin\rdtm-extra\tpl\sap
```

Create the `deploy_to_main\bin\rdtm-extra\tpl\sap` directory if it does not already exist.

Note: If you upgrade from a 32-bit operating system, the Secure Agent copies the 32-bit SAP JCo libraries to the directory. You must replace the 32-bit JCo libraries with 64-bit JCo libraries. If you upgrade from a 64-bit operating system, you do not need to perform this step. The Secure Agent copies the 64-bit SAP JCo libraries to the directory.

4. Configure the JAVA_LIBS property in Data Integration.

1. Log in to Data Integration.
2. Click **Runtime Environments** to access the **Runtime Environments** page.
3. To the left of the agent name, click **Edit Secure Agent**.
4. From the **Service** list, select **Data Integration Server**.
5. From the **Type** list, select **Tomcat JRE**.
6. Enter the JAVA_LIBS value based on the operating system on which the Secure Agent runs.

Operating System	Value
Windows	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar

Note: Copy the value to a text editor and make sure that the value you copied is not corrupted. If you copy the value directly from the table, the hyphens (-) in the value are incorrectly copied.

7. Click **OK** to save the changes.
8. Repeat steps 2 through 7 on every machine where you installed the Secure Agent.
5. Restart the Secure Agent.

Step 3. Installing SAP BW Reader transport files

Install the SAP BW Reader transport files on the SAP machines that you want to connect to. Before you install the transports on the production system, install and test the transports in a development system.

Installing transport files

Install transport files from a Secure Agent directory to read data from a Unicode SAP system. The transport files are for SAP NetWeaver BW version 7.x.

1. Find the transport files in the following directory on the Secure Agent machine:

```
<Informatica Secure Agent installation directory>\downloads\package-bwreader.4\package  
\rdtm\sap-transport\SAPBWReader
```

2. Copy the cofile transport file to the `Cofile` directory in the SAP transport management directory on each SAP machine that you want to access.

The cofile transport file uses the following naming convention: `RUN_BWRDR_K<number>.g00`

3. Remove "RUN_BWRDR_" from the file name to rename the cofile. For example, for a cofile transport file named `RUN_BWRDR_K900723.g00`, rename the file to `K900723.g00`.

4. Copy the data transport file to the `Data` directory in the SAP transport management directory on each SAP machine that you want to access.

The data transport file uses the following naming convention: `RUN_BWRDR_R<number>.g00`

5. Remove "RUN_BWRDR_" from the file name to rename the file. For example, for a data transport file named `RUN_BWRDR_R900723.g00`, rename the file to `R900723.g00`.

6. To import the transports to SAP, in the STMS, click **Extras > Other Requests > Add** and add the transport request to the system queue.

7. In the **Add Transport Request to Import Queue** dialog box, enter the request number for the cofile transport.

The request number inverts the order of the renamed cofile as follows: `g00K<number>`.

For example, for a cofile transport file renamed as `K900723.g00`, enter the request number as `g00K900723`.

8. In the Request area of the import queue, select the transport request number that you added, and click **Import**.

Step 4: Configuring HTTPS

To connect to SAP through HTTPS and read data from SAP BW sources, you must configure the machine that hosts the Secure Agent and the machine that hosts the SAP system. You must also enable HTTPS when you configure an SAP BW Reader connection in Data Integration.

Perform the following configuration tasks on the Secure Agent and SAP systems:

HTTPS Configuration on the Secure Agent System

To configure HTTPS on the machine that hosts the Secure Agent, perform the following tasks:

1. Create a certificate using OpenSSL and JAVA KeyTool.
2. Convert the OpenSSL certificate (PKCS#12 certificate) to SAP specific format (PSE) using the SAPGENPSE tool.

Currently, self-signed certificates are supported.

HTTPS Configuration on the SAP System

To configure HTTPS on the machine that hosts the SAP system, perform the following tasks:

1. Enable the HTTPS service on the SAP system.
2. Import the certificate in PSE format to the SAP system trust store.

Step 5. Configuring SAP user authorizations

An SAP administrator needs to create a profile in the development, test, and production SAP system so that you can use the integration features. This profile name must include authorization for the objects and related activities. The profile on the test system should be the same as the profile on the production system.

The setup of the user and profiles is done within SAP using the SAP GUI. This activity is external to Data Integration.

The following table describes the authorization an SAP BW user requires to execute tasks with SAP BW Connector:

Authorization Object	Authorization Value
S_RS_ADMWB	ACTVT=3 (DISPLAY)
S_RS_ICUBE	ACTVT=3 (DISPLAY)
S_RS_ISET	ACTVT=3 (DISPLAY)
S_RS_ODSO	ACTVT=3 (DISPLAY)

SAP ODP Extractor Connector administration

Before you can use an SAP ODP Extractor connection to extract data from an ODP, an SAP Administrator must perform the following tasks:

1. Verify if the required licences are enabled.
2. Verify and install the required SAP Notes in the SAP server.
3. Install the SAP ODP Extractor connection transport files.
4. Configure the SAP user authorization.
5. Download and configure the SAP libraries.

After the administrator has performed the configuration, you can set up and use an SAP ODP Extractor connection in mapping tasks.

Step 1. Verifying if the required licenses are available for SAP ODP Extractor Connector

You must verify if the required licenses for SAP ODP Extractor Connector are available before you create an SAP connection and extract data from ODPs.

1. In the Data Integration home page, click the **Administer** tab.
2. Under **Connector Licences**, verify if the **SAP ODP Extractor Connector** licence is enabled.

Step 2. Verifying and installing prerequisite SAP Notes in the SAP server

SAP ODP Extractor Connector uses the ODP Replication APIs version 2.0.

Before using SAP ODP Extractor Connector, verify that the following SAP Notes are available in the SAP server:

- 1931427 - ODP Data Replication API 2.0
- 2232584 - Release of SAP extractors for ODP replication (ODP SAPI)
- 1560241 - Release of DataSources for ODP data replication API

Step 3. Installing SAP ODP Extractor Connector transport files

Install the SAP ODP Extractor transport files on the SAP machines that you want to access. Before you install the transports on your production system, install and test the transports in a development system.

Install the following data file and cofile to read data from the SAP ODP object:

Data and Cofile Names	Required/Optional	Transport Request	Functionality
<ul style="list-style-type: none">- K900426.IN7- R900426.IN7	Required	IN7K900426	Install the transports only when you want to read from an SAP ODP that supports hierarchy. You can use the SAP ODP Extractor Connector without installing the SAP ODP Extractor transport files for objects that do not support hierarchy.

Installing Transport Files

Install transport files from a Secure Agent directory to read from a Unicode SAP system. The transport files are for SAP version ERP 6.0 EHP7 system or later. To install transport files to write to an SAP system, contact Informatica Global Customer Support.

1. Find the transport files in the following directory on the Secure Agent machine:

```
<Informatica Secure Agent installation directory>\downloads\package-SAPConnector.  
350\package\rdtm\sap-transport\SAPODPReader
```

2. Copy the cofile transport file to the **Cofile** directory in the SAP transport management directory on each SAP machine that you want to access.

The cofile transport file uses the following naming convention: <number>.<sap system>.

3. Copy the data transport file to the **Data** directory in the SAP transport management directory on each SAP machine that you want to access.

The data transport file uses the following naming convention: <number>.<sap-system>.

4. To import the transports to SAP, in the STMS, click **Extras > Other Requests > Add** and add the transport request to the system queue.

5. In the **Add Transport Request to Import Queue** dialog box, enter the request number for the cofile transport.

The request number inverts the order of the renamed cofile as follows: <sap-system><number>.

6. In the Request area of the import queue, select the transport request number that you added, and click **Import**.

7. If you are upgrading from a previous version of the Informatica Transports, select the **Overwrite Originals** option.

Step 4. Configure SAP user authorization

Configure the SAP user account to process the SAP ODP data.

The following table describes the required authorization to read from SAP ODPs:

Read Object Name	Required Authorization Values	Value	Activity	Design Time/Run Time
S_RFC	RFC_TYPE - Function Group(FUGR)	SYST	16	Both
	RFC_TYPE - Function Module(FUGR)	RFC1		Both
	RFC_TYPE - Function Module(FUNC)	RFCPING		Both
	RFC_TYPE - Function Group(FUGR)	RFC_METADATA		Both
	RFC_TYPE - Function Module(FUNC)	RFC_METADATA_GET		Both
	RFC_TYPE - Function Module(FUNC)	RFC_GET_FUNCTION_INTERFACE		Both
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_CONTEXT_GET_LIST		Both
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_ODP_GET_DETAIL		Both
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_ODP_GET_LIST		Both
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_ODP_OPEN		Both
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_ODP_CLOSE		Both
	RFC_TYPE - Function Module(FUNC)	/INFADI/ODP_FETCH_XML		Run Time
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_ODP_FETCH		Run Time
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_ODP_FETCH_XML		Run Time
	RFC_TYPE - Function Module(FUNC)	DDIF_FIELDINFO_GET		Both

Read Object Name	Required Authorization Values	Value	Activity	Design Time/Run Time
S_BTCH_ADM	FIELD NAME - BTCADMIN	Y	N/A	Both
S_BTCH_JOB	FIELD NAME - JOBACTION	RELE	RELE(Release Jobs)	Both
	FIELD NAME - JOBGROUP	' '	N/A	Both
S_RS_ODPH	FIELD NAME - RSODPHNAME	*	3	Both
	FIELD NAME - RSODPHPKG	*		Both
S_RO_OSOA	FIELD NAME - OLTPSOURCE	*	3	Both
	FIELD NAME - OSOAAPCO	*		Both
	FIELD NAME - OSOAPART	Data, Definition		Both
S_RS_HYBR	FIELD NAME - RSHYBRPROV	'*'	3	Both
	FIELD NAME - RSHYBRPROJ	Definition		Both
S_RS_ICUBE	FIELD NAME - OLTPSOURCE	*	3	Both
	FIELD NAME - OSOAAPCO	*		Both
	FIELD NAME - OSOAPART	Data, Definition		Both
S_RS_IOMAD	FIELD NAME - RSINFOAREA	*	3	Both
	FIELD NAME - RSAPPLNM	*		Both
	FIELD NAME - RSIOBJNM	*		Both
S_RS_MPRO	FIELD NAME - RSINFOAREA	*	3	Both
	FIELD NAME - RSMPRO	*		Both
	FIELD NAME - RSMPROOBJ	Data		Both
S_RS_ODSO	FIELD NAME - RSINFOAREA	*	3	Both
	FIELD NAME - RSODSOBJ	*		Both
	FIELD NAME - RSODSPART	Data		Both
S_ADMI_FCD	FIELDNAME - S_ADMI_FCD	PADM	N/A	Both

Step 5. Download and configure the SAP libraries

To read data from SAP ODPs, you must download the SAP JCo libraries and configure them on the machine where the Secure Agent runs. Contact SAP Customer Support if you encounter any issues with downloading the libraries.

1. Go to the SAP Service Marketplace: <http://service.sap.com/connectors>

Note: You must have the SAP credentials to access the Service Marketplace.

2. Download the 64-bit SAP JCo libraries based on the operating system on which the Secure Agent runs:

Secure Agent System	SAP File Name
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

You must download the latest patch for the SAP JCo version 3.1.

3. Copy the JCo libraries to the following directory: <Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\tpl\sap
Create the deploy_to_main\bin\rdtm-extra\tpl\sap directory if it does not already exist.

4. Configure the **JAVA_LIBS** property in Data Integration:
 - a. Log in to Data Integration.
 - b. Click **Runtime Environments** to access the Runtime Environments page.
 - c. To the left of the agent name, click **Edit Secure Agent**.
 - d. From the **Service** list, select **Data Integration Server**.
 - e. From the **Type** list, select **Tomcat JRE**.
 - f. Enter the **JAVA_LIBS** value based on the operating system on which the Secure Agent runs.

Operating System	Value
Windows	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javaliib/sap/sap-adapter-common.jar

Note: Copy the value to a text editor and make sure that the value you copied is not corrupted. If you copy the value directly from the table, the hyphens (-) in the value are incorrectly copied.

- g. From the **Type** list, select **DTM**.

- h. Enter the *JVMClassPath* value based on the operating system on which the Secure Agent runs.

Operating System	Value
Windows	pmserverSDK.jar;../../bin/rdtm-extra/tpl/sap/sapjco3.jar;../../bin/rdtm/javaliB/sap/sap-adapter-common.jar
Linux	pmserverSDK.jar:../../bin/rdtm-extra/tpl/sap/sapjco3.jar:../../bin/rdtm/javaliB/sap/sap-adapter-common.jar

Note: Copy the value to a text editor and make sure that the value you copied is not corrupted. If you copy the value directly from the table, the hyphens (-) in the value are incorrectly copied.

- i. Click **OK** to save the changes.
- j. Repeat steps 2 through 7 on every machine where you installed the Secure Agent.
5. Restart the Secure Agent.

SAP ADSO Writer Connector administration

Before you can use an SAP ADSO Writer connection to load data into an ADSO, an SAP Administrator must perform the following tasks:

1. Verify if the required licences are enabled.
2. Verify the prerequisites in the SAP server.
3. Install the SAP ADSO Writer connection transport files.
4. Configure the SAP user authorization.
5. Download and configure the SAP libraries.

After the administrator has performed the configuration, you can set up and use an SAP ADSO Writer connection in mapping tasks.

Step 1. Verifying if the required licenses are available for SAP ADSO Writer

You must verify if the required licenses for SAP ADSO Writer Connector are available before you create an SAP ADSO Writer connection and load data to an SAP ADSO.

1. In the Data Integration home page, click the **Administer** tab.
2. Under **Connector Licences**, verify if the **SAP ADSO Writer Connector** licence is enabled.

Step 2. Verifying the prerequisites for SAP server

SAP ADSO Writer Connector supports only the SAP BW/4HANA system.

The minimum version of the BW/4HANA system must be 2.0, and is identified through the SAP component *DW4CORE, Release 200*.

Step 3. Installing SAP ADSO Writer Connector transport files

Install the SAP ADSO Writer transport files on the SAP machines that you want to access. Before you install the transports on your production system, install and test the transports in a development system.

Install the following data file and cofile to load data to an SAP BW/4HANA ADSO object.

Data and Cofile Names	Required/Optional	Transport Request	Functionality
- K900105.B42 - R900105.B42	Required	- B42900105	Install the transports to write to an SAP ADSO.

Installing transport files

Install the transport files from a Secure Agent directory to write to a Unicode SAP BW/4HANA system. The transport files are for SAP BW/4HANA version 2.0 or later. To install transport files to write to an SAP system, contact Informatica Global Customer Support.

- Find the transport files in the following directory on the Secure Agent machine:
`<Informatica Secure Agent installation directory>\downloads\package-SAPConnector.350\package\rdtm\sap-transport\SAPBWADSOWriter`
- Copy the cofile transport file to the **Cofile** directory in the SAP transport management directory on each SAP machine that you want to access.
The cofile transport file uses the following naming convention: `<TR Number>.<Sap system>`.
- Copy the data transport file to the **Data** directory in the SAP transport management directory on each SAP machine that you want to access.
The data transport file uses the following naming convention: `ADSO_WRITER_R<TR Number>.<Sap system>`.
- To import the transports to SAP, in the STMS, click **Extras > Other Requests > Add** and add the transport request to the system queue.
- In the **Add Transport Request to Import Queue** dialog box, enter the request number for the cofile transport.
The request number inverts the order of the renamed cofile as follows: `<Sap system><number>`.
- In the Request area of the import queue, select the transport request number that you added, and click **Import**.
- If you are upgrading from a previous version of the Informatica Transports, select the **Overwrite Originals** option.

Step 4. Configure SAP user authorization

Configure the SAP user account to process SAP BW/4HANA ADSO data.

The following table describes the required authorization to read from an SAP BW/4HANA ADSO:

Read Object Name	Required Authorization Values	Value	Activity	Design Time/Run Time
S_RFC	RFC_TYPE - Function Group	SYST	16	Both
	RFC_TYPE - Function Module	RFCPING		Both
	RFC_TYPE - Function Group	RFC1		Both
	RFC_TYPE - Function Module	RFC_GET_FUNCTION_INTERFACE		Both
	RFC_TYPE - Function Group	RFC_METADATA		Both
	RFC_TYPE - Function Module	RFC_METADATA_GET		Both
	RFC_TYPE - Function Group	RSDSO_UPDATE		Both
	RFC_TYPE - Function Module	DDIF_FIELDINFO_GET		Both
	RFC_TYPE - Function Module	BW4_FLP_NOTIFICATIONS_PUSH		Run Time
	RFC_TYPE - Function Module	/INFADI/ADSO_LIST		Both
	RFC_TYPE - Function Module	/INFADI/ADSO_METADATA		Both
	RFC_TYPE - Function Module	/INFADI/RSDSO_WRITE_API RFC		Run Time
S_RS_ADSO	Field Name - RSINFOAREA	*	23	Both
	Field Name - RSOADSONM	*		Both
	Field Name - RSOADSOPAR	Data, Definition		Both
Optional Authorization Object's				

Read Object Name	Required Authorization Values	Value	Activity	Design Time/Run Time
S_RS_AREA	RSINFOAREA	'INFO Area Name'	3	Both
S_ADMI_FCD	S_ADMI_FCD	PADM	N/A	Both

Step 5. Download and configure the SAP libraries

To read data from SAP BW/4HANA ADSO, you must download the SAP JCo libraries and configure them on the machine where the Secure Agent runs. Contact SAP Customer Support if you encounter any issues with downloading the libraries.

- Go to the SAP Service Marketplace: <http://service.sap.com/connectors>
Note: You must have the SAP credentials to access the Service Marketplace.
- Download the 64-bit SAP JCo libraries based on the operating system on which the Secure Agent runs:

Secure Agent System	SAP File Name
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

You must download the latest patch for the SAP JCo version 3.1.

- Copy the JCo libraries to the following directory: <Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\tpl\sap
Create the deploy_to_main\bin\rdtm-extra\tpl\sap directory if it does not already exist.
- Configure the `JAVA_LIBS` property in Data Integration:
 - Log in to Data Integration.
 - Click **Runtime Environments** to access the Runtime Environments page.
 - To the left of the agent name, click **Edit Secure Agent**.
 - From the **Service** list, select **Data Integration Server**.
 - From the **Type** list, select **Tomcat JRE**.
 - Enter the `JAVA_LIBS` value based on the operating system on which the Secure Agent runs.

Operating System	Value
Windows	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javaliib/sap/sap-adapter-common.jar

Note: Copy the value to a text editor and make sure that the value you copied is not corrupted. If you copy the value directly from the table, the hyphens (-) in the value are incorrectly copied.

- g. From the **Type** list, select **DTM**.
- h. Enter the *JVMClassPath* value based on the operating system on which the Secure Agent runs.

Operating System	Value
Windows	pmserver sdk.jar;../../bin/rdtm-extra/tpl/sap/ sapjco3.jar;../../bin/rdtm/javali b/sap/sap-adapter-common.jar
Linux	pmserver sdk.jar:../../bin/rdtm-extra/tpl/sap/ sapjco3.jar:../../bin/rdtm/javali b/sap/sap-adapter-common.jar

Note: Copy the value to a text editor and make sure that the value you copied is not corrupted. If you copy the value directly from the table, the hyphens (-) in the value are incorrectly copied.

- i. Click **OK** to save the changes.
 - j. Repeat steps 2 through 7 on every machine where you installed the Secure Agent.
5. Restart the Secure Agent.

Part III: Connections

This part contains the following chapters:

- [SAP connections, 54](#)
- [Troubleshooting, 78](#)

CHAPTER 3

SAP connections

This chapter includes the following topics:

- [SAP connections overview, 54](#)
- [SAP Table connections, 55](#)
- [SAP IDoc and BAPI/RFC connections, 57](#)
- [SAP BW Reader connections, 59](#)
- [SAP ADSO Writer connections, 61](#)
- [SAP ODP Extractor connections, 66](#)
- [Creating an SAP Table connection, 70](#)
- [Creating an SAP IDoc Reader connection, 71](#)
- [Creating an SAP IDoc Writer or SAP RFC/BAPI interface connection , 72](#)
- [Creating an SAP BW Reader connection, 73](#)
- [Creating an SAP ADSO Writer connection, 74](#)
- [Creating an SAP ODP Extractor connection, 76](#)

SAP connections overview

Use an SAP connection to read from and write data to SAP systems.

Data Integration supports ABAP, IDocs, BAPI/RFC functions, and streaming to integrate with SAP systems. You can choose one of seven SAP connection types to connect to SAP systems based on the interface requirements.

The following table describes the different SAP connections:

SAP Connection Type	Use the connection to ...
SAP Connector	Read data from SAP and write to any target. You can also write data from any source to custom tables in SAP. Contact Global Customer Support for information about using the SAP Table connection to write data to SAP systems.
SAP RFC/BAPI Interface	Read and write data by using BAPI/RFC functions.
IDoc Reader	Read Intermediate Documents (IDocs) from SAP systems.

SAP Connection Type	Use the connection to ...
IDoc Writer	Write IDocs to SAP systems.
SAP BW Reader	Read data from SAP BW objects such as InfoCubes, InfoSets, MultiProviders, and DataStore objects.
SAP ADSO Writer	Write data to SAP ADSO objects in BW4/HANA.
SAP ODP Extractor	Read data from SAP ODP objects from S/4HANA.

SAP Table connections

SAP Table connections enable you to access data directly from SAP tables. You can use the SAP Table connection type in synchronization tasks, mappings, and mapping tasks.

You can use the SAP Table connection type to read data from transparent tables, cluster tables, pool tables, or views. You can also use the SAP Table connection type to write data to custom transparent tables.

To enable the Secure Agent to connect to SAP through HTTPS, you must enable HTTPS and specify the keystore details when you configure an SAP Table connection. To read SAP table sources through HTTPS, specify an SAP Table connection configured for HTTPS when you create synchronization tasks, mappings, or mapping tasks.

SAP Table connection properties

To process SAP table data, select the **SAP Table Connector** connection type and configure the connection properties.

The following table describes the SAP Table connection properties:

Connection property	Description
Runtime Environment	Required. Runtime environment that contains the Secure Agent that you want to use to access SAP tables.
Username	Required. SAP user name with the appropriate user authorization.
Password	Required. SAP password.
Client	Required. SAP client number.
Language	Language code that corresponds to the SAP language.
Saprfc.ini Path	Required. Local directory to the <code>sapnwrfc.ini</code> file. To write to SAP tables, use the following directory: <Informatica Secure Agent installation directory>/main/bin/rdtm

Connection property	Description
Destination	Required. DEST entry that you specified in the <code>sapnwrfc.ini</code> file for the SAP application server. Destination is case sensitive. Note: Use all uppercase letters for the destination.
Port Range	HTTP port range. The SAP Table connection uses the specified port numbers to connect to SAP tables using the HTTP protocol. Ensure that you specify valid numbers to prevent connection errors. Default: 10000-65535. Enter a range in the default range, for example, 10000-20000. When a range is outside the default range, the connection uses the default range.
Test Streaming	Tests the connection. When selected, tests the connection using both RFC and HTTP protocol. When not selected, tests connection using HTTP protocol.
Https Connection	When selected, connects to SAP through HTTPS protocol. To successfully connect to SAP through HTTPS, verify that an administrator has configured the machines that host the Secure Agent and the SAP system.
Keystore Location	The absolute path to the JKS keystore file.
Keystore Password	The destination password specified for the .JKS file.
Private Key Password	The export password specified for the .P12 file.

SAP connection rules and guidelines

The following SAP data types are not supported for the SAP table writer at this time:

- SSTRING
- STRING
- RAWSTRING

Tasks that include these data types for the SAP table writer might fail.

SAP IDoc and BAPI/RFC connections

SAP connections enable you to access SAP data through the IDoc or BAPI/RFC interfaces. You can use the connections in mappings and mapping tasks.

SAP RFC/BAPI interface connection properties

To access SAP data through the RFC/BAPI interface, select the **SAP RFC/BAPI Interface** connection type and configure the connection properties.

The following table describes the SAP RFC/BAPI Interface connection properties:

Connection property	Description
User Name	Required. SAP user name with authorization on S_DATASET, S_TABU_DIS, S_PROGRAM, and B_BTCH_JOB objects.
Password	Required. SAP password.
Connection String	Required. DEST entry that you specified in the <code>sapnwrfc.ini</code> file for the SAP application server.
Code Page	The code page compatible with the SAP target. Select one of the following code pages: <ul style="list-style-type: none">- MS Windows Latin 1. Select for ISO 8859-1 Western European data.- UTF-8. Select for Unicode data.- Shift-JIS. Select for double-byte character data.- ISO 8859-15 Latin 9 (Western European).- ISO 8859-2 Eastern European.- ISO 8859-3 Southeast European.- ISO 8859-5 Cyrillic.- ISO 8859-9 Latin 5 (Turkish).- IBM EBCDIC International Latin-1.
Language Code	Required. Language code that corresponds to the SAP language.
Client Code	Required. SAP client number.

SAP IDoc Reader connection properties

To read SAP data through the IDoc interface, select the **iDoc Reader** connection type and configure the connection properties.

The following table describes the SAP IDoc Reader connection properties:

Connection property	Description
Destination Entry	Required. DEST entry that you specified in the <code>sapnwrfc.ini</code> file for the RFC server program registered at an SAP gateway. The Program ID for this destination entry must be the same as the Program ID for the logical system you defined in SAP to receive IDocs.
Code Page	Required. The code page compatible with the SAP source. Select one of the following code pages: <ul style="list-style-type: none">- MS Windows Latin 1. Select for ISO 8859-1 Western European data.- UTF-8. Select for Unicode data.- Shift-JIS. Select for double-byte character data.- ISO 8859-15 Latin 9 (Western European).- ISO 8859-2 Eastern European.- ISO 8859-3 Southeast European.- ISO 8859-5 Cyrillic.- ISO 8859-9 Latin 5 (Turkish).- IBM EBCDIC International Latin-1.

SAP IDoc Writer connection properties

To write SAP data through the IDoc interface, select the **iDoc Writer** connection type and configure the connection properties.

The following table describes the SAP IDoc Writer connection properties:

Connection property	Description
User Name	Required. SAP user name with authorization on S_DATASET, S_TABU_DIS, S_PROGRAM, and B_BTCH_JOB objects.
Password	Required. SAP password.
Connection String	Required. DEST entry that you specified in the <code>sapnwrfc.ini</code> file for the SAP application server.
Code Page	Required. The code page compatible with the SAP target. Select one of the following code pages: <ul style="list-style-type: none">- MS Windows Latin 1. Select for ISO 8859-1 Western European data.- UTF-8. Select for Unicode data.- Shift-JIS. Select for double-byte character data.- ISO 8859-15 Latin 9 (Western European).- ISO 8859-2 Eastern European.- ISO 8859-3 Southeast European.- ISO 8859-5 Cyrillic.- ISO 8859-9 Latin 5 (Turkish).- IBM EBCDIC International Latin-1.

Connection property	Description
Language Code	Required. Language code that corresponds to the SAP language.
Client code	Required. SAP client number.

SAP BW Reader connections

You must create an SAP BW Connector connection to read data from SAP BW objects such as InfoCubes, InfoSets, MultiProviders, and DataStore objects. You can use the SAP BW Reader connection in synchronization tasks, mappings, and mapping tasks.

To enable the Secure Agent to connect to the SAP BW system through HTTPS, you must enable HTTPS and specify the keystore details in the SAP BW Reader connection. To read data from SAP BW objects through HTTPS, specify an SAP BW Reader connection configured for HTTPS when you create synchronization tasks, mappings, or mapping tasks.

SAP BW Reader connection properties

To read data from SAP BW objects, select the **SAP BW Connector** connection type and configure the connection properties.

The following table describes the SAP BW connection properties:

Connection property	Description
Runtime Environment	Required. Runtime environment that contains the Secure Agent that you want to use to read data from SAP BW objects.
Username	Required. SAP user name with the appropriate user authorization.
Password	Required. SAP password.
Connection type	Required. Type of connection that you want to create. Select one of the following values: <ul style="list-style-type: none"> - Application. Create an application connection when you want to connect to a specific SAP BW server. - Load balancing. Create a load balancing connection when you want to use SAP load balancing. Default is Application.
Host name	Required when you create an SAP application connection. Host name or IP address of the SAP BW server that you want to connect to.
System number	Required when you create an SAP application connection. SAP system number.

Connection property	Description
Message host name	Required when you create an SAP load balancing connection. Host name of the SAP message server.
R3 name/SysID	Required when you create an SAP load balancing connection. SAP system name.
Group	Required when you create an SAP load balancing connection. Group name of the SAP application server.
Client	Required. SAP client number.
Language	Language code that corresponds to the language used in the SAP system.
Trace	<p>Use this option to track the JCo calls that the SAP system makes.</p> <p>Specify one of the following values:</p> <ul style="list-style-type: none"> - 0. Off - 1. Full <p>Default is 0.</p> <p>SAP stores information about the JCo calls in a trace file.</p> <p>You can access the trace files from the following directories:</p> <ul style="list-style-type: none"> - Design-time information: <Informatica Secure Agent installation directory>\main\tomcat - Run-time information: <Informatica Secure Agent installation directory>\main\bin\rdtm
Additional parameters	<p>Additional JCo connection parameters that you want to use.</p> <p>Use the following format:</p> <p><parameter name1>=<value1>, <parameter name2>=<value2></p>
Port Range	<p>HTTP port range that the Secure Agent must use to read data from the SAP BW server in streaming mode.</p> <p>Enter the minimum and maximum port numbers with a hyphen as the separator. The minimum and maximum port number can range between 10000 and 65535.</p> <p>Default is 10000-65535.</p>
Use HTTPS	Select this option to enable https streaming.
Keystore location	Absolute path to the JKS keystore file.
Keystore password	Password for the .JKS file.

Connection property	Description
Private key password	Export password specified for the .P12 file.
SAP Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system as an RFC client.</p> <p>You can specify the required RFC-specific parameters and connection information to enable communication between Data Integration and SAP.</p> <p>For example, you can specify the SNC connection parameters as additional arguments to connect to SAP:</p> <pre>GROUP=interfaces ASHOST=tzxscs20.bmwgroup.net SYSNR=20 SNC_MODE=1 SNC_PARTNERNAME=p:CN=ZXS, OU=SAP system, O=BMW Group SNC_MYNAME=p:CN=CMDB_SWP-2596, OU=SNC partner system, O=BMW Group SNC_LIB=/global/informatica/104/server/bin/libsapcrypto.so X509CERT=/global/informatica/104/SAPSNCertfiles/ROOT_CA_V3.crt TRACE=2</pre> <p>Note: For information about the SNC parameters that you can configure in this field, see the Informatica How-To Library article.</p> <p>Note: If you have specified the mandatory connection parameters in the connection, those values override the additional parameter arguments.</p>

SAP ADSO Writer connections

Use SAP ADSO Writer Connector to connect to the SAP BW/4HANA on-premise application.

You can use SAP ADSO Writer Connector to create an application server connection or a load balancing connection to connect using the SAP user name and password. You can also use create a Secured Network Application (SNC) application server connection or a load balancing connection to connect to SAP BW/4HANA using the SNC parameters.

You must create a connection to SAP BW/4 HANA on-premise systems before designing the mapping or mapping task.

SAP ADSO Writer connection properties

Select the **SAP ADSO Writer** connection type and configure the connection properties. .

The following table describes the SAP ADSO Writer connection properties:

Connection property	Description
Runtime Environment	Runtime environment that contains the Secure Agent that you want to use to access SAP BW/4HANA.
SAP Server Connection Type	<p>The SAP server connection type to use.</p> <p>Select from the following options:</p> <ul style="list-style-type: none">- Application Server Connection. Connect to an SAP Application Server using the SAP user name and password.- Application Server SNC Connection. Connect to an SAP Application Server using the secured network connection:<ul style="list-style-type: none">- With X.509 Certificate. You do not need to specify the SAP user name and password explicitly. You must provide the path of the x.509 certificate file.- Without X.509 Certificate. You must provide the SAP user name.- Load Balancing Server Connection. Connect to an SAP Application Server with the least load at run time.- Load Balancing Server SNC Connection. Connect to an SAP Application Server using SNC with the least load at run time. <p>Note: Before you use an SNC connection, you must verify that SNC is configured both on the SAP Server and the machine where the Secure Agent runs.</p>

The following table describes the properties that must configure when you select **Application Server Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Application Server	The host name of the SAP Application Server.
SAP System Number	The system number of the SAP Server to connect.
SAP Username	The SAP user name with the appropriate user authorization.

Connection property	Description
SAP Password	The SAP password.
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:</p> <pre><Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm</pre> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location:</p> <pre><Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>tomcat.out</pre>

The following table describes the properties that must configure when you select **Load Balancing Server Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Message Server	The IP address or the host name of the SAP Message Server.
SAP System ID	The system ID of the SAP Message Server.
SAP Group	The login group name, for example, PUBLIC.
SAP Username	The SAP user name with the appropriate user authorization.
SAP Password	The SAP password.
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:</p> <pre><Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm</pre> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location:</p> <pre><Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>tomcat.out</pre>

The following table describes the properties that must configure when you select **Application Server SNC Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Application Server	The host name of the SAP Application Server.
SAP System Number	The system number of the SAP Server to connect.
SNC My Name	Optional. The Informatica client Personal Security Environment (PSE) or certificate name. Default length is 256.
SNC Partner Name	The Informatica client PSE or certificate name. Default length is 256.
SNC Quality of Protection (QoP)	Specifies the SAP PSE or certificate name. You can select from the following options: <ul style="list-style-type: none"> - 1 - Apply authentication only. - 2 - Apply integrity protection (authentication). - 3 - Apply privacy protection (integrity and authentication). - 8 - Apply the default protection. - 9 - Apply the maximum protection. Default is 3 - <i>Apply privacy protection (integrity and authentication)</i> .
SAP Cryptographic Library Path	The path to the cryptographic library. Specify <code>sapcrypto.dll</code> for Windows or <code>libsapcrypto.so</code> for Linux.
Use X509 Certificate	Specifies the quality of protection. Select to use X509 Certificate based SNC connection.
X509 Certificate Path or SAP Username	The path to the X509 certificate file. If you select to use the X509 certificate, specify the path to the X509 certificate file with <code>.crt</code> extension. You do not need to specify the SAP user name and password. If you do not want to use the X509 certificate, specify the SAP username for which SNC is configured in SAP Server.
Additional Parameters	Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties: <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> During the runtime, the JCo and CPIC traces file are generated in the following location: <code><Informatica Secure Agent installation directory>\apps</code> <code>\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm</code> During the design time, the CPIC traces are generated in the <code>tomcat.out</code> files at the following location: <code><Informatica Secure Agent installation directory>\apps</code> <code>\Data_Integration_Server\<DIS version>tomcat.out</code>

The following table describes the properties that must configure when you select **Load Balancing Server SNC Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Message Server	The IP address or the host name of the SAP Message Server.
SAP System ID	The system ID of the SAP Message Server.
SAP Group	The login group name, for example, PUBLIC.
SNC My Name	Optional. The Informatica client PSE or certificate name generated on the Secure Agent machine. Default length is 256.
SNC Partner Name	The Informatica client PSE or certificate name generated on the SAP Server. Default length is 256.
SNC Quality of Protection (QoP)	Specifies the SAP PSE or certificate name. You can select from the following options: <ul style="list-style-type: none"> - 1 - Apply authentication only. - 2 - Apply integrity protection (authentication). - 3 - Apply privacy protection (integrity and authentication). - 8 - Apply the default protection. - 9 - Apply the maximum protection. Default is 3 - <i>Apply privacy protection (integrity and authentication)</i> .
SAP Cryptographic Library Path	The path to the cryptographic library. Specify <code>sapcrypto.dll</code> for Windows or <code>libsapcrypto.so</code> for Linux.
Use X509 Certificate	Specifies the quality of protection. Select to use X509 Certificate based SNC connection.
X509 Certificate Path or SAP Username	The path to the X509 certificate file. If you select to use the X509 certificate, specify the path to the X509 certificate file with <code>.cert</code> extension. You do not need to specify the SAP user name and password. If you do not want to use the X509 certificate, specify the SAP user name for which SNC is configured in the SAP Server.
Additional Parameters	Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties: <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> During the runtime, the JCo and CPIC traces file are generated in the following location: <code><Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm</code> During the design time, the CPIC traces are generated in the <code>tomcat.out</code> files at the following location: <code><Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>tomcat.out</code>

SAP ODP Extractor connections

Use the SAP ODP Extractor Connector to connect to SAP S/4HANA on-premise solutions. You must create the connection to the SAP system before designing the mapping or mapping task.

You can use SAP ODP Connector to create an application server connection or a load balancing connection to connect using the SAP user name and password. You can also use create a Secured Network Application (SNC) application server connection or a load balancing connection to connect to SAP S/4HANA using the SNC parameters.

You must create the connection to the SAP system before designing the mapping or mapping task.

SAP ODP Extractor connection properties

Select the **SAP ODP Extractor** connection type and configure the connection properties.

The following table describes the SAP ODP Extractor connection properties:

Connection property	Description
Runtime Environment	Runtime environment that contains the Secure Agent that you want to use to access SAP S/4HANA.
SAP Server Connection Type	<p>The SAP server connection type to use.</p> <p>Select from the following options:</p> <ul style="list-style-type: none">- Application Server Connection. Connect to an SAP Application Server using the SAP user name and password.- Application Server SNC Connection. Connect to an SAP Application Server using the secured network connection:<ul style="list-style-type: none">- With X.509 Certificate. You do not need to specify the SAP user name and password explicitly. You must provide the path of the x.509 certificate file.- Without X.509 Certificate. You must provide the SAP user name.- Load Balancing Server Connection. Connect to an SAP Application Server with the least load at run time.- Load Balancing Server SNC Connection. Connect to an SAP Application Server using SNC with the least load at run time. <p>Note: Before you use an SNC connection, you must verify that SNC is configured both on the SAP Server and the machine where the Secure Agent runs.</p>

The following table describes the properties that must configure when you select **Application Server Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Application Server	The host name of the SAP Application Server.
SAP System Number	The system number of the SAP Server to connect.

Connection property	Description
SAP Username	The SAP user name with the appropriate user authorization.
SAP Password	The SAP password.
Subscriber Name	A name which defines the Secure Agent as a unique subscriber in the SAP system. SAP uses this name to define unique operational delta queue (ODQ) in case of delta read from ODP.
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:</p> <pre><Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm</pre> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location:</p> <pre><Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>tomcat.out</pre>

The following table describes the properties that must configure when you select **Load Balancing Server Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Message Server	Host name of the SAP Message Server.
SAP System ID	The system ID of the SAP Message Server.
SAP Group	The login group name, for example, PUBLIC.
SAP Username	The SAP user name with the appropriate user authorization.
SAP Password	The SAP password.

Connection property	Description
Subscriber Name	A name which defines the Secure Agent as a unique subscriber in the SAP system. SAP uses this name to define unique operational delta queue (ODQ) in case of delta read from ODP.
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location: <Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm</p> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location: <Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>tomcat.out</p>

The following table describes the properties that must configure when you select **Application Server SNC Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Application Server	The host name of the SAP Application Server.
SAP System Number	The system number of the SAP Server to connect.
SNC My Name	Optional. The Informatica client Personal Security Environment (PSE) or certificate name. Default length is 256.
SNC Partner Name	The Informatica client PSE or certificate name. Default length is 256.
SNC Quality of Protection (QoP)	<p>Specifies the SAP PSE or certificate name. You can select from the following options:</p> <ul style="list-style-type: none"> - 1 - Apply authentication only. - 2 - Apply integrity protection (authentication). - 3 - Apply privacy protection (integrity and authentication). - 8 - Apply the default protection. - 9 - Apply the maximum protection. <p>Default is 3 - <i>Apply privacy protection (integrity and authentication)</i>.</p>
SAP Cryptographic Library Path	<p>The path to the cryptographic library. Specify <code>sapcrypto.dll</code> for Windows or <code>libsapcrypto.so</code> for Linux.</p>
Use X509 Certificate	Specifies the quality of protection. Select to use X509 Certificate based SNC connection.

Connection property	Description
X509 Certificate Path or SAP Username	<p>The path to the X509 certificate file.</p> <p>If you select to use the X509 certificate, specify the path to the X509 certificate file with .crt extension. You do not need to specify the SAP user name and password.</p> <p>If you do not want to use the X509 certificate, specify the SAP user name for which SNC is configured in SAP Server.</p>
Subscriber Name	<p>A name which defines the Informatica Secure Agent as a unique subscriber in the SAP system.</p> <p>SAP uses this name to define unique operational delta queue (ODQ) when the Secure Agent reads delta data from ODP.</p>
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system.</p> <p>For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:</p> <pre><Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm</pre> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location:</p> <pre><Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>tomcat.out</pre>

The following table describes the properties that must configure when you select **Load Balancing Server SNC Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Message Server	Host name of the SAP Message Server.
SAP System ID	The system ID of the SAP Message Server.
SAP Group	The login group name, for example, PUBLIC.
SNC My Name	<p>Optional. The Informatica client PSE or certificate name generated on the Secure Agent machine.</p> <p>Default length is 256.</p>
SNC Partner Name	<p>The Informatica client PSE or certificate name generated on the SAP Server.</p> <p>Default length is 256.</p>

Connection property	Description
SNC Quality of Protection (QoP)	<p>Specifies the SAP PSE or certificate name.</p> <p>You can select from the following options:</p> <ul style="list-style-type: none"> - 1 - Apply authentication only. - 2 - Apply integrity protection (authentication). - 3 - Apply privacy protection (integrity and authentication). - 8 - Apply the default protection. - 9 - Apply the maximum protection. <p>Default is 3 - <i>Apply privacy protection (integrity and authentication)</i>.</p>
SAP Cryptographic Library Path	<p>The path to the cryptographic library.</p> <p>Specify <code>sapcrypto.dll</code> for Windows or <code>libsapcrypto.so</code> for Linux.</p>
Use X509 Certificate	<p>Specifies the quality of protection. Select to use X509 Certificate based SNC connection.</p>
X509 Certificate Path or SAP Username	<p>The path to the X509 certificate file.</p> <p>If you select to use the X509 certificate, specify the path to the X509 certificate file with <code>.crt</code> extension. You do not need to specify the SAP user name and password.</p> <p>If you do not want to use the X509 certificate, specify the SAP user name for which SNC is configured in SAP Server.</p>
Subscriber Name	<p>A name which defines the Informatica Secure Agent as a unique subscriber in the SAP system.</p> <p>SAP uses this name to define unique operational delta queue (ODQ) when the Secure Agent reads delta data from ODP.</p>
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system.</p> <p>For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:</p> <pre><Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm</pre> <p>During the design time, the CPIC traces are generated in the <code>tomcat.out</code> files at the following location:</p> <pre><Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>tomcat.out</pre>

Creating an SAP Table connection

1. Click **Administrator > Connections**, and then click **New Connection** to create a connection.
The **New Connection** page appears.
2. Enter a name for the SAP Table connection.
Connection names can contain alphanumeric characters, spaces, and the following special characters:
_ . + -
Connection names are not case sensitive.
3. Enter a description for the connection.

The description can have a maximum length of 255 characters.

4. Select **SAP Table Connector** as the connection type.
The **SAP Table Connector Connection Properties** section appears.
5. Select the name of the runtime environment where you want to run the tasks.
6. Enter an SAP user name with the appropriate user authorization.
7. Enter the SAP password.
8. Enter the SAP client number.
9. Enter the language code that corresponds to the SAP language.
10. Enter the complete path to the `sapnwrfc.ini` file.
11. Enter the destination entry that you specified in the `sapnwrfc.ini` file for the SAP application server.
12. Enter a range of HTTP port numbers that you can use.
13. Select **Test Streaming**, to test the connection with both RFC and HTTP protocol. Clear the field to test the connection with HTTP protocol.
14. Select **Https Connection** to connect to SAP through HTTPS protocol.
15. Enter the absolute path to the JKS keystore file.
16. To specify the destination keystore password as the Keystore Password, type the destination password specified for the .JKS file while creating the OpenSSL certificate.
17. To specify the source keystore password as the Private Key Password, type the export password specified for the .P12 file while creating the OpenSSL certificate.
18. Click **Test Connection** to test the SAP Table connection using HTTP protocol.
19. Click **Save** to save the connection.

Creating an SAP IDoc Reader connection

1. Click **Administrator > Connections**, and then click **New Connection** to create a connection.
The **New Connection** page appears.
2. Enter a name for the SAP IDoc Reader connection.
Connection names can contain alphanumeric characters, spaces, and the following special characters:
_ . + -
Connection names are not case sensitive.
3. Enter a description for the connection.
The description can have a maximum length of 255 characters.
4. Select **SAP** as the connection type.
The **SAP Connection Properties** section appears.
5. Select the name of the runtime environment where you want to run the tasks.
6. Select **iDoc Reader** as the SAP connection type.
The **iDoc Reader Connection Properties** section appears.
7. Enter the destination entry that you specified in the `sapnwrfc.ini` file for the RFC server program registered at an SAP gateway.

The Program ID for this destination entry must be the same as the Program ID for the logical system you defined in SAP to receive IDocs.

8. Select UTF-8 as the code page compatible with the SAP source.
9. Click **Test Connection** to test the connection.
10. Click **Save** to save the connection.

Creating an SAP IDoc Writer or SAP RFC/BAPI interface connection

1. Click **Administrator > Connections**, and then click **New Connection** to create a connection.
The **New Connection** page appears.
2. Enter a name for the connection.
Connection names can contain alphanumeric characters, spaces, and the following special characters:
_ . + -
Connection names are not case sensitive.
3. Enter a description for the connection.
The description can have a maximum length of 255 characters.
4. Select **SAP** as the connection type.
The **SAP Connection Properties** section appears.
5. Select the name of the runtime environment where you want to run the tasks.
6. Select the SAP connection type. You can choose one of the following options:
 - To create an IDoc Writer connection, select **IDoc Writer**.
 - To create a BAPI/RFC connection, select **SAP RFC/BAPI Interface**.The connection properties appear.
7. Enter an SAP user name with the appropriate user authorization.
8. Enter the SAP password.
9. Enter the destination entry that you specified in the `sapnwrfc.ini` file for the SAP application server.
10. Select the code page compatible with the SAP system.
11. Enter the language code that corresponds to the SAP language.
12. Enter the SAP client number.
13. Click **Test Connection** to test the connection.
14. Click **Save** to save the connection.

Creating an SAP BW Reader connection

1. Click **Administrator > Connections**, and then click **New Connection** to create a connection.
The **New Connection** page appears.
2. Enter a name for the SAP BW Reader connection.
Connection names are not case sensitive. Connection names can contain alphanumeric characters, spaces, and the following special characters:
_ . + -
3. Enter a description for the connection.
The description can have a maximum length of 255 characters.
4. Select **SAP BW Connector** as the connection type.
The **SAP BW Connector Connection Properties** section appears.
5. Select the name of the runtime environment where you want to run the tasks.
6. Enter an SAP user name with the appropriate user authorization.
7. Enter the SAP password.
8. Select one of the following connection types:
 - Application. Create an application connection if you want to connect to a specific SAP BW server.
 - Load balancing. Create a load balancing connection if you want SAP to connect to the BW server with the least load at run time.
9. Enter the host name or IP address of the SAP BW server that you want to connect to.
10. Enter the SAP system number.
11. Enter the host name of the SAP message server.
12. Enter the SAP system name.
13. Enter the group name of the SAP BW server.
14. Enter the SAP client number.
15. Enter the language code that corresponds to the language used in the SAP system.
16. Enable the trace option to track the JCo calls that the SAP system makes.
You can enter one of the following values:
 - 0. Off
 - 1. FullDefault is 0.
SAP stores information about the JCo calls in a trace file.
You can access the trace files from the following directories:
 - Design-time information: <Secure Agent installation directory>\main\tomcat
 - Run-time information: <Secure Agent installation directory>\main\bin\rdtm
17. Enter any SAP additional connection parameters that you want to use.
18. Enter the HTTP port range that the Secure Agent must use to read data from the SAP BW server in streaming mode.
Enter the minimum and maximum port numbers with a hyphen as the separator. The minimum and maximum port number can range between 10000 and 65535. When a range is outside the default range,

the connection uses the default range. Ensure that you specify valid numbers to prevent connection errors.

Default is 10000-65535.

19. Select the **Use HTTPS** option to enable https streaming.
 - a. Enter the absolute path to the JKS keystore file.
 - b. Enter the password for the .JKS file.
 - c. Enter the export password for the .P12 file.
20. Click **Test Connection** to determine if the connection to the SAP BW system is successful.
21. Click **Save** to save the connection.

Creating an SAP ADSO Writer connection

1. Click **Administrator > Connections**, and then click **New Connection** to create a connection.
The **New Connection** page appears.
2. Enter a name for the SAP ADSO Writer connection.
3. Enter a description for the connection.
The description can have a maximum length of 255 characters.
4. Select **SAP ADSO Writer** as the connection type.
The **SAP ADSO Writer Connector Connection Properties** section appears.
5. Select the name of the runtime environment where you want to run the tasks.
6. In the **Connection** section, perform the following tasks based on your requirement:
 - a. Select from one of the following connection types:
 - Application Server. Use this connection type to connect to the SAP Application Server using the SAP user name and password.
 - Application Server SNC. Use this connection type to connect to the SAP Application Server using the secured network.
 - Load Balancing. Use this connection type to connect to the SAP message server that uses a load balanced application server. This connection type uses the SAP user name and password.
 - Load Balancing Server SNC. Use this connection type to connect to the SAP message server using the secured network. This connection type uses the secured network connection.

Note: The connection properties appear based on the selected connection type. When you use an SNC connection type, you must configure SNC in both SAP and in the Informatica Secure Agent server.
 - b. Enter the SAP client number.
 - c. Enter the SAP language with which you want to establish the connection.

7. In the **System Connection Details** section, specify the system connection details based on the type of SAP connection type.
 - a. If you select the Application Server or the Load Balancing connection type, you must specify the following system details:
 - SAP Application Server. Specify the IP address or the host name of the Application Server to which you want to connect.
 - SAP System Number. Specify the SAP system number.
 - b. If you select the Application Server SNC connection or the Load Balancing Server SNC connection, you must specify the following system details:
 - SAP Message Server. Specify the details of the SAP message server, for example, the IP address or the host name.
 - SAP System ID. Specify the system ID of the SAP message server.
 - SAP Group. Specify the logon group name, for example, *PUBLIC*.
8. In the **Connection Logon Details** section, specify the login details depending on the connection type.
 - a. If you select the Application Server or Load Balancing Server connection, specify the following SAP credentials:
 - Username. Specify the SAP user name.
 - Password. Specify the SAP password.
 - b. If you select the Application Server SNC Server or Load Balancing Server SNC connection, specify the following connection parameters:
 - SNC My Name. The client PSE or certificate name generated for the Secure Agent.
 - SNC Partner Name. The server PSE or certificate name generated on the SAP server.
 - SNC Quality of Protection (QoP). Select from one of the following options:
 - 1 - Apply authentication only.
 - 2 - Apply authentication and integrity protection.
 - 3 - Apply authentication, integrity and privacy protection (encryption).
 - 8 - Apply global default protection.
 - 9 - Apply the maximum protection.
 - c. SAP Cryptographic Library Path. Specify the path of the SAP Cryptographic library.
You must specify `sapcrypto.dll` for Windows or `libsapcrypto.so` for Linux.
 - d. Use X509 Certificate. Select this option to use the X.509 certificate to log in.
 - e. X509 Certificate Path or SAP Username. Specify the path of the X509 certificate file with `.cert` extension if you selected the X509 certificate. Otherwise, specify the SAP user name for which SNC is configured in the SAP server.
 - f. Additional Parameters. Enter any additional connection parameters that you want to use.
9. Click **Test Connection** to determine if the connection to the SAP BW4/HANA system is successful.
10. Click **Save** to save the connection.

Creating an SAP ODP Extractor connection

1. Click **Administrator > Connections**, and then click **New Connection** to create a connection.
The **New Connection** page appears.
2. Enter a name for the SAP ODP Extractor connection.
3. Enter a description for the connection.
The description can have a maximum length of 255 characters.
4. Select **SAP ODP Extractor** as the connection type.
The **SAP ODP Extractor Connector Connection Properties** section appears.
5. Select the name of the runtime environment where you want to run the tasks.
6. In the **Connection** section, perform the following tasks based on your requirement:
 - a. Select from one of the following connection types:
 - Application Server. Use this connection type to connect to the SAP Application Server using the SAP user name and password.
 - Application Server SNC. Use this connection type to connect to the SAP Application Server using the secured network.
 - Load Balancing. Use this connection type to connect to the SAP message server that uses a load balanced application server. This connection type uses the SAP user name and password.
 - Load Balancing Server SNC. Use this connection type to connect to the SAP message server using the secured network. This connection type uses the secured network connection.

Note: The connection properties appear based on the selected connection type. When you use an SNC connection type, you must configure SNC in both SAP and in the Informatica Secure Agent server.
 - b. Enter the SAP client number.
 - c. Enter the SAP language with which you want to establish the connection.
7. In the **System Connection Details** section, specify the system connection details based on the type of SAP connection type.
 - a. If you select the Application Server or the Load Balancing connection type, you must specify the following system details:
 - SAP Application Server. Specify the IP address or the host name of the Application Server to which you want to connect.
 - SAP System Number. Specify the SAP system number
 - b. If you select the Application Server SNC connection or the Load Balancing Server SNC connection, you must specify the following system details:
 - SAP Message Server. Specify the details of the SAP message server, for example, the IP address or the host name.
 - SAP System ID. Specify the system ID of the SAP message server.
 - SAP Group. Specify the logon group name, for example, *PUBLIC*.

8. In the **Connection Logon Details** section, specify the login details depending on the connection type.
 - a. If you select the Application Server or Load Balancing Server connection, specify the following SAP credentials:
 - Username. Specify the SAP user name.
 - Password. Specify the SAP password.
 - b. If you select the Application Server SNC Server or Load Balancing Server SNC connection, specify the following connection parameters:
 - SNC My Name. The client PSE or certificate name generated for the Secure Agent.
 - SNC Partner Name. The server PSE or certificate name generated on the SAP server.
 - SNC Quality of Protection (QoP). Select from one of the following options:
 - 1 - Apply authentication only.
 - 2 - Apply authentication and integrity protection.
 - 3 - Apply authentication, integrity and privacy protection (encryption).
 - 8 - Apply global default protection.
 - 9 - Apply the maximum protection.
 - c. SAP Cryptographic Library Path. Specify the path of the SAP Cryptographic library.
You must specify `sapcrypto.dll` for Windows or `libsapcrypto.so` for Linux.
 - d. Use X509 Certificate. Select this option to use the X.509 certificate to log in.
 - e. X509 Certificate Path or SAP Username. Specify the path of the X509 certificate file with `.crt` extension if you selected the X509 certificate. Otherwise, specify the SAP user name for which SNC is configured in the SAP server.
 - f. Additional Parameters. Enter any additional connection parameters that you want to use.
9. In the **Subscriber Details** field, specify the subscriber name.
The subscriber name uniquely identifies the Informatica Secure Agent in the SAP Server. SAP uses this name to define the unique operational delta queue (ODQ) when the Secure Agent reads delta data from ODP.
10. Click **Test Connection** to determine if the connection to the SAP S4/HANA system is successful.
11. Click **Save** to save the connection.

CHAPTER 4

Troubleshooting

This chapter includes the following topics:

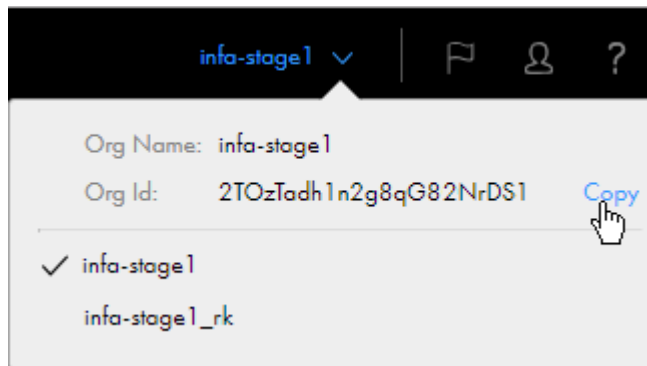
- [Troubleshooting, 78](#)
- [SAP Table connection errors, 79](#)

Troubleshooting

Use the following sections to troubleshoot errors in Data Integration.

Note: To get support for Data Integration, you might need to give your organization ID to Informatica Global Customer Support. You can find your organization ID through the **Organization** menu in the upper right corner.

The following image shows the **Organization** menu:



To copy the organization ID, click the **Copy** option that appears when you hover the cursor to the right of the **Org ID** field.

You can also find your organization ID on the **Organization** page in Administrator.

SAP Table connection errors

The following error displays when I test an SAP Table connection:

```
Test Connection Failed for <connection name>/sap/conn/jco/JCoException
```

Verify that the sapjco3.jar has been saved to the appropriate directories.

Restart the Secure Agent after you copy the sapjco3.jar.

The following error displays when I test an SAP Table connection or use the connection in a task:

```
Test Connection Failed for <connection name>. Error getting the version of the native layer: java.lang.UnsatisfiedLinkError: no sapjco3 in java.library.path.
```

Verify that the location of the sapjco3.dll file is in the to PATH variable for the Secure Agent machine.

The following error displays when I test an SAP Table connection or use the connection in a task:

```
Test Connection Failed for <connection name>. Error getting the version of the native layer: java.lang.UnsatisfiedLinkError: C:\Program Files\vikram\sapjco3-NTintel-3.0.9\sapjco3.dll: This application has failed to start because the application configuration is incorrect. Reinstalling the application may fix this problem.
```

The following error displays when I test an SAP Table connection or use the connection in a task:

```
Test Connection Failed for <connection name>. Error getting the version of the native layer: java.lang.UnsatisfiedLinkError: no sapjco3 in java.library.path.
```

Add the location of sapjco3.dll to PATH variable and restart the Secure Agent.

A task that reads from SAP tables fails with the following error:

```
Error occurred processing data from SAP : Unable to establish Http Communication between SAP server and agent! Shutting down reader.
```

The HTTP port is not open or the incoming request is being blocked by Windows Firewall. To resolve the issue, in Windows Firewall, use the advanced settings to create a new incoming rule. Apply the rule to TCP and all ports, and choose the HTTP-In protocol.

The following error message displays when I select an SAP table as a source object in a synchronization task.

```
Field QUERYRESULT not a member of TABLES
```

Install the latest transport files and clear the browser cache.

Part IV: Data Integration using SAP Table

This part contains the following chapters:

- [SAP Table , 81](#)
- [Synchronization tasks with SAP Table, 84](#)
- [Mappings and mapping tasks with SAP Table, 95](#)

CHAPTER 5

SAP Table

This chapter includes the following topics:

- [SAP objects, 81](#)
- [ABAP CDS views, 81](#)
- [Rules and guidelines for SAP sources and targets, 82](#)

SAP objects

You can connect to SAP views, ABAP CDS views, transparent, pool and cluster tables using an SAP Table connection.

Data Integration does not differentiate between tables and views. You extract data from views the same way you extract data from tables. When you select a table, Data Integration displays the table name followed by the business name in the **Select Object** dialog box. You can filter by table name or business name when you connect to the SAP system.

Data Integration imports the following SAP table information:

- Source name
- Column names
- Business descriptions
- Data types, length, precision, and scale

ABAP CDS views

You can use an ABAP CDS view as a source or lookup in mappings.

Note: ABAP CDS views are supported from SAP NetWeaver system version 7.50 SP4 or later.

When you import an ABAP CDS view into Cloud Data Integration, the agent adds a prefix to the parameter name. The prefix is used to indicate the parameter type.

You can use the following types of parameters:

- **Mandatory Parameter.** A parameter for which you must specify a value. For example, in the field `paramM_P_FISCALYEAR`, `paramM` is the prefix for a mandatory parameter that the agent adds. `P_FISCALYEAR` is the parameter name that is a part of ABAP CDS views.

- **Optional Parameter.** When you define a parameter in SAP and use the annotation `@Environment.systemField`, the parameter appears as an optional parameter in the list of fields. If you do not provide a value, the optional parameter uses the ABAP system fields values.
For example, in the field `paramO_P`, `paramO` is the prefix for an optional parameter that the agent adds. `P_TOFISCALPER` is the parameter name that is a part of ABAP CDS views.

The following image shows the mandatory and optional parameter when you select a CDS view:

	Name	Type	Precision	Scale	Origin
1	paramM_P_FISCALYEAR	string	4	0	C_CN_CADEASSETRETIR...
2	paramM_P_FROMFISCAL...	string	3	0	C_CN_CADEASSETRETIR...
3	paramO_P_TOFISCALPER...	string	3	0	C_CN_CADEASSETRETIR...
4	COMPAN-YCODE	string	4	0	C_CN_CADEASSETRETIR...
5	CN_CADENATLSTDRELVE...	string	10	0	C_CN_CADEASSETRETIR...

In the example, `paramO` denotes an optional parameter and `paramM` denotes a mandatory parameter.

Rules and guidelines for SAP sources and targets

Use the following rules and guidelines when you configure SAP sources and targets:

- When you configure an SAP source, configure row limits using the advanced source properties available on the scheduling page of the task wizard. Row limits on the data filters page of the task wizard are not enabled for SAP sources.
- Do not use tables as SAP Table sources if the sources have circular primary key-foreign key relationships.
- When you use more than one SAP table in a synchronization task, you can use one cluster table or one pool table. If you use more than one cluster or pool table, errors occur at run time. You can use the Object Search dialog box to see if a table is a cluster table or a pool table. You can use multiple transparent tables in a task.
- When you join a cluster table or pool table with a transparent table, include all key fields in the transparent table in the join condition. List the fields in the order that they appear in the SAP system.
- When you join a cluster table or pool table with a transparent table, use all of the source fields in the transparent table that you use in the joins and filters in the field mapping. Also, map at least one field from the cluster or pool table.
- Define relationships for multiple sources after the data preview displays the data. You can use the wizard in advanced mode to avoid waiting to preview data.
- Data sorting is not supported on cluster or pool table fields.
- You can use Data Integration variables and ABAP variables in simple data filters for SAP tables. Do not use ABAP syntax in simple data filters for SAP tables.
- You can use ABAP variables and ABAP syntax in advanced data filters for SAP tables. Do not use Data Integration variables in advanced data filters for SAP tables.
- Do not use the Is Null or Is Not Null operators in data filters for SAP cluster and pool tables.
- Do not use the Is Null or Is Not Null operators in data filters on SAP character fields.
- Use the `$LastRunTime` data filter to display the time when the task ran successfully in the UTC time zone.

- Due to an SAP limitation, tasks that require a read longer than 30 minutes can fail. You might use one or more of the following suggestions if you encounter this problem:
 - Use the SAP advanced source properties to limit the number of rows to be read.
 - Configure a data filter to reduce the number of rows to be read.
 - Reduce the number of output fields for the task.
 - Configure the SAP parameter `rdisp/max_wprun_time` to allow more time for the read. For more information, see the SAP documentation.
 - To increase the amount of records that the Secure Agent can retrieve at one time, you can increase the Java heap memory for the Secure Agent. To do this, edit the Secure Agent. In the System Configuration Details section, select DTM and set the `JVMOption1` property to the following value: `Xmx512m`. Click OK to save the change and restart the Secure Agent. Adjust the value for the `JVMOption1` property based on the amount of records you want to retrieve and the available memory on the Secure Agent machine.
- For a lookup on an SAP object, configure the lookup to return less than 20 rows. Tasks might fail if the lookup returns more than 20 rows.
- A lookup on an SAP object does not return matching rows if the lookup comparison value is NULL.
- When you define a reject file name for an SAP target, use the default name or the variable `$ErrorFileName`. The `$ErrorFileName` variable uses the following convention for reject file name:


```
s_dss_<task name>_<run number>_error.csv.bad
```
- When you define a reject directory for an SAP target, use the variable `$PMBadFileDir`. When you use the `$PMBadFileDir` variable, the synchronization task writes the reject file to the following Secure Agent directory:


```
<SecureAgent_InstallDir>/main/rdtmDir/error
```
- Consider the following rules when you configure a mapping to read from CDS views:
 - When you select a CDS view as an SAP source object in a mapping, you cannot preview the data.
 - When you configure a mapping with a lookup transformation to look up records in CDS views with parameters, only uncached lookup is supported.
 - Delta extraction is not supported for CDS views.
 - Do not use completely parameterized or advanced filters for CDS view parameters.
 - Do not use the `CLNT` field optional parameter in a mapping.
- To establish communication from the SAP system with the Secure Agent using the IP address of the NAT gateway, you must add the DTM property named `SapTableReaderNatIpAddress` for the Secure Agent and specify the NAT IP address as the value.

CHAPTER 6

Synchronization tasks with SAP Table

This chapter includes the following topics:

- [Synchronization tasks with SAP Table overview, 84](#)
- [SAP Table sources in synchronization tasks, 84](#)
- [SAP Table lookups in synchronization tasks, 86](#)
- [Configuring a synchronization task with a single SAP object as the source, 86](#)
- [Configuring a synchronization task with multiple SAP objects as the source, 88](#)
- [Monitoring a synchronization task, 90](#)
- [Synchronization task example, 90](#)

Synchronization tasks with SAP Table overview

The Synchronization application allows you to synchronize data between a source and target.

You can configure a synchronization task using the Synchronization Task wizard. You can use SAP Table objects as sources, targets, or lookup objects. You can use expressions to transform the data according to your business logic, use data filters to filter data before writing it to targets, sort data in ascending or descending order of multiple fields.

When you create a task, you can associate it with a schedule to run it at specified times or on regular intervals. Or, you can run it manually. You can monitor tasks that are currently running and view logs about completed tasks.

SAP Table sources in synchronization tasks

When you configure a synchronization task to use an SAP Table source, you can configure the source properties.

The source properties appear on the **Source** page of the Synchronization Task wizard when you specify an SAP Table connection.

The following table describes the SAP Table source properties:

Property	Description
Connection	Name of the source connection.
Source Type	Source type. Select one of the following types: <ul style="list-style-type: none"> - Single. Select to specify a single SAP Table object. - Multiple. Select to specify multiple SAP Table objects. When you specify multiple source objects, you must create relationships between the source objects.
Source Object	Source object for the task.
Add	Adds multiple source objects.
Create Relationship	Creates relationship between selected source object and related source object. Specify a join condition between a source object key field and a related source object key field.
Edit Relationship	Edits a join condition.
Display technical field names instead of labels	When selected, displays technical names instead of business names of the fields in the specified source object.
Display source fields in alphabetical order	When selected, displays source fields in alphabetic order. By default, fields appear in the order returned by the source system.
Data Preview	Displays the first 10 rows of the first five columns in the object and the total number of columns in the object.
Preview All Columns	Previews all source columns in a file.

You can also configure advanced source properties when you schedule the synchronization task. Advanced source properties appear on the **Schedule** page of the Synchronization Task wizard.

The following table describes the SAP Table advanced source properties:

Property	Description
Number of rows to be fetched	The number of rows that are randomly retrieved from the SAP Table. Default value of zero retrieves all the rows in the table.
Number of rows to be skipped	The number of rows to be skipped.
Packet size in MB	Packet size. Default is 10 MB.
Enable Compression	Enables compression. If the Secure Agent and the SAP System are not located in the same network, you may want to enable the compression option to optimize performance.

SAP Table lookups in synchronization tasks

When you configure field mappings in a synchronization task, you can create a lookup to an SAP Table object.

If you configure an uncached lookup, you can use only the = logical operator in the lookup condition.

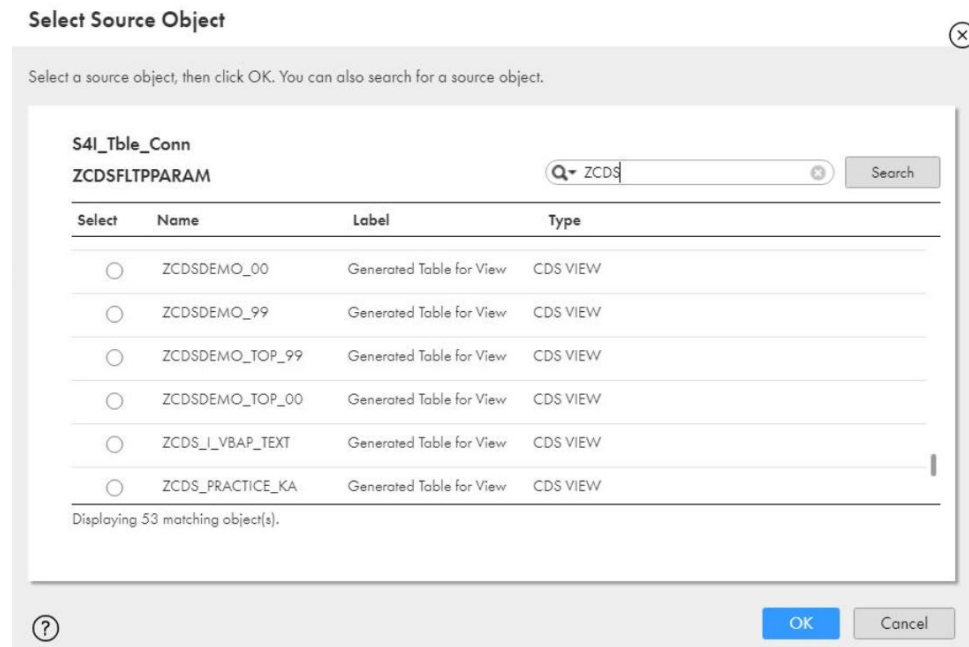
When you configure an uncached lookup, ensure that the data does not contain the pipe (|) character, otherwise data corruption occurs.

When you use an SAP Table object as a lookup, you do not need to configure specific SAP Table properties.

Configuring a synchronization task with a single SAP object as the source

1. To create a synchronization task, click **Data Integration > New > Tasks**. Select **Synchronization Task** and click **Create**.
2. Enter a name for the synchronization task.
The names of synchronization tasks must be unique within the organization. Synchronization task names can contain alphanumeric characters, spaces, and the following special characters: _ . + -
Synchronization task names are not case sensitive.
3. Enter a description for the synchronization task.
The description can have a maximum length of 255 characters.
4. Select the task operation that you can perform on the target. Select one of the following options: Insert, Update, Upsert, and Delete.
5. Click **Next** to enter the source details.
 - a. Select an SAP Table connection.
 - b. Select **Single** as the source type.
 - c. Click **Select** to specify the SAP source object.
The **Select Source Object** dialog box appears. The dialog box displays up to 200 objects. If the objects you want to use do not appear, enter a search string to search based on name and description.

The following image displays the CDS views that you can select:



d. Click **Select**.

The Data Preview area displays the first 10 rows of the first five columns in the SAP object and the total number of columns in the object. To preview all source columns in a file, click **Preview All Columns**.

6. To display technical names instead of business names, select **Display technical field names instead of labels**.
7. To display source fields in alphabetic order, click **Display source fields in alphabetical order**.
By default, fields appear in the order returned by the source system.
8. Click **Next** to specify the target connection and target objects.
9. Click **Next** to specify any data filters or sort criteria.
Note: Specify the row limit in the **Advanced Source Properties** section in the **Schedule** page.
10. Click **New** to create a data filter. You can choose to create a simple or advanced data filter.
 - To create a simple data filter, select a source object, source field, and operator. Enter the value you want to use and click **OK**.
 - To create an advanced data filter, click **Advanced**. Select a source object and enter the field expression you want to use and click **OK**.
You can use parameters defined in a parameter file in the data filters. When you use a parameter in a data filter, start the data filter with the parameter.
11. Click **New** to configure the sort criteria.
 - a. Select the source object, sort by field, and the sort direction.
 - b. Click **New** to configure additional sort criteria or click **Delete** to remove a sort criteria.
12. Click **Next** to configure the field mappings. Perform any of the following steps based on your requirements.
 - a. Click **Edit Types** in the Source column to edit the precision and scale of the SAP object.

- b. Click **Add Mapplet** to select a mapplet and optionally specify a connection for the mapplet.
 - c. Click **Automatch** to match source and target fields with similar names.
 - d. Click **Refresh Fields** to update the cache and view the latest field attributes.
 - e. Click **Edit Types** in the Target column to edit the data type, precision, and scale of the target object. Note that this option is not available for all target types.
 - f. Select a source field and drag it to the target field to map the source and target fields. Repeat for all the fields that you want to map.
 - g. Click the **Add or Edit Expression** icon to define a field expression to transform data.
 - h. Click the **Add or Edit Lookup** icon to create a lookup. Specify the lookup connection, object, source and lookup fields, output field, multiplicity, and lookup expression.
 - i. Click **Validate Mapping** to validate all the field mappings.
 - j. Click **Clear Mapping** to clear all the field mappings.
13. Click **Next** to configure a schedule and advanced options. Perform any of the following steps based on your requirements.
- a. Click **Run this task on schedule** and specify the schedule you want to use.
 - b. Configure the email notification options.
 - c. Configure advanced options for the task.
 - d. Configure the advanced source properties and advanced target properties.
 - e. Specify the execution mode.
14. Save the synchronization task. You can choose one of the following save options.
- Click **Save and Close** to save the task and close the synchronization task.
 - Click **Save and Continue** to save the task and continue with configuring the synchronization task.
 - Click **Save and Run** to save and run the synchronization task.

Configuring a synchronization task with multiple SAP objects as the source

1. To create a synchronization task, click **Data Integration > New > Tasks**. Select **Synchronization Task** and click **Create**.
2. Enter a name for the synchronization task.
The names of synchronization tasks must be unique within the organization. Synchronization task names can contain alphanumeric characters, spaces, and the following special characters: _ . + -
Synchronization task names are not case sensitive.
3. Enter a description for the synchronization task.
The description can have a maximum length of 255 characters.
4. Select the task operation that you can perform on the target. Select one of the following options: Insert, Update, Upsert, and Delete.
5. Click **Next** to enter the source details.
 - a. Select an SAP Table connection.

- b. Select **Multiple** as the source type.
 - c. Click **Add** to specify an SAP source object.
The **Select Source Object** dialog box appears. The dialog box displays up to 200 objects. If the objects you want to use do not appear, enter a search string to search based on name and description. To search for an object using the technical name, enclose the name in double quotes.
 - d. Repeat the previous steps to add multiple SAP objects. To remove a selected object, click the **Delete** icon.
6. Create relationships between the multiple SAP objects.
 - a. Select an SAP object and click **Create Relationship** to create the join conditions between the source and the related object.
The **Create Relationship** dialog box appears.
 - b. Specify the key field in the source SAP object, the type of join, the join operator, the related SAP object, and the key field in the related object.
 - c. Click **OK** to create the relationship.
 - d. Repeat the previous steps to create multiple relationships.
7. To display technical names instead of business names, select **Display technical field names instead of labels**.
8. To display source fields in alphabetic order, click **Display source fields in alphabetical order**.
By default, fields appear in the order returned by the source system.
9. Click **Next** to specify the target connection and target objects.
10. Click **Next** to specify any data filters or sort criteria.
Note: Specify the row limit in the **Advanced Source Properties** section in the **Schedule** page.
11. Click **New** to create a data filter. You can choose to create a simple or advanced data filter.
 - To create a simple data filter, select a source object, source field, and operator. Enter the value you want to use and click **OK**.
 - To create an advanced data filter, click **Advanced**. Select a source object and enter the field expression you want to use and click **OK**.
You can use parameters defined in a parameter file in data filters. When you use a parameter in a data filter, start the data filter with the parameter.
12. Click **New** to configure the sort criteria.
 - a. Select the source object, sort by field, and the sort direction.
 - b. Click **New** to configure additional sort criteria or click **Delete** to remove a sort criteria.
13. Click **Next** to configure the field mappings. Perform any of the following steps based on your requirements.
 - a. In the Source column, select one of the SAP objects or All source objects to map the fields.
 - b. Click **Edit Types** in the Source column to edit the precision and scale of the selected SAP object.
 - c. Click **Add Mapplet** to select a mapplet and optionally specify a connection for the mapplet.
 - d. Click **Automatch** to match source and target fields with similar names.
 - e. Click **Refresh Fields** to update the cache and view the latest field attributes.
 - f. Click **Edit Types** in the Target column to edit the data type, precision and scale of the target object. Note that this option is not available for all target types.

- g. Select a source field and drag it to the target field to map the field. Repeat for all the fields that you want to map.
 - h. Click the **Add or Edit Expression** icon to define a field expression to transform data.
 - i. Click the **Add or Edit Lookup** icon to create a lookup. Specify the lookup connection, object, source and lookup fields, output field, multiplicity, and lookup expression.
 - j. Click **Validate Mapping** to validate all the field mappings.
 - k. Click **Clear Mapping** to clear all the field mappings.
14. Click **Next** to configure a schedule and advanced options. Perform any of the following steps based on your requirements.
- a. Click **Run this task on schedule** and specify the schedule you want to use.
 - b. Configure the email notification options.
 - c. Configure advanced options for the task.
 - d. Configure the advanced source properties and advanced target properties.
 - e. Specify the execution mode.
15. Save the synchronization task. You can choose one of the following save options.
- Click **Save and Close** to save the task and close the synchronization task.
 - Click **Save and Continue** to save the task and continue with configuring the synchronization task.
 - Click **Save and Run** to save and run the synchronization task.

Monitoring a synchronization task

After you run a synchronization task, you can monitor the task and view the logs.

In **Monitor**, you can monitor the status of the logs after you run the task.

You can also monitor the progress of the task by calling Transaction SM37 from SAP. You can view the actual job duration in SAP. The job duration listed in the Data Integration activity log is a higher value because it also includes time required to complete processing in Data Integration.

You can view the HTTP and HTTPS log files in the SMICM transaction. Optionally, you can increase trace level to 3 to view the detailed logs.

Synchronization task example

You can create a synchronization task to read data from multiple SAP objects and write the data to a flat file object.

You can read General Ledger Accounting line items from the BKPF and BSEG tables in SAP. BSEG is an SAP Cluster table that is used to store Accounting Document Segment information. BKPF is a Transparent SAP Table that is used to store Accounting Document Header information. In this example, you can join the BKPF and BSEG tables and map the source object to a flat file target object.

In this example to write the accounting document details to a flat file object, perform the following steps:

1. Define the synchronization task.

2. To configure the SAP Table sources, select an SAP Table connection, and select the BKPF transparent table and the BSEG cluster table as the source objects. Create join conditions between the source BKPF table and the related BSEG table.
3. To configure a flat file target for the task, select a flat file connection and specify a flat file object.
4. Configure the field mappings to define the data that the synchronization task writes to the target.
5. Save and run the synchronization task.

Step 1: Define the synchronization task

1. To create a synchronization task, click **Data Integration > New > Tasks**. Select **Synchronization Task** and click **Create**.
2. Enter a name for the synchronization task.
3. Enter a description for the synchronization task.
4. Select the insert task operation for the target.

The following image shows the task definition page:

5. Click **Next**.

Step 2: Configure the SAP Table source

1. Select an SAP Table connection.
2. Select **Multiple** as the source type.
3. Click **Add** to specify the SAP source object.
The **Select Source Object** dialog box appears. Select the BKPF transparent table.
4. Click **Select**.

5. Click **Add** to select the BSEG cluster table.

The following image shows the **Select Source Object** dialog box:

Select Source Object

Select a source object, and then click Select. You can also search for a source object.

Available Objects*

Demo1_Tableconnector

Q bseg Search

Select	Name	Label	Type
<input type="checkbox"/>	VBSEGK	Vendor Document Parking	TRANSP
<input type="checkbox"/>	VBSEGS	Document Segment for Document Parking - G/L Account Database	TRANSP
<input checked="" type="checkbox"/>	BSEG	Accounting Document Segment	TRANSP
<input type="checkbox"/>	CBSEGFMOBJP	Generated Table for View	VIEW

Displaying 71 matching object(s).

Selected Objects*

Accounting Document Header
Accounting Document Segment

Select Cancel

6. Create relationships between the SAP tables.
 - a. Select the BKPF SAP object and click **Create Relationship** to create the join conditions between the source BKPF table and the related BSEG table.
The **Create Relationship** dialog box appears.
 - b. Specify the key field in the source SAP object, the type of join, the join operator, the related SAP object, and the key field in the related object.
 - c. Click **OK** to create the relationship.
 - d. Repeat the previous steps to create multiple relationships.

The following image shows the **Create Relationship** dialog box:

Create Relationship

Select related object, match the key from source object to key in related object. An example of such keys would primary key and foreign key. Click OK to create this relationship.

Source Object

Source Object: Accounting Document Header

Source Key: Fiscal Yr

Join Options

Join Type: Inner Join

Join Operator: Equals

Related Object

Object: Accounting Document Segment

Object Key: Fiscal Yr

OK Cancel

7. Select a source object to preview the data. The Data Preview area displays the first 10 rows of the first five columns in the SAP object. You can also view the total number of columns in the object. To preview all source columns in a file, click **Preview All Columns**.
8. To display technical names instead of business names, select **Display technical field names instead of labels**.
9. To display source fields in alphabetic order, click **Display source fields in alphabetical order**.
By default, fields appear in the order returned by the source system.

The following image shows the join conditions for multiple SAP objects in the task source details page:

New SAP_TABLE_READER

Source Details

Connection: Demo1_Tableconnector (SAPTableConnect... View... New... Sample... ?

Source Type: ☐ Single ☒ Multiple ☐ Saved Query

Source Objects:

Add... Create Relationship Edit Relationship

Actions	Source Object	Join Condition
<input checked="" type="checkbox"/>	BKPF	
<input checked="" type="checkbox"/>	BSEG	BKPF INNER JOIN BSEG ON BKPF.GJAHR = BSEG.GJAHR
<input checked="" type="checkbox"/>		BKPF INNER JOIN BSEG ON BKPF.MANDT = BSEG.MANDT
<input checked="" type="checkbox"/>		BKPF INNER JOIN BSEG ON BKPF.BUKRS = BSEG.BUKRS
<input checked="" type="checkbox"/>		BKPF INNER JOIN BSEG ON BKPF.BELNR = BSEG.BELNR

☒ Display technical names instead of labels
☐ Display source fields in alphabetical order

Data Preview

Select an object to preview its data.

10. Click **Next**.

Step 3: Configure the flat file target

1. Select a flat file connection and select a flat file object.

2. Select a target flat file object and click **OK**.

The following image shows a flat file object in the task target details page:

New SAP_TABLE_READER

Target Details

Connection: * Demo1_flat (Flat File) View... New... Sample... ?

Target Object: * BKPF-BSEG.csv Select... Formatting Options... ?

☐ Display target fields in alphabetical order

Data Preview

BKPF-BSEG.csv Preview All Columns (Total columns: 1)

Bukrs
1000

3. Click **Next** to specify any data filters or sort fields.
4. Click **Next**.

Step 4: Configure the field mapping

1. Map the source and target fields.
You can select all source objects or one of the source objects to map with the target fields.
2. Click **Next** to configure a schedule and advanced options.
3. Save and run the synchronization task.

CHAPTER 7

Mappings and mapping tasks with SAP Table

This chapter includes the following topics:

- [Mapping and mapping tasks with SAP Table overview, 95](#)
- [SAP Table sources in mappings, 96](#)
- [Delta extraction for SAP table reader mappings, 97](#)
- [Key range partitioning for SAP Table sources, 103](#)
- [SAP Table lookups in mappings, 104](#)
- [Configuring a mapping with an SAP Table source, 105](#)
- [Creating a mapping task, 106](#)
- [Mapping with an SAP Table source example, 107](#)

Mapping and mapping tasks with SAP Table overview

Use a mapping to define data flow logic that is not available in synchronization tasks, such as specific ordering of logic or joining sources from different systems. Use the Data Integration Mapping Designer to configure mappings.

When you configure a mapping to describe the flow of data from source and target, you can also add transformations to transform data. A transformation includes field rules to define incoming fields. Links visually represent how data moves through the data flow.

After you create a mapping, you can run the mapping or you can deploy the mapping in a mapping task. The Mapping Configuration application allows you to process data based on the data flow logic defined in a mapping or integration template.

Use the Mapping task wizard to create a mapping task. When you create a mapping task, you select the mapping or integration template for the task to use.

If you configured parameters, which are placeholders for information, in a mapping, you can define the parameters in the mapping task. Defining parameters provides additional flexibility and allows you to use the same mapping in multiple mapping tasks. For example, you can use a parameter for a source connection in a mapping, and then define the source connection when you configure the mapping task.

When you create a mapping task, you can associate the task with a schedule to run it at specified times or on regular intervals. Or, you can run it manually. You can also configure advanced session properties. You can monitor tasks that are currently running and view details about completed tasks.

SAP Table sources in mappings

To read data from an SAP application, configure an SAP table object as the Source transformation in a mapping.

Specify the name and description of the SAP table source. Configure the source and advanced properties for the source object.

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

Property	Description
Connection	Name of the source connection.
Source Type	Select one of the following types: <ul style="list-style-type: none">- Single. Select to specify a single SAP Table object.- Multiple. Select to specify multiple SAP Table objects. You can use custom relationships to join multiple source objects. When you create a custom relationship for SAP Table objects, you can select the type of join and the source fields to use.- Parameter. Select to specify a parameter name. You can configure the source object in a mapping task associated with a mapping that uses this source transformation.
Object	Source object. When you specify multiple source objects, you must create relationships between the source objects.

The following table describes the SAP Table advanced source properties:

Property	Description
Number of rows to be fetched	The number of rows that are randomly retrieved from the SAP Table. Default value of zero retrieves all the rows in the table.
Number of rows to be skipped	The number of rows to be skipped.
Packet size in MB	The HTTP packet size. When you use bulk mode to read data from an SAP table, you can tune the packet size to increase the throughput. Tune the packet size according to the network bandwidth, memory, and CPU resources available on the Secure Agent. Based on the packet size that you configure and the row length, the Secure Agent calculates the number of rows to be read in a single packet. If you increase the packet size, increase the heap size accordingly to improve the throughput. Default is 10 MB.

Property	Description
Data Extraction Mode	<p>You can use one of the following modes to read data from an SAP Table:</p> <ul style="list-style-type: none"> - Normal Mode. Use this mode to read small volumes of data from the SAP Table. - Bulk Mode. Use this mode to read large volumes of data from the SAP Table. Use bulk mode for better performance. Bulk mode consumes more resources as compared to normal mode. You might need to tune the packet size according to the available resources and data set to increase the performance. <p>Default is normal mode.</p>
Enable Compression	<p>Enables compression.</p> <p>If the Secure Agent and the SAP system are not located in the same network, you might want to enable the compression option to optimize performance.</p>
Update Mode	<p>When you read data from SAP tables, you can configure a mapping to perform delta extraction. You can use one of the following options based on the update mode that you want to use:</p> <ul style="list-style-type: none"> - 0- Full. Use this option when you want to extract all the records from an SAP table instead of reading only the changed data. - 1- Delta initialization without transfer. Use this option when you do not want to extract any data but want to record the latest change number in the Informatica custom table /INFADI/ TBLCHNGN for subsequent delta extractions. - 2- Delta initialization with transfer. Use this option when you want to extract all the records from an SAP table to build an initial set of the data and subsequently run a delta update session to capture the changed data. - 3- Delta update. Use this option when you want to read only the data that changed since the last data extraction. - 4- Delta repeat. Use this option if you encountered errors in a previous delta update and want to repeat the delta update. - Parameter. When you use this option, the Secure Agent uses the update mode value from a parameter file. <p>Default is 0- Full.</p>
Parameter Name for Update Mode	The parameter name that you defined for update mode in the parameter file.
Override Table Name for Delta Extraction	Overrides the SAP table name with the SAP structure name from which you want to extract delta records that are captured with the structure name in the CDPOS table.
Tracing Level	Sets the amount of detail that appears in the log file. You can choose terse, normal, verbose initialization or verbose data. Default is normal.

Delta extraction for SAP table reader mappings

When you read data from SAP tables, you can configure a mapping to perform delta extraction. With delta extraction, you can choose to read only the changed data.

The SAP table and SAP columns for which you want to perform delta extraction must be part of a change document object in SAP. For more information about creating a change document in SAP, see the SAP documentation.

The Secure Agent uses the CDHDR (Change Document Header) and CDPOS (Change Document Position) tables in SAP to extract the changed data. The CDHDR table stores the change document header information. The CDPOS table stores the new value and the old value of the changed data. The Secure Agent uses the change document number in the CDHDR table to find the latest change number in the CDPOS table.

Delta extraction behavior

When you configure a delta extraction, the Secure Agent does not fetch the change indicators marked for insert, delete, update, or data driven for delta records from SAP. Hence, the delta rows that are extracted from the source are marked for upsert by default.

When you perform a delta extraction and if the row is available in the SAP target table, the Secure Agent updates the delta records to the target table. If the row is not available, the Secure Agent inserts the records to the SAP target table.

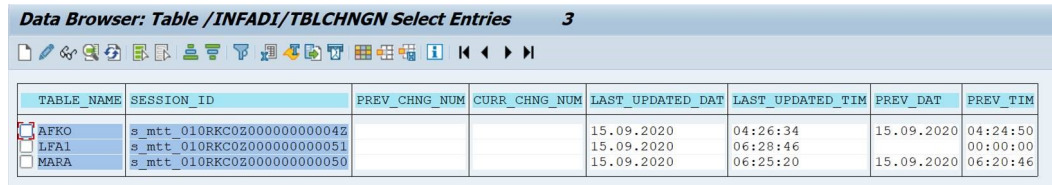
If multiple transactions such as insert, update, or delete occurs for the same record in the SAP source, the Secure Agent fetches only one record. However, if an operation, for example, an insert for a record occurs in the SAP source table and you run the mapping, the Secure Agent fetches the inserted record. Later, if an update occurs for the same record in the SAP source table and you run the delta extraction mapping, the Secure Agent fetches the updated record.

When you perform a delta extraction for deleted records in the SAP table, the records that are marked for hard deletion in the SAP source table are not fetched. If the records are marked for soft deletion, where the `isDeleted` flag for the record is set to true, you can add transformations in the SAP Table Reader mapping to extract that record.

Informatica custom table /INFADI/TBLCHNGN

The Secure Agent creates and maintains an Informatica custom table in SAP named `/INFADI/TBLCHNGN`. The `/INFADI/TBLCHNGN` table captures the time that is used for delta extraction through the Informatica mappings. You can use transaction SE11 or SE16 to view the table entries.

The following image shows the `/INFADI/TBLCHNGN` table:



TABLE_NAME	SESSION_ID	PREV_CHNG_NUM	CURR_CHNG_NUM	LAST_UPDATED_DAT	LAST_UPDATED_TIM	PREV_DAT	PREV_TIM
<input checked="" type="checkbox"/> AFKO	s_mtt_010RKC0Z000000000004Z			15.09.2020	04:26:34	15.09.2020	04:24:50
<input type="checkbox"/> LFAL	s_mtt_010RKC0Z0000000000051			15.09.2020	06:28:46		00:00:00
<input type="checkbox"/> MARA	s_mtt_010RKC0Z0000000000050			15.09.2020	06:25:20	15.09.2020	06:20:46

The `/INFADI/TBLCHNGN` table contains the following columns:

TABLE_NAME

Specifies the SAP source table name from which data is extracted.

SESSION_ID

Specifies the unique Informatica session ID for delta extraction. The Secure Agent generates a unique session ID for each mapping run for a particular SAP table.

PREV_CHNG_NUM

Not applicable.

CURR_CHNG_NUM

Not applicable.

PREV_DAT

Indicates the date from when changes were extracted in the last delta extraction. The Secure Agent uses this information when you use the Delta Repeat option.

PREV_TIME

Indicates the time from when the changes were extracted in the last delta extraction. The Secure Agent uses this information when you use the Delta Repeat option.

LAST_UPDATED_DAT

Indicates the date up to when the changes were extracted from the source in the last delta extraction. This value also indicates the date from when the changes will be extracted for the subsequent delta extraction.

LAST_UPDATED_TIM

Indicates the time up to when the changes were extracted from the source in the last delta extraction. This value also indicates the time from when the changes will be extracted for the subsequent delta extraction.

Update modes for delta extraction

When you configure delta extraction for SAP table reader mappings, you can select the update mode that you want to use.

You can select one of the following update modes:

Full

If you select the **Full** option, the Secure Agent extracts all the records from an SAP table. The Secure Agent does not update any details in the Informatica custom table /INFADI/TBLCHNGN.

Use this option when you want to extract all the records from an SAP table instead of reading only the changed data.

Default is **Full**.

Delta initialization without transfer

If you select the **Delta initialization without transfer** option, the Secure Agent does not extract any data from an SAP table but records the LAST_UPDATED_DAT and LAST_UPDATED_TIM in the Informatica custom table /INFADI/TBLCHNGN for subsequent delta extractions.

The Secure Agent performs the following actions:

- Sets the values for LAST_UPDATED_DAT and LAST_UPDATED_TIM columns.
- Initializes and sets the values for the PREV_DAT and PREV_TIM columns.

Use this option when you do not want to extract any data but you want to record the LAST_UPDATED_DAT and LAST_UPDATED_TIM in the Informatica custom table /INFADI/TBLCHNGN for subsequent delta extractions.

For example, you have a table named **Customers** that contains 5 million records. You want to read the initial set of records by using another product such as Informatica Data Replication and then write the records to a Teradata data warehouse. You then want to use SAP Connector to read only the new customer records that get added to the table. In this case, you can configure delta initialization without transfer and then subsequently run a delta update session to capture the changed data.

Delta initialization with transfer

If you select the **Delta initialization with transfer** option, the Secure Agent extracts all the records from an SAP table but you want to record the LAST_UPDATED_DAT and LAST_UPDATED_TIM in the Informatica custom table /INFADI/TBLCHNGN for subsequent delta extractions.

The Secure Agent performs the following actions:

- Sets the LAST_UPDATED_DAT and LAST_UPDATED_TIM columns.
- Initializes the PREV_DAT and PREV_TIM.

- Extracts all the data present in the SAP table.

Use this option when you want to extract all the records from an SAP table to build an initial set of the data and subsequently run a delta update session to capture the changed data.

Delta update

If you select the **Delta update** option, the Secure Agent extracts the changed data since the last data extraction.

The Secure Agent performs the following actions:

- Extracts records from the columns LAST_UPDATED_DAT AND LAST_UPDATED_TIM to the current date and time.
- Moves the values from columns LAST_UPDATED_DAT and LAST_UPDATED_TIM to PREV_DAT and PREV_TIM, respectively.
- Updates the values in columns LAST_UPDATED_DAT and LAST_UPDATED_TIM to the current date and time.

Use this option when you want to read only the data that changed since the last data extraction.

Before you run a delta update session, you must have performed a delta initialization with transfer or delta initialization without transfer. The delta initialization records the LAST_UPDATED_DAT AND LAST_UPDATED_TIM that the Secure Agent uses to run a delta update session.

Note: To avoid data loss, the current date and time is frozen before the Secure Agent runs the query. If any data enters at the time when the mapping runs, that data is extracted only when you run the next mapping.

Delta repeat

If you select the **Delta repeat** option, the Secure Agent repeats a previous delta update in case of errors. It returns records from the PREV_DAT and PREV_TIM values in the Informatica custom table /INFADI/TBLCHNGN to the LAST_UPDATED_DAT and LAST_UPDATED_TIM values in the Informatica custom table /INFADI/TBLCHNGN. It does not update any change numbers in the /INFADI/TBLCHNGN table.

Use this option if you encountered errors in a previous delta update and want to repeat the delta update.

Before you run a delta repeat session, you must have performed a delta update.

Parameter

If you select the **Parameter** option, the Secure Agent uses the update mode value from a parameter file. Define a parameter name and parameter value in a parameter file. In the SAP table reader mapping that you create for delta extraction, specify the same parameter name that you defined in the parameter file. Then, create a mapping task and specify the parameter file name in the task. Instead of updating the parameter value in the mapping every time, you can update the parameter value in the parameter file and run the mapping task again.

Configuring a parameter file for delta extraction

A parameter file is a list of user-defined parameters and their associated values. To perform a delta extraction, you can specify the update mode in a parameter file so that you do not need to edit the mapping every time you want to change the update mode.

To use a parameter file, perform the following steps:

1. Create a parameter file in the following directory:
`<Secure Agent installation directory>/apps/Data_Integration_Server/data/userparameters`
2. In the parameter file, enter a parameter name and specify the parameter value that you want to use.

The parameter name must start with \$\$ and cannot contain space characters.

You can use one of the following parameter values based on the update mode that you want to use:

- **0.** Use for Full.
- **1.** Use for Delta initialization without transfer.
- **2.** Use for Delta initialization with transfer.
- **3.** Use for Delta update.
- **4.** Use for Delta repeat.

Use the following format to specify the parameter name and parameter value:

```
$$<parameter_name>=<parameter_value>
```

Do not use space characters while specifying the parameter name and parameter value.

For example, enter: `$$deltaparameter=0`

3. Save the parameter file.
4. Open the SAP table reader mapping that you want to use for delta extraction.
5. Select **Parameter** from the **Update Mode** list.
6. In the **Parameter Name for Update Mode** field, enter the parameter name that you defined in the parameter file.
7. Create a mapping task based on the SAP table reader mapping.
8. In the **Schedule** page of the mapping task, enter the parameter file name under the **Advanced Options** section.
9. Run the mapping task.

To change the update mode, update the parameter value in the parameter file, and run the mapping task again. For example, the first time you run a mapping task, you can specify the parameter value as **2** to use delta initialization with transfer. After the initial extraction is done, you might want to change the parameter value to **3** to capture only the changed data in the next mapping task run. Instead of updating the parameter value in the mapping every time, you can update the parameter value in the parameter file and run the mapping task again.

Configure a table name override for delta extraction

When you configure a SAP Table reader mapping, you can override the selected table name at runtime with the structure name to perform a delta extraction.

When you run an SAP Table reader mapping for delta extraction, the Secure Agent fetches changed records from the SAP table for entries logged for the SAP table name in the Change Document Position (CDPOS) table. If there are entries logged for the SAP table structure in the CDPOS table, you can fetch those records by overriding the table name in the **Override Table Name for Delta Extraction** field in the SAP Table advanced source properties.

For example, if the table name you specified as the object type in the mapping is *CRMD_ORDERADM_H*, to get the delta records for entries captured in the CDPOS table for the structure name, specify the structure name *CRMA_ORDERADM_H* in the **Override Table Name for Delta Extraction** field. The Secure Agent fetches records from *CRMA_ORDERADM_H* that has change entries logged for the table structure.

If the delta data captured in the CDPOS table does not include the structure name, keep this field blank.

Rules and guidelines for delta extraction

Consider the following rules and guidelines when you configure delta extraction for SAP table reader mappings:

- You can perform delta extraction only for a single SAP table. You cannot use native joins to join data from two or more SAP tables.
- You cannot configure delta extraction to look up data from SAP tables.
- You cannot configure delta extraction with partitioning.
- You cannot configure delta extraction for multiple pipelines within the same mapping.
- When the Secure Agent performs a delta extraction, it does not retrieve the records in the same order in which they were inserted or updated in the SAP table. For example, record 10 might have been updated first in the SAP table before record 20. However, while extracting the data, the Secure Agent might fetch record 20 first and then record 10.
- The Secure Agent does not print any information in the session log to indicate whether the records extracted through delta extraction were part of an insert or update operation in SAP.
- During delta extraction, if there are multiple entries for a key between the current and last updated date and time, the Secure Agent fetches only the latest entry for the key.
For example, consider that a record was inserted into a Customer table in SAP with the customer name set to `John`. The record was later updated and the name was changed to `Bill`. The Secure Agent fetches the name value as only `Bill`.
- QUAN and CURR data types are not supported in delta extraction mappings.
- You cannot configure delta extraction in data transfer tasks.

Configuring delta extraction for an SAP table reader mapping

To configure delta extraction for an SAP table reader mapping, select the update mode that you want to use and optionally define a parameter in the mapping.

1. Create a mapping to read data from an SAP table and write data to a target.
2. Click the Source transformation in the mapping.
3. In the **Properties** panel, click the **Source** tab.
4. Under the advanced properties, select one of the following values from the **Update Mode** list:
 - **0 - Full**
 - **1 - Delta initialization without transfer**
 - **2 - Delta initialization with transfer**
 - **3 - Delta update**
 - **4 - Delta repeat**
 - **Parameter**

For information about using a parameter for delta extraction, see [“Configuring a parameter file for delta extraction” on page 100](#).

5. Save and run the mapping.

Troubleshooting delta extraction for SAP Table Reader mappings

Why do I see the error "Only Full Update Mode is supported for table {table_name} because it is not a part of any change document object in SAP"?

The error occurs because the SAP table for which you are trying to perform delta extraction is not part of a change document object in SAP.

If the SAP table and SAP columns for which you want to perform delta extraction are not part of a change document object in SAP, you cannot perform delta extraction. You can only perform a full extraction.

Why do I see the error "An error occurred while fetching the current date and time from SAP because there is no entry present in the /INFADI/TBLCHNGN table. Run a delta initialization session first."?

The error occurs when you run a delta update or delta repeat session directly without performing a delta initialization.

The delta initialization records the LAST_UPDATED_DAT and LAST_UPDATED_TIM that the Secure Agent uses to run a delta update or delta repeat session. Without delta initialization, the Secure Agent does not have access to the LAST_UPDATED_DAT and LAST_UPDATED_TIM to run a delta update or delta repeat session.

In the INFADI/TBLCHNGN table, how can I view entries corresponding to my mapping run?

You can refer to the session log to find out the session ID for your mapping. In the INFADI/TBLCHNGN table, look for the same session ID to view details about your mapping run. The Secure Agent generates a unique session ID for each mapping run for a particular SAP table. You can also sort the INFADI/TBLCHNGN table entries based on the session ID.

Why does the number of records extracted through the Full or Delta initialization with transfer option not match the number of records extracted through the Delta repeat option?

When you use the **Full** or **Delta initialization with transfer** option, the Secure Agent extracts all the records directly from the SAP table and not only the records that are captured in the change document. However, when you use the **Delta repeat** option, the Secure Agent extracts only the records that are captured in the change document.

Therefore, after you perform a full extraction or delta initialization with transfer, if you run a delta repeat session, the extracted records count might not match with the number of records extracted through the **Full** or **Delta initialization with transfer** option.

Key range partitioning for SAP Table sources

You can configure key range partitioning when you use a mapping task to read data from SAP table sources using normal mode. With key range partitioning, the Secure Agent distributes rows of source data based on the fields that you define as partition keys. The Secure Agent compares the field value to the range values for each partition and sends rows to the appropriate partitions.

Use key range partitioning for columns that have an even distribution of data values. Otherwise, the partitions might have unequal size. For example, a column might have 10 rows between key values 1 and 1000 and the column might have 999 rows between key values 1001 and 2000. If the mapping includes multiple sources, use the same number of key ranges for each source.

When you define key range partitioning for a column, the Secure Agent reads the rows that are within the specified partition range. For example, if you configure two partitions for a column with the ranges as 10

through 20 and 30 through 40, the Secure Agent does not read the rows 20 through 30 because these rows are not within the specified partition range.

You can configure a partition key for fields of the following data types:

- ACCP
- DATS
- INT1
- INT2
- INT4
- NUMC
- TIMS

You cannot use key range partitions when a mapping includes any of the following transformations:

- Web Services
- XML to Relational

Configuring key range partitioning for SAP Table sources

When you use a mapping task to read data from SAP table sources, you can configure key range partitioning to improve performance. Define the partition keys and key ranges based on which the Secure Agent must distribute rows of source data.

1. In the source properties, click the **Partitions** tab.
2. In the **Partition Key** field, select the required partition key from the list.
3. In the **Key Ranges** section, click **Add New Key Range** to define the number of partitions and the key ranges based on which the Secure Agent must partition data.

Use a blank value for the start range to indicate the minimum value. Use a blank value for the end range to indicate the maximum value.

Best practices for key range partitioning

If you increase the partitions in normal mode, tune the value of the parameter `rdisp/wp_no_btc` on the SAP server accordingly to increase the throughput. The parameter `rdisp/wp_no_btc` denotes the number of background processes.

Contact your SAP administrator to increase the value of the parameter on the SAP side.

SAP Table lookups in mappings

In a mapping, you can configure a Lookup transformation to look up data from SAP Table objects.

If you configure an uncached lookup, you can use only the = logical operator in the lookup condition.

When you configure an uncached lookup, ensure that the data does not contain the pipe (|) character, otherwise data corruption occurs.

When you use an SAP Table object as a lookup, you do not need to configure specific SAP Table properties.

Configuring a mapping with an SAP Table source

Use the Data Integration Mapping Designer to configure a mapping and describe the data flow between the source and target. You can also configure filter and sort options, advanced source properties, key range partitioning, and transformations in the mapping.

1. To create a mapping, click **Data Integration > New > Mappings**. Select **Mapping** and click **Create**.
2. Enter a name and description for the mapping, and click **OK**.
You can use alphanumeric characters and underscores (_) in the mapping name.
3. To configure a source, on the **Transformation palette**, click **Source**.
4. In the **Properties** panel, on the **General** tab, enter a name and description.
5. Click the **Source** tab and configure source details.
6. Specify the source type. You can choose one of the following options:
 - Select **Single Object** to select a single SAP object.
 - Select **Multiple Objects** to specify source object, related source object, and configure the relationship between the source objects. You can use custom relationships to join multiple source objects. When you create a custom relationship for SAP Table objects, you can select the type of join and the source fields to use.
 - Select **Parameter** to configure the source objects in a mapping task associated with this mapping.
7. Click **Query Options** in the **Source** tab to specify any filter and sort options for the SAP object.
8. Click **Advanced** to specify the advanced source properties.
9. To add or remove source fields, to update field metadata, or to synchronize fields with the source, click the **Fields** tab.
Note: You can edit the type, precision, and scale in the SAP table source object metadata.
10. To configure key range partitioning, click the **Partitions** tab.
 - a. In the **Partition Key** field, select the required partition key from the list.
 - b. In the **Key Ranges** section, click **Add New Key Range** to define the number of partitions and the key ranges based on which the Secure Agent must partition data.
Use a blank value for the start range to indicate the minimum value. Use a blank value for the end range to indicate the maximum value.
11. To add a transformation, on the **Transformation palette**, click the transformation name. Or, drag the transformation onto the mapping canvas.
 - a. On the **General** tab, you can enter a name and description for the transformation.
 - b. Draw a link to connect the previous transformation to the transformation.
When you link transformations, the downstream transformation inherits the incoming fields from the previous transformation.
For a Joiner transformation, draw a master link and a detail link.
 - c. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.
 - d. Configure additional transformation properties, as needed.
The properties that you configure vary based on the type of transformation you create.
 - e. To add another transformation, repeat these steps.
12. To add a Target transformation, on the **Transformation palette**, click **Target**.
 - a. On the **General** tab, you can enter a name and description.

- b. Draw a link to connect the previous transformation to the Target transformation.
 - c. Click the **Target** tab and configure target details. If necessary, configure the advanced target properties.
Target details and advanced target properties appear based on the connection type. For more information, see *Transformations*.
 - d. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.
 - e. Click **Field Mapping** and map the fields that you want to write to the target.
 - f. To add another Target transformation, repeat these steps.
13. Save and run the mapping or save and create a mapping task.

Creating a mapping task

You can create a mapping task based on a valid mapping or integration template on the Mappings page.

1. To create a mapping task, click **Data Integration > New > Tasks** and then complete one of the following steps:
 - To create a mapping task based on a mapping, select **Mapping Task** and click **Create**.
 - To create a mapping task using a template, expand the appropriate template category and select the template you want to use, and then click **Create**.

To edit a mapping task, on the **Explore** page, navigate to the mapping task. In the row that contains the task, click **Actions** and select **Edit**.

2. Enter a name for the task.
Task names must be unique within the organization. Task names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Task names are not case sensitive.
3. Select the runtime environment that contains the Secure Agent that you want to use to access the SAP tables.
4. Select **Mapping** as the task based on which you want to create the mapping task.
5. Click **Select** to specify a mapping.
The **Select a Mapping** dialog box appears.
6. Select a mapping or search for the required mapping and select **OK**.
The image of the selected mapping appears.
7. Click **Next**.
If you specified any parameters in the source or target details in the mapping, the Source or Target page appears. If not, the Schedule page appears.
8. Click **Next** to configure a schedule and advanced options. Perform any of the following steps based on your requirements.
 - a. Click **Run this task on schedule** and specify the schedule you want to use.
 - b. Configure the email notification options.
 - c. Configure advanced options for the task.
 - d. Configure the advanced source properties and advanced target properties.

- e. Specify the execution mode.
9. Optionally, add advanced session properties.
 - a. Click **Add**.
 - b. Select a session property.
 - c. Configure the value of the session property.
10. Save and run the mapping task.

Mapping with an SAP Table source example

You can create a mapping to read data from a single SAP object and write the data to a target object.

You can read data from an SAP purchasing document header, the EKKO table, and write the purchasing details to any target.

In this example to read data from the EKKO table and write the data to a flat file target object, perform the following steps:

1. Define the mapping.
2. To configure an SAP Table source, select an SAP Table connection and select the EKKO table.
3. To configure a flat file target, select a flat file connection, specify a flat file object, and map the source and target fields.
4. Save the mapping and create a mapping task.

Step 1: Define the mapping

1. To create a mapping, click **Data Integration > New > Mappings**. Select **Mapping** and click **Create**.
2. Enter a name and description for the mapping.

The following image shows the **New Mapping** dialog box:

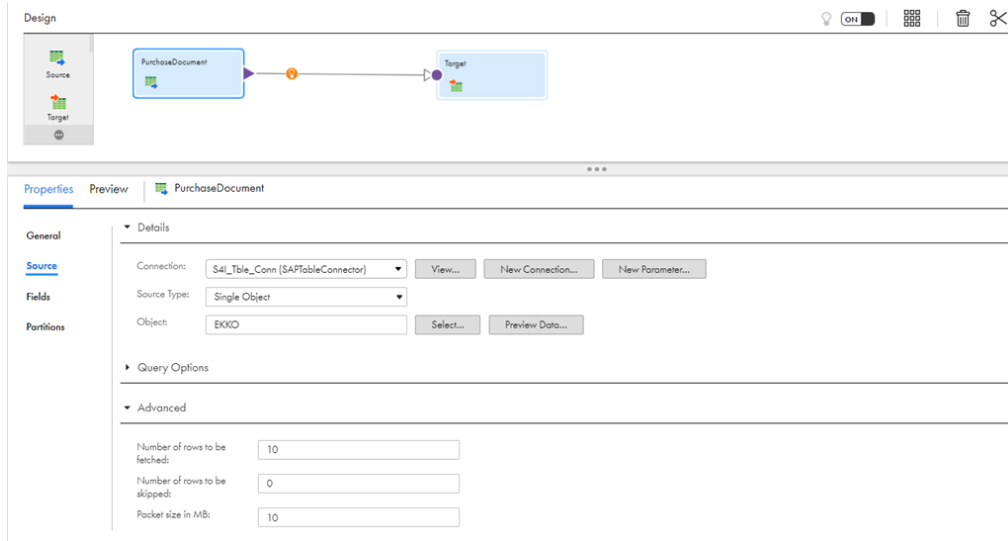
3. Click **OK**.

Step 2: Configure the SAP Table source

1. To configure an SAP source, on the **Transformation** palette, click **Source**.
2. In the **Properties** panel, on the **General** tab, enter a name and description.
3. Click the **Source** tab to configure source details.
4. Specify an SAP Table connection as the source object connection.
5. Specify the source type as **Single Object** and click **Select**.
6. In the **Select Source Object** dialog box, select the EKKO table,
7. Click **Query Options** in the **Source** tab to specify any filter and sort options for the SAP Table object.

8. Click **Advanced** to specify the advanced source properties.

The following image shows the source details page:

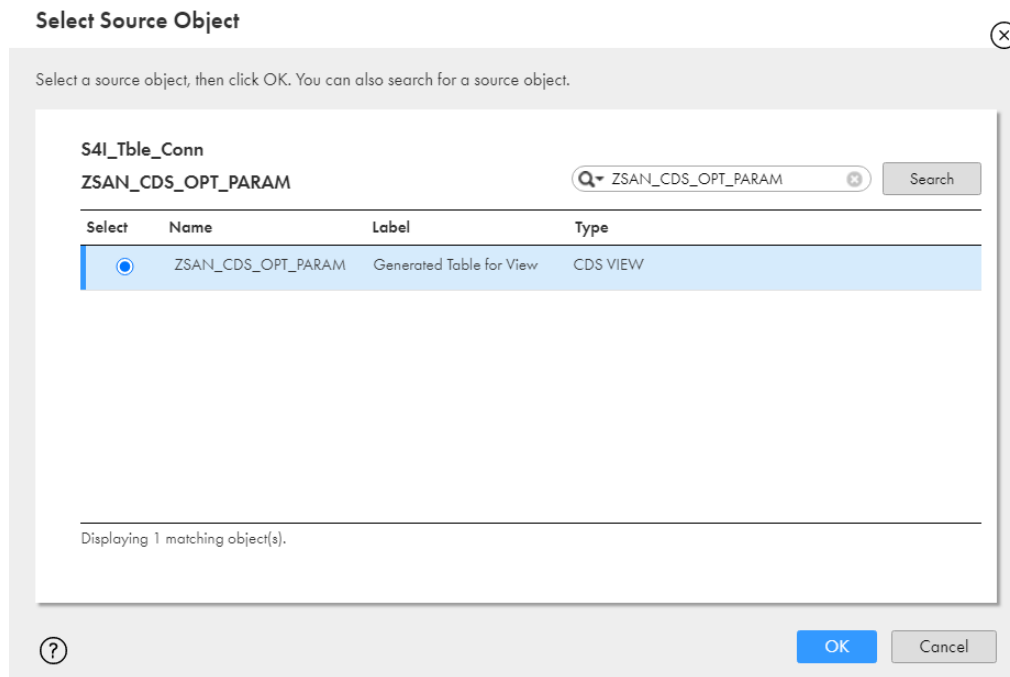


Configure an ABAP CDS view as an SAP source

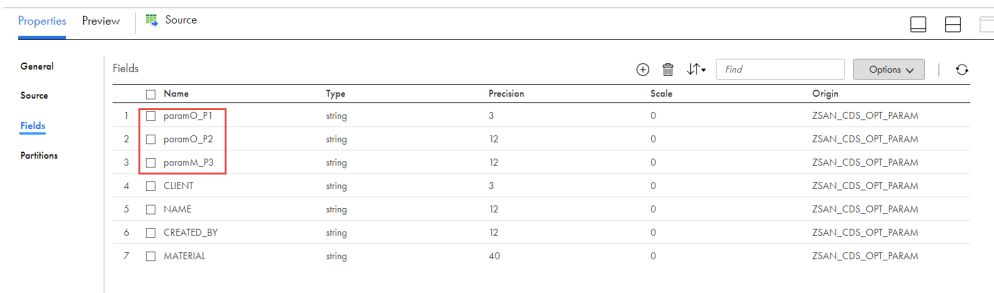
To read from an ABAP CDS view, configure the ABAP CDS view as the source in a mapping.

1. On the **Transformation** palette, click **Source**.
2. In the **Properties** panel, on the **General** tab, enter a name and description.
3. Click the **Source** tab to configure source details.
4. Specify an SAP Table connection as the source object connection.
5. Specify the source type as **Single Object** and click **Select**.
6. In the **Select Source Object** dialog box, select the CDS view object:

The following image displays a CDS view object:

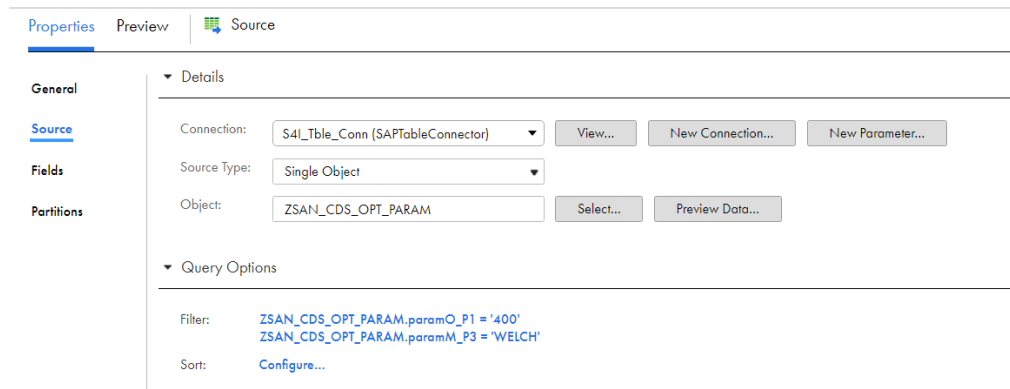


7. When you select a CDS view, on the **Fields** tab, you can view the mandatory and optional parameters:



8. Click **Query Options** in the **Source** tab to specify any filter and sort options for the CDS view:

The following image shows the basic filter options configured for the CDS view:



9. Click **Advanced** to specify the advanced source properties.

Configure an ABAP CDS view as a lookup

You can configure an uncached lookup in a mapping to look up data in an ABAP CDS view.

1. From the **Transformation** palette, add a lookup.
2. In the **Properties** panel, on the **General** tab, enter a name and description.
3. On the **Lookup Object** tab, configure the lookup object details.
 - a. Specify an SAP Table connection for the lookup object.
 - b. Specify the source type as **Single Object**.
 - c. In the **Lookup Object** field, click **Select**, and then select the CDS view object as the lookup object.

The screenshot shows the 'Properties' panel for a 'Lookup' transformation. The 'Lookup Object' tab is selected. The 'Lookup Object Details' section contains the following fields:

- Connection:** S4_Tble_Conn (SAPTableConnector) [View... New Connection... New Parameter...]
- Source Type:** Single Object
- Lookup Object:** ZSAN_SAMPLE_VIEW_EMP [Select... Preview Data...]
- Multiple Matches:** Return all rows

The left sidebar shows the 'Lookup Object' tab is active.

4. On the **Lookup Condition** tab, specify the lookup condition:

The screenshot shows the 'Properties' panel for a 'Lookup' transformation. The 'Lookup Condition' tab is selected. The 'Lookup Condition' dropdown is set to 'Simple'. Below it, the 'Lookup Conditions' table is displayed:

Lookup Field	Operator	Incoming Field
EMP_DEPT_NUM	=	s1_DEPT_ID

The left sidebar shows the 'Lookup Condition' tab is active.

5. On the **Advanced** tab, do not select the **Lookup Caching Enabled** checkbox, and then specify the lookup properties:

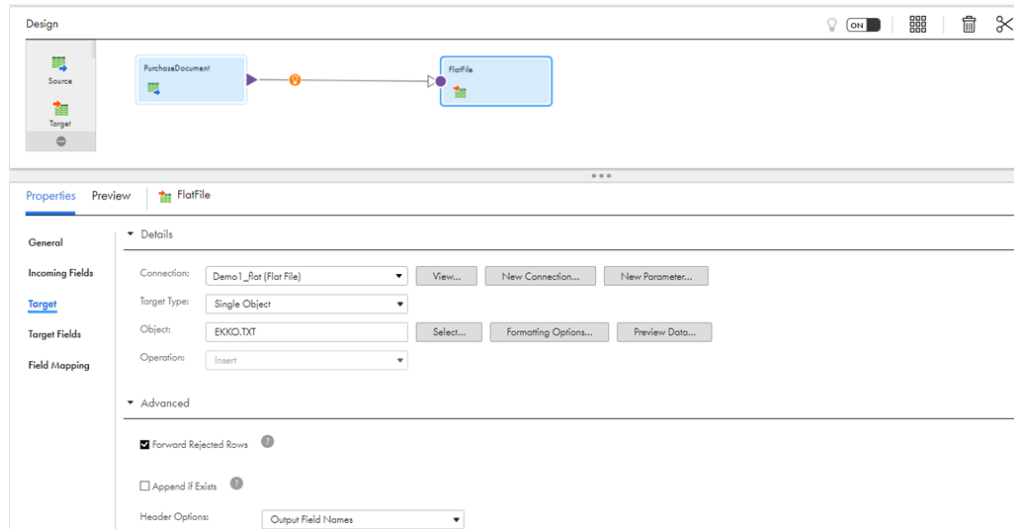
The screenshot shows the 'Properties' panel for a 'Lookup' transformation. The 'Advanced' tab is selected. The 'Tracing Level' is set to 'Normal'. The 'Lookup Caching Enabled' checkbox is unchecked. The 'Lookup Cache Directory Name' is set to '\$PMCacheDir'. The 'Cache File Name Prefix' is empty. The 'Re-cache from lookup source' checkbox is unchecked. The 'Lookup Data Cache Size' and 'Lookup Index Cache Size' are both set to 'Auto'.

Step 3: Configure the flat file target

1. To add a flat file Target transformation, on the **Transformation** palette, click **Target**.
2. On the **General** tab, enter a name and description.

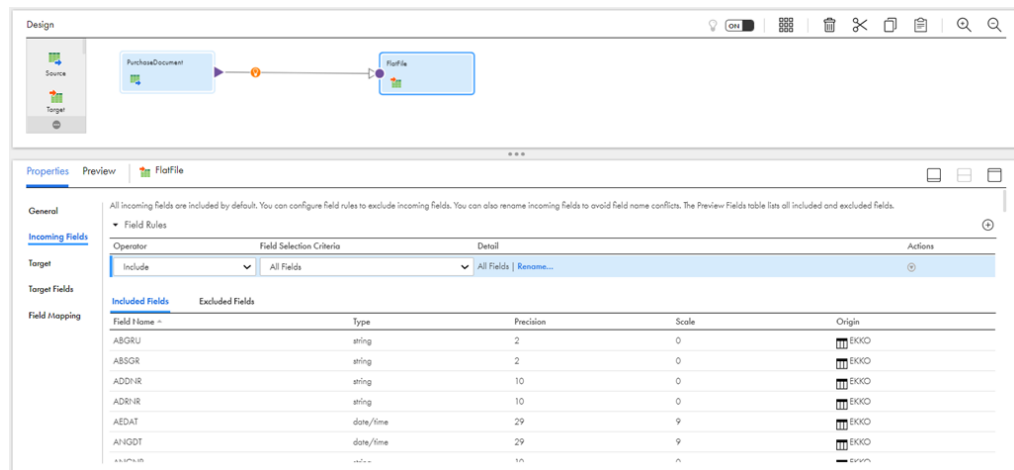
3. Draw a link to connect the Source transformation to the Target transformation.
4. Click the **Target** tab to configure the flat file target details.
5. Specify a flat file connection as the target connection.
6. Select the target type as **Single Object** and click **Select**.
7. Specify a flat file object.

The following image shows the target details:



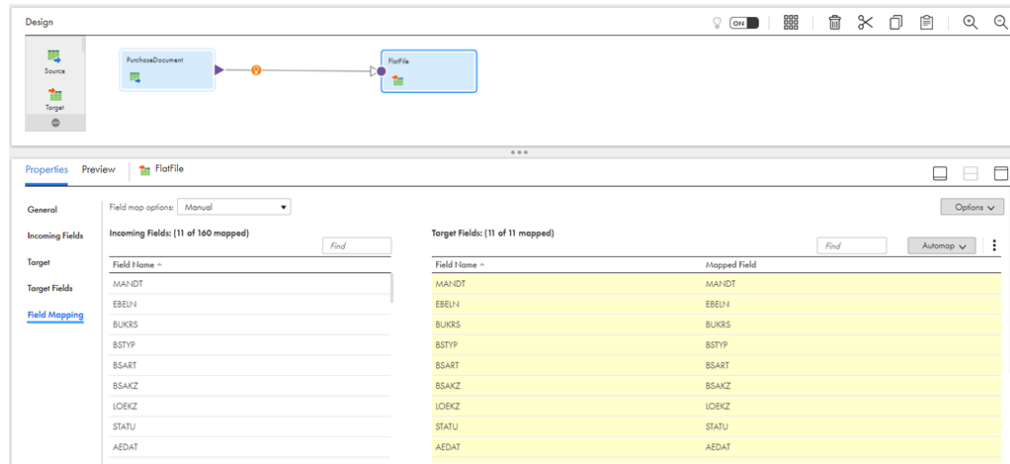
8. To preview fields, click **Incoming Fields**.

The following image shows the incoming field details:



- Click **Field Mapping** and map the fields that you want to write to the target.

The following image shows the field mapping details:



Step 4: Save the mapping and create a mapping task

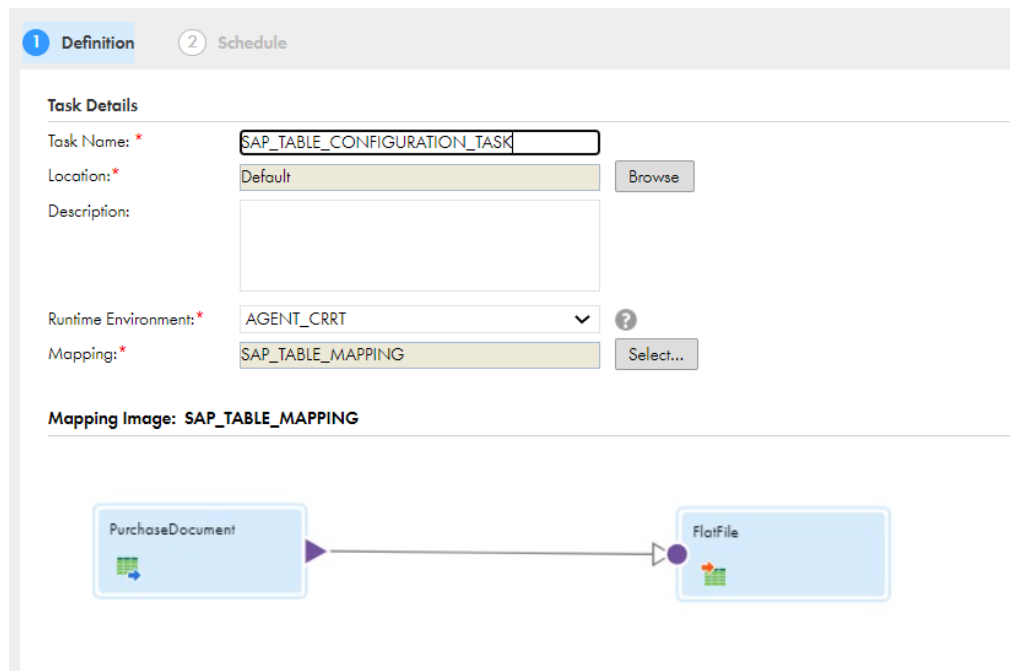
- Click **Save > Save and New Configuration Task**.

The **New Mapping Task** page appears.

- Enter a name and description for the task.
- Select the runtime environment that contains the Secure Agent you want to use to access SAP tables.

The following image shows the mapping task details:

New MappingTask5



- Click **Next** to configure the schedule and advanced options.
- Save and run the mapping task.

Part V: Data Integration using BAPI/RFC functions

This part contains the following chapters:

- [BAPI/RFC mapplets, 114](#)
- [Mapping and mapping tasks using BAPI/RFC functions, 119](#)

CHAPTER 8

BAPI/RFC mapplets

This chapter includes the following topics:

- [BAPI/RFC mapplets overview, 114](#)
- [BAPI/RFC mapplet parameters, 115](#)
- [Target object for BAPI/RFC error output, 118](#)
- [Rules and guidelines for BAPI/RFC mapplets in mappings, 118](#)

BAPI/RFC mapplets overview

You can generate SAP BAPI/RFC mapplets in Data Integration.

The BAPI/RFC mapplet includes a BAPI/RFC transformation. The BAPI/RFC transformation makes BAPI/RFC calls in SAP. BAPI/RFC calls include requests to the SAP system, such as creating, changing, or deleting data in SAP applications. To perform these tasks, BAPI/RFC functions use function parameter values.

Configuring SAP BAPI Connector as a Business Service

You can configure SAP BAPI Connector as a business service within a mapping or a mapping task for SAP BAPI data integration.

For more information about configuring SAP BAPI Connector as a business service within a mapping or a mapping task, see the Informatica How-To Library article "How to Configure SAP BAPI Connector as a Business Service in Cloud Data Integration":

<https://docs.informatica.com/integration-cloud/cloud-data-integration-connectors/h2l/how-to-configure-sap-bapi-connector-as-a-business-service-in-clo/abstract.html>

BAPI/RFC mapplet parameters

BAPI/RFC functions use function parameter values to perform tasks. A BAPI/RFC mapplet includes input and output groups based on the BAPI/RFC transformation.

Function Parameters

BAPI/RFC functions can have the following parameters:

Function Parameter	Description
Scalar input parameters.	Scalar input values. Some BAPI functions require scalar input values to perform tasks such as changing data.
Scalar output parameters.	Scalar output values that a BAPI function returns after performing a task.
Table parameters.	SAP structures with more than one row. Table parameters can be input, output, or both. Input table parameters pass table input values to a BAPI/RFC function. For example, some BAPI/RFC functions require table inputs to change data.

Input and Output Groups

The BAPI/RFC transformation can contain the following groups:

Group Name	Description
Scalar input	Input group for scalar parameters. Contains a field for each scalar input parameter. The group name is SCALAR_INPUT and the field names are SI_<FieldName>.
Table input	One group for each table parameter. The fields represent import structures. The group name is TABLE_INPUT_<structure name> and field names are TI_<StructureName>_<FieldName>.
Scalar output	Output group for scalar parameters. Contains a field for each scalar output parameter. The group name is SCALAR_OUTPUT and field names are SO_<FieldName>.
Table output	One group for each table parameter. The fields represent output structures. The group name is TABLE_OUTPUT_<structure name> and field names are TO_<StructureName>_<FieldName>.
Error output	Passes data from data conversion errors and invalid BAPI/RFC calls. Map the error output field to a target to see error messages about data conversion and BAPI/RFC calls.

BAPI/RFC parameter properties

When you generate a BAPI/RFC mapplet, you can view the parameter properties and return structures.

You can also change the direction of the BAPI/RFC table parameters. The direction of the table parameters determine which groups in the transformation are input groups and which are output groups.

If the BAPI return structure is custom, you can edit the return structure properties that you selected during import for reusable BAPI/RFC transformations. Otherwise, you can view the BAPI/RFC return structure parameters.

The following table describes the BAPI/RFC function parameter properties:

Parameter	Description
Name	Name of the export, import, and table parameters and columns.
Associated Type	Definition of the parameter in SAP.
Short Description	Short description of the export, import, and table parameters and columns.
Optional	Indicates if the Secure Agent should pass a value to the parameter when it calls the BAPI.
Direction	Indicates if the parameter requires input or provides output. Values are: Input, Output, Both, or None.
Datatype	Object data type.
Precision	Object precision.
Scale	Object scale.
Default	Default value of the parameter in SAP, if any. SAP uses the default value when the Secure Agent does not pass a value to SAP.

The following table describes the parameter properties in the Return Structure tab:

Return Structure Parameter	Description
Return Structure	Return parameter name to determine the status of function calls. Value is RETURN if the BAPI contains a default return structure. If the BAPI does not contain a default return structure, select any table output parameter or scalar output parameter of type STRUCTURE. Default is None.
Status Field	Required if you select a value for the return structure. Select a field from the structure for status. If you select None for the return structure, this parameter is blank.
Text Field	Required if you select a value for the return structure. Select a field from the structure for status messages. If you select None for the return structure, this parameter is blank.
Status Indicator For Warning	Enter an indicator message for warning. If you select None for the return structure, the value is W. Default is W.
Status Indicator for Error	Enter an indicator message for error. If you select None for the return structure, the value is E. Default is E.
Status Indicator for Abort	Enter an indicator message for abort. If you select None for the return structure, the value is A. Default is A.

BAPI/RFC functions with nested structures

You can import metadata for a BAPI/RFC functions with nested structures.

A BAPI/RFC transformation includes multiple groups. When a BAPI function contains a nested structure, ports for the input and output groups in a BAPI/RFC transformation use the following naming convention:

```
<group_name>_<parameter_name>_<field name>
```

For example:

```
SCALAR_INPUT_PARAM1_FIELD1
```

If there are multiple input or output structures, the BAPI/RFC transformation includes each structure parameter name in the port names. For example, BAPI Z_TST2 has the parameter INPUT1, which is of the type ZTYPE1. ZTYPE1 has several components such as FIELD1 and FIELD2. FIELD2 is a component of the type structure. It contains field F1. The naming convention in the BAPI/RFC transformation for FIELD 1 is:

```
SCALAR_INPUT_INPUT1_FIELD1
```

The naming convention in the BAPI/RFC transformation for the field F1 is:

```
SCALAR_INPUT_INPUT1_FIELD2_F1
```

System variables

SAP uses system variables to set default values for some BAPI import parameters. The variables provide information, such as current date and time for the operating system on which SAP runs. System variables start with "SY-". For example, SY-DATLO represents the local date of the SAP system.

The Secure Agent provides values for some system variables to define default input values for BAPI/RFC parameters. The Secure Agent uses the values as default input values for some ports of BAPI/RFC transformations. The Secure Agent uses the default values when there is no input for a port or when the port is not connected to an upstream transformation or source.

You can use the following system variables:

System Variable Name	Description
SY-LANGU	Log in language from the SAP application connection properties.
SY-MODNO	RFC handle value.
SY-MANDT	Value taken from the SAP application connection properties.
SY-DATUM	Local date on the Security Agent machine processing the data.
SY-UZEIT	Local time on the Security Agent machine processing the data.
SY-UNAME	Logon user ID from the SAP application connection properties.
SY-HOST	SAP host name from the SAP application connection properties.

Integration ID in BAPI/RFC mapplet

The Integration ID field is a key field in the BAPI mapplet. Each BAPI/RFC mapplet includes an Integration ID input field and output field.

When you run a mapping with a BAPI/RFC mapplet, the Secure Agent makes a BAPI/RFC call to SAP to process the data. When it reaches the end of file, the Secure Agent makes the BAPI/RFC call. Depending on the mapping configuration, the Secure Agent can also issue a commit.

The BAPI/RFC call is based on the input data of the Integration ID ports. The Secure Agent makes one call to SAP for each Integration ID. Pass a value to the Integration ID ports in the scalar input group and all mandatory table input groups of the BAPI/RFC mapplet.

Note: You must map the Integration ID input field even when a BAPI or RFC does not require other input fields.

If the BAPI/RFC call fails or if there is a data conversion error, SAP passes the data for the integration ID in comma-separated format to an error output group. If the mapping contains a target instance that is connected to the error output group, the Secure Agent writes the data to the target.

Target object for BAPI/RFC error output

To receive input data from a BAPI/RFC function call or data conversion errors from SAP, you can map a target transformation to a BAPI/RFC mapplet.

Create a target transformation with a column of the String data type and precision of 65535. Connect the column in the target object to the Error Output Group in the BAPI/RFC mapplet. The Secure Agent writes the error output data up to 65,535 characters to the target in comma-delimited format. If the error output data is longer than 65,535 characters, the Secure Agent truncates the data.

Rules and guidelines for BAPI/RFC mapplets in mappings

When you configure a mapping with a BAPI/RFC mapplet, use the following rules and guidelines:

- Pass a value to the Integration ID ports in the scalar input group and all mandatory table input groups of the BAPI/RFC transformation.
- Add a target object if you want to receive BAPI/RFC function call errors from the BAPI error group.

Use the following guidelines when passing data to BAPI/RFC function input parameters:

- When the function input parameter data type is INT1 or NUMC, provide positive values for the function input.
- When the source input data for a BAPI/RFC function is of the integer data type, do not use string data in the source transformation. Otherwise, the mapping fails.
- If the input data for a BAPI/RFC function mapping has a higher scale than the SAP metadata specification, the Secure Agent rounds the data to comply with the SAP metadata. When you run a mapping in high precision mode, the mapping can fail due to overflow if the round-off data cascades to the precision digits. For example, the data type and precision for a BAPI/RFC function parameter is DEC (6,5). The input data that you pass to the function parameter is 9.99999. When the Secure Agent processes the input data, it rounds the input data to 10, which is not compatible with the SAP metadata. The mapping fails.

CHAPTER 9

Mapping and mapping tasks using BAPI/RFC functions

This chapter includes the following topics:

- [Mapping and mapping tasks using BAPI/RFC functions overview, 119](#)
- [Generating a BAPI/RFC mapplet, 120](#)
- [Configuring a mapping with a BAPI/RFC mapplet, 120](#)
- [Mappings with BAPI/RFC function example, 121](#)

Mapping and mapping tasks using BAPI/RFC functions overview

You can generate a BAPI/RFC mapplet in Data Integration. You can then configure a mapping with the mapplet to manage data in SAP systems.

For example, to update sales order data in SAP, generate a BAPI/RFC mapplet from the BAPI_SALESORDER_CHANGE function and configure a mapping using the mapplet.

You can configure a mapping with a BAPI/RFC mapplet to pass input data to BAPI/RFC function input parameters.

To access the BAPI/RFC functionality through Data Integration, perform the following tasks:

1. Generate a BAPI/RFC mapplet in Data Integration.
2. Configure a mapping using the generated BAPI/RFC mapplet. Map the Integration ID field and other inputs and outputs. Save and run the mapping or create a mapping task using this mapping.

Configuring SAP BAPI Connector as a Business Service

You can configure SAP BAPI Connector as a business service within a mapping or a mapping task for SAP BAPI data integration.

For more information about configuring SAP BAPI Connector as a business service within a mapping or a mapping task, see the Informatica How-To Library article "How to Configure SAP BAPI Connector as a Business Service in Cloud Data Integration":

<https://docs.informatica.com/integration-cloud/cloud-data-integration-connectors/h2l/how-to-configure-sap-bapi-connector-as-a-business-service-in-clo/abstract.html>

Generating a BAPI/RFC mapplet

You can generate a BAPI/RFC mapplet in Data Integration and use the mapplet in a mapping.

Perform the following steps to generate a BAPI/RFC mapplet:

1. To create a mapplet, click **Data Integration > New > Mapplets > Mapplet - SAP** and then click **Create**.
To edit a mapplet, on the **Explore** page, navigate to the mapplet. In the row that contains the mapplet, click **Actions** and select **Edit**.

2. Enter a unique name for the BAPI/RFC mapplet.
3. Optionally, enter a description for the BAPI/RFC mapplet that you want to generate.
4. Select the transformation type as **BAPI**.
5. Select the BAPI/RFC connection that you want to use.
6. Select the scope of the transformation.

For real-time processing, select the transformation scope as **Transaction**. For batch processing and validation in a non-production environment, select the transformation scope as **All Input**.

7. Enter the name of the BAPI/RFC function.

You can also search for a BAPI/RFC function by entering % as a wildcard character along with the search string. For example, to search for all BAPI/RFC functions whose names start with the term *Customer*, enter the search string as *Customer%*. To search for all BAPI/RFC functions whose names end with the term *Customer*, enter the search string as *%Customer*.

8. Click **Get Objects**.

The **Select Source Object** dialog box appears displaying the search results. You can drill down the search results further by entering a search string in the **Select Source Object** dialog box.

9. Click the required BAPI/RFC function name and click **Select**.

The import, export, and table parameter details of the BAPI/RFC function appear.

10. Specify the direction for the tables to indicate if the table parameters in the BAPI are input, output, or both.
11. Click **Save**.

The mapplet for the specified BAPI/RFC function is created. You can create a mapping for the generated mapplet.

Configuring a mapping with a BAPI/RFC mapplet

1. To create a mapping, click **Data Integration > New > Mappings**. Select **Mapping** and click **Create**.
2. Enter a name and description for the mapping, and click **OK**.
You can use alphanumeric characters and underscores (_) in the mapping name.
3. To configure a source, on the **Transformation** palette, click **Source**.
4. In the **Properties** panel, on the **General** tab, you can enter a name and description.
5. Click the **Source** tab and configure the source details.

Source details and advanced source properties appear based on the connection type.

6. To add a BAPI/RFC mapplet transformation, on the **Transformation palette**, click Mapplet.
 - a. On the **General** tab, enter a name and description for the mapplet.
 - b. Draw a link to connect the previous transformation to the mapplet transformation.
 - c. On the **Mapplet** tab, click **Select**.

The **Select Mapplet** dialog box appears.
 - d. Specify a BAPI/RFC mapplet that you generated in Data Integration and click **OK**.
 - e. Click **Connection** to specify an SAP RFC/BAPI Interface connection. You can create a connection, select a connection, or specify a parameter name for the connection.
 - f. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.
 - g. Click **Field Mapping** and map the incoming source fields with the Integration ID in the BAPI/RFC mapplet.
 7. To add any other transformation, on the **Transformation palette**, click the transformation name. Or, drag the transformation onto the mapping canvas.
 - a. On the **General** tab, enter a name and description for the transformation.
 - b. Draw a link to connect the previous transformation to the transformation.

When you link transformations, the downstream transformation inherits the incoming fields from the previous transformation.

For a Joiner transformation, draw a master link and a detail link.
 - c. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.
 - d. Configure additional transformation properties, as needed.

The properties that you configure vary based on the type of transformation you create.
 - e. To add another transformation, repeat these steps.
 8. To add a Target transformation, on the **Transformation palette**, click **Target**.
 - a. On the **General** tab, you can enter a name and description.
 - b. Draw a link to connect the previous transformation to the Target transformation.
 - c. Click the **Target** tab and configure target details. If necessary, configure the advanced target properties.

Target details and advanced target properties appear based on the connection type.
 - d. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.
 - e. Click **Field Mapping** and map the fields that you want to write to the target.
 - f. To add another Target transformation, repeat these steps.
 9. Save and run the mapping or save and create a mapping task.
- For more information about transformations, see *Transformations*.

Mappings with BAPI/RFC function example

You can use the `bapi_salesorder_createfromdat1` BAPI function to create sales order details for a customer in your organization.

In this example to create a sales order, perform the following tasks:

Step1: Generate a BAPI/RFC maplet in Data Integration for the bapi_salesorder_createfromdat1 BAPI function.

Log in to Data Integration and generate a BAPI/RFC maplet that contains the metadata of the bapi_salesorder_createfromdat1 BAPI function.

Step: 2 Configure a mapping using the generated maplet.

Perform the following steps to configure a mapping:

1. Specify source objects to enter the order header data from the ORDER_HEADER_IN structure, the partner data using the ORDER_PARTNERS table, and item data using the ORDER_ITEMS_IN table as input parameters.
2. Add the Maplet transformation. Draw a link to connect the flat file Source transformation to the Maplet transformation. Draw the following links:
 - ORDER_HEADER_IN source object to the Scalar_Input input port of the BAPI maplet.
 - ORDER_ITEMS_IN source object to the Table_Input_Order_Items_IN input port of the BAPI maplet.
 - ORDER_PARTNERS source object to the Table_Input_Order_partners input port of the BAPI maplet.
3. Configure the maplet transformation.
 - a. Select the generated maplet. Verify that you specify an SAP RFC/BAPI Interface connection for the maplet.
 - b. Map the incoming source fields with the BAPI parameter properties.
4. Configure a flat file object to which you can write the sales order details. Draw a link to connect the Table Output in the Maplet transformation to the flat file Target transformation. Create multiple flat file target objects to write the sales order. Create the following target objects and map them to the associated output ports in the BAPI maplet:
 - ORDER_CFGS_BLOB, ORDER_CFGS_INST, ORDER_CFGS_PART_OF, ORDER_CFGS_REF, and ORDER_CFGS_VALUE to write item configuration data.
 - ORDER_ITEMS_OUT to write detailed item data.
 - ORDER_CCARD to write the credit card details.
 - ORDER_SCHEDULE_EX to write the structure of VBEP with English field names.
 - Scalar_Output to write the Scalar_Output from the maplet.
 - Error_Output to write the Error_Output from the maplet.

Step 1: Generating a BAPI/RFC mapplet in Data Integration for the BAPI_SALESORDER_CREATEFROMDAT1 BAPI function

Perform the following steps to generate a BAPI/RFC mapplet:

1. To create a mapplet, click **Data Integration > New > Mapplets > Mapplet - SAP** and then click **Create**.
To edit a mapplet, on the **Explore** page, navigate to the mapplet. In the row that contains the mapplet, click **Actions** and select **Edit**.

The **New SAP Mapplet** page appears. The following image shows the **New SAP Mapplet** page:

Mapplet Details

Mapplet Name: ?

Location: Browse

Description:

Transformation Type: ☒ BAPI ☐ IDoc ?

Connection: View... New...

Transformation Scope: ?

Select the BAPI/RFCs to be imported

BAPI/RFC Object: Get Objects

Set Parameters

	Name	Associated Type	Short Description	Optional	Direction	Datatype	Precision	Scale	Default
▶	Import								
▶	Export								
▼	Tables								
▶	ORDER_ITEMS_IN	BAPIITEMIN	Item Data Input	No	Input				
▶	ORDER_PARTNERS	BAPIPARTNR	Partners	No	Input				
▶	ORDER_ITEMS_OUT	BAPIITEMEX	Item Data Output	Yes	Output				
▶	ORDER_CFGS_REF	BAPICUCFG	Configuration: Reference Data	Yes	Output				
▶	ORDER_CFGS_INST	BAPICUINS	Configuration: Instances	Yes	Output				

2. Enter a unique name for the BAPI/RFC mapplet.
3. Optionally, enter a description for the BAPI/RFC mapplet you want to generate.
4. Select the transformation type as **BAPI**.
5. Select the BAPI/RFC connection that you want to use.
6. Select the scope of the transformation.

In real time, select the transformation option as Transaction. For batch processing and validating in non-production environment, select ALL INPUT as the transformation scope.

7. Enter the name of the BAPI/RFC function.
Note: Verify that you enter the exact name of the BAPI/RFC function that you want to retrieve.
8. Click **Get Objects**.

You can view the import, export, and table parameter details of the BAPI/RFC function.

9. Specify the direction for the tables to indicate if the table parameters in the BAPI are input, output, or both.
10. Click **OK**.

The mapplet for the specified BAPI/RFC function is created. You can create a mapping for the generated mapplet.

Step 2: Configuring a mapping with the bapi_salesorder_createfromdat1 mapplet

1. To create a mapping, click **Data Integration > New > Mappings**. Select **Mapping** and click **Create**.
2. Enter a name and description for the mapping, and click **OK**.
3. To configure the flat file source, on the **Transformation** palette, click **Source**.
4. In the **Properties** panel on the **General** tab, enter a name and description.
5. Click the **Source** tab and configure the source details.
 - a. Select a flat file connection.
 - b. Select Single Object as the **Source Type**.
 - c. Click **Select** to specify a flat file that contains the source fields.

The following image shows the flat file source details:

The screenshot shows the 'Source' tab of the configuration dialog. The 'Details' section is expanded, showing the following fields and buttons:

- Connection:** A dropdown menu showing 'Demo1_Flat (Flat File)' with buttons 'View...', 'New Connection...', and 'New Parameter...'.
- Source Type:** A dropdown menu showing 'Single Object'.
- Object:** A text field containing 'scalar_salesorder_in.csv' with buttons 'Select...', 'Formatting Options...', and 'Preview Data...'.

Below the 'Details' section are two collapsed sections: 'Query Options' and 'Advanced'.

6. Add order header, order items, and order partners as flat file source objects for the mapping.
7. To add a BAPI/RFC mapplet transformation, on the **Transformation palette**, click Mapplet.
 - a. On the **General** tab, enter a name and description for the mapplet.
 - b. Draw a link to connect the flat file Source transformation to the Mapplet transformation.
 - c. On the **Mapplet** tab, click **Select**.
The **Select Mapplet** dialog box appears.
 - d. Select the `bapi_salesorder_createfromdat1` mapplet and click **OK**.
 - e. Click **Connection** to specify an SAP RFC/BAPI Interface connection.

The following image shows the `bapi_salesorder_createfromdat1` mapplet details:

The screenshot shows the 'Mapplet' tab of the configuration dialog. The 'General' section is expanded, showing the following fields and buttons:

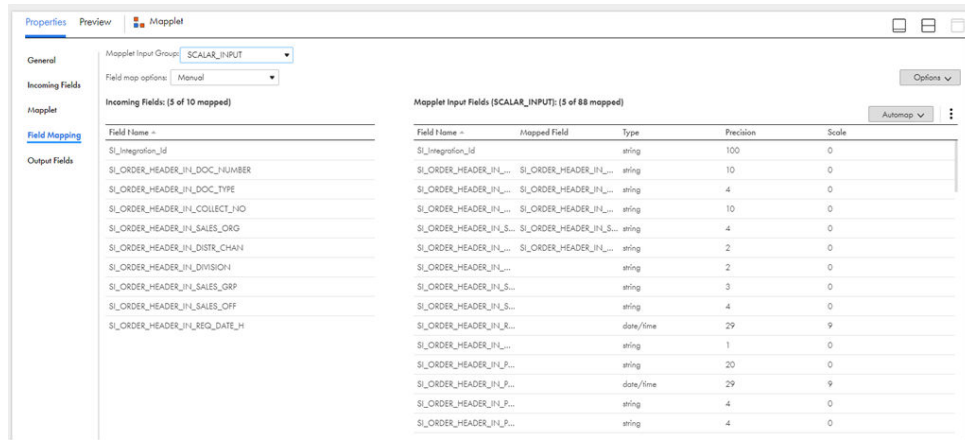
- Mapplet:** A text field containing 'Default\BAPI_SALESORDER_CREATEFROMDAT1' with buttons 'Select...', 'View', and 'Synchronize'.
- Description:** A text field.
- Type:** A dropdown menu showing 'Active'.

Below the 'General' section is the 'Connections' section, which contains a table:

Connection Name (Mapplet)	Used In	Connection	View
BAPI/RFC connection	Transform_Transform(Custom Transform...	S41_Mapplet	

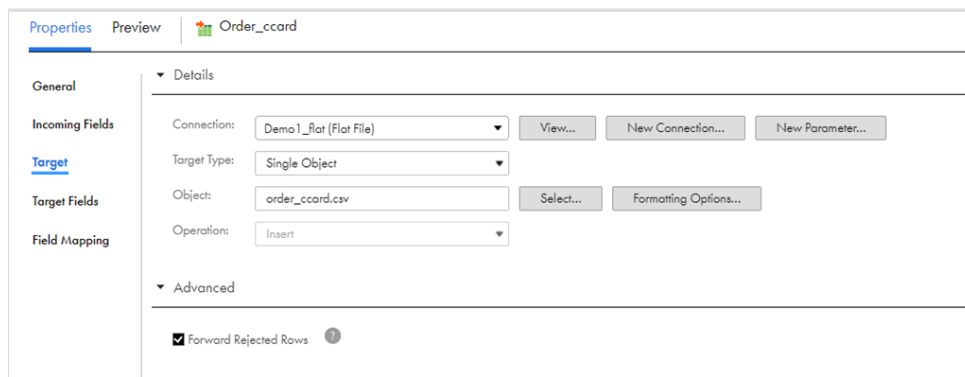
- f. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.

- g. Click **Field Mapping** and map the incoming source fields with the appropriate maplet input fields. The following image shows the field mapping of the incoming source fields with the maplet input fields:



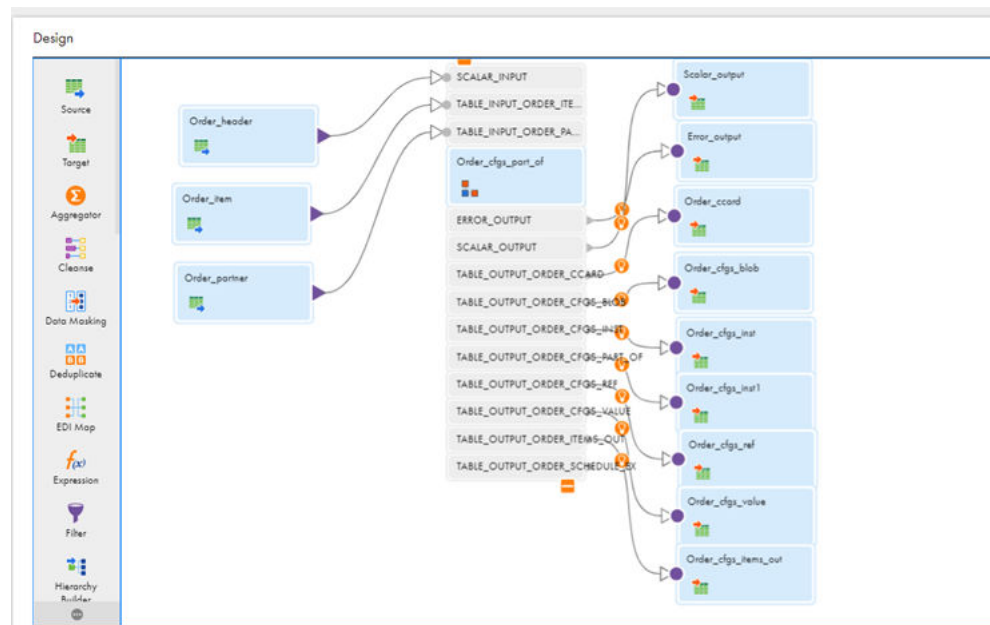
8. To add a flat file target, on the **Transformation palette**, click **Target**.
9. On the **General** tab, enter a name and description for the target.
10. Click the **Target** tab and configure target details.
 - a. Select a flat file connection for the target.
 - b. Select Single Object as the **Source Type**.
 - c. Click **Select** to specify the target object.
The **Target Object** dialog box appears.
 - d. Select the flat file object, and click **OK**.
 - e. Optionally, you can choose to forward rejected rows in the Advanced Target options.
 - f. Repeat the above steps to add all the flat file target objects.

The following image shows the target transformation details:



11. Draw a link to connect the output ports in the Mapplet transformation to the flat file Target transformation.

The following image shows the mapping configured for the bapi_salesorder_createfromdat1 mapplet:



12. Save and run the mapping.

Part VI: Data Integration Using IDocs

This part contains the following chapters:

- [IDoc mapplets, 128](#)
- [Mapping and mapping tasks using IDocs, 137](#)

CHAPTER 10

IDoc mapplets

This chapter includes the following topics:

- [IDoc mapplets overview, 128](#)
- [Segments and groups, 128](#)
- [Outbound mapplet, 131](#)
- [Inbound mapplet, 132](#)
- [Importing IDoc metadata, 135](#)

IDoc mapplets overview

You can import an IDoc as a mapplet using the SAP Metadata utility. An IDoc contains a hierarchical structure consisting of segments. Each segment is an SAP structure defined in the SAP system.

An IDoc has header and data record components. The header component contains control information, such as creation date and status. The control information is in an SAP structure called EDIDC. The data records are in an SAP structure called EDIDD.

Segments and groups

An IDoc is a hierarchical structure that contains segments. A segment can be a parent or child. A child segment depends on another segment. A parent segment contains child segments. A parent segment can be a child of another segment.

IDoc segments are organized into groups. The following rules determine the group to which a segment belongs:

- A parent segment starts a new group. For example, in the MATMAS04 IDoc, the E1MARCM segment contains a child and therefore starts a group.
- A child segment that is not a parent belongs to the group that is started by its immediate parent. For example, in the MATMAS04 IDoc, the E1MARA1 segment does not contain a child and therefore belongs to the group of its parent E1MARAM.
- A group can also be a parent or a child.

Segment and group status

After you specify the message and doc type in the SAP Metadata utility, you can view the segments and groups in the IDoc.

Segments and groups can be required or optional. In an IDoc mapplet, a required segment must exist in the IDoc only if its group, its parent groups, and its parent segments are required or selected. For example, the E1MARAM group is required. Therefore, its required child segment E1MAKTM must exist in the IDoc while its optional child segment E1MARA1 does not have to exist in the IDoc.

If a required segment belongs to an optional group that is not selected, then the segment does not have to exist in the IDoc. For example, the E1MARCM group is optional. Therefore, the required E1MARCM segment also becomes optional.

When a segment is required, the Segment Status column is selected. When a group is required, the Group Status column is selected.

For example, specify the message type as MATMAS, the IDoc Type as MATMAS04, and click Fetch. You can view the segments and groups in the IDoc.

The following table describes how you can use the Segment Status and Group Status columns to understand which segments are required in the MATMAS04 IDoc:

Segment Name	Segment Group	Segment Status	Group Status	Required in IDoc
E1MARAM	E1MARAM	Required	Required	Required
E1MARA1	E1MARAM	Optional	Optional	Optional
E1MARCM	E1MARCM	Required	Optional	Optional

The following image shows that the E1MARAM segment and the E1MARAM group are required:

The screenshot displays the SAP Metadata utility interface. The top table lists segments and groups with their status. The bottom table lists fields with their data types and precision.

Segment Name	Description	Select	Segment Status	Group Status	Min. Occurs	Max. Occurs
E1MARAM	Master material general data (MARA)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	1
E1MARA1	Additional Fields for E1MARAM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	1
E1MAKTM	Master material short texts (MAKT)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	99
E1MARCM	Master material C segment (MARC)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	1
E1MARCL	Additional Fields for E1MARCM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	1
E1MARDM	Master material warehouse/batch segment (MARD)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	9999
E1MFHMM	Master material production resource/tool (MFHM)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	1
E1MPGDM	Master material product group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	1
E1MPOPM	Master material forecast parameter	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	1
E1MPRWM	Master material forecast value	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	9999999999

Name	Description	SAP Datatype	Precision	Scale
MSGFN	Function	CHAR	3	0
MATNR	Material Number	CHAR	18	0
ERSDA	Creation date	DATS	8	0
ERNAM	Name of Person who Created the Object	CHAR	12	0
LAEDA	Date of Last Change	DATS	8	0
AENAM	Name of Person Who Changed Object	CHAR	12	0
PSTAT	Maintenance status	CHAR	15	0
LVORM	Flag Material for Deletion at Client Level	CHAR	1	0
MTART	Material type	CHAR	4	0
MBRSH	Industry sector	CHAR	1	0

Segment Definition: E2MARAM005 Total Fields: 109 Select Location: C:\

IDocs properties

When you fetch an IDoc in the SAP Metadata utility, you can view all the IDoc segments. Select a segment to view the fields in the segment.

IDocs Properties

The following table describes the IDocs properties that you can view and specify in the SAP Metadata utility:

Property	Description
Message Type	Application messages that classify categories of data. For example, ORDERS and MATMAS (Material Master).
IDoc Type	Data structure associated with the message type. For example, MATMAS01, MATMAS02 for MATMAS. IDocs contain the data associated with the message type.
Control Page	Displays the control record. You can add partner profiles to the control record as key value pairs. You can also update and delete any partner profiles associated with the control record.
Select All Segments	Includes all segments in the IDoc mapplet.
Deselect All Segments	Removes all selected segments except required segments from the IDoc mapplet.
Select Transformation	Indicates the type of transformation you want to use to generate the IDoc mapplet. Select one of the following values: <ul style="list-style-type: none">- Prepare. Select to generate a mapplet that writes source data as an IDoc message.- Interpreter. Select to generate a mapplet that reads IDoc messages.- Both. Select to generate a mapplet that read IDoc messages and another mapplet to write IDoc messages.
Transformation Scope	Indicates how the Secure Agent applies the transformation logic to incoming data. Select one of the following values: <ul style="list-style-type: none">- Transaction- All Input Choose Transaction to apply the transformation logic to all rows in a transaction. Select Transaction when the results of the transformation depend on all rows in the same transaction, but not on rows in other transactions. When you select Transaction, associated mappings can run in real time. Choose All Input to apply the transformation logic to all incoming data, and to drop the incoming transaction boundaries. Select All Input when the results of the transformation depend on all rows of data in the source. Default is All Input.
Segment Name	Segment names of the IDoc type.
Description	Description of the segments.
Select	Selects the data segments to include in the transformation. When you select a segment, the parent segments and all required child segments are also selected. When you clear a segment, all child segments are also cleared.
Segment Status	When selected, indicates that the segment is required in the IDoc mapplet.
Group Status	When selected, indicates that the group is required in the IDoc mapplet.

Property	Description
Min. Occurs	Minimum number of occurrences of the segment in an IDoc.
Max Occurs	Maximum number of occurrences of the segment in an IDoc.

Segment Fields

Select a segment name to view the field names of the segment.

The following table describes the segment field details:

Field	Description
Name	Field name of a segment.
Description	Description of the field.
SAP Datatype	SAP data type of the field.
Precision	Precision of the field.
Scale	Scale of the field.

Outbound mapplet

You can capture changes to the master data or transactional data in the SAP application database in real time.

When data in the application database changes, the SAP system creates IDocs to capture the changes and sends the IDocs to Data Integration. You can use the IDoc Reader connection to read the IDoc message in real time as they are generated by the SAP system.

If the Secure Agent is not running when the SAP system sends outbound IDocs, the Secure Agent does not receive the IDocs. However, the SAP system stores the outbound IDocs in EDI tables, which are a staging area for guaranteed message delivery. You can configure the SAP system to resend the IDocs by configuring the tRFC port used to communicate with the Secure Agent. When you configure the port, you can enable background processes in SAP that try to resend the IDocs to the Secure Agent a set number of times.

To generate the outbound mapplet to read IDoc messages from SAP system, use the IDoc Interpreter when you import the IDoc metadata. Import the outbound mapplet to Data Integration and configure an outbound mapping.

Outbound mapplet ports

An outbound IDoc mapplet contains predefined ports. You cannot edit the ports.

The following table describes the mapplet ports:

Port Name	Description
Basic IDoc Type	Basic IDoc type name. Basic IDoc type defines the structure of an IDoc. Each basic type describes standard IDoc segments, format of data fields, and size. Basic type contains all the standard fields that are necessary for carrying out a business transaction.
Extended IDoc Type	Extended IDoc type name. IDoc extension is extension of basic type and contains additional custom IDoc segments and fields that are not available in the standard basic type.
IDocRecord	IDoc message data.
DocumentNumber	Unique message number of the IDoc.

Target object for outbound mapplet error output

You can configure an outbound IDoc mapping to write IDocs that are not valid to a relational or flat file target. To write IDocs that are not valid to a relational or flat file target, connect the IDoc_Interpreter_Error_Output_Group port in the outbound mapplet to a relational or flat file target object. You must also configure the error log type session property in the **Schedule** page.

Inbound mapplet

You can synchronize transactional data in a legacy application with the data in the SAP application database.

Use an inbound SAP IDoc mapping to send the transactional data from the legacy application database to the SAP system. Data Integration extracts the data from the legacy application data source, prepares the data in SAP IDoc format, and sends the data to the SAP system as inbound IDocs using ALE. You can use the IDoc Writer connection to write inbound SAP IDoc messages to SAP systems.

To generate the inbound mapplet to write IDocs to SAP systems, use the Prepare transformations when you import the IDoc metadata. Import the inbound mapplet to Data Integration and configure an inbound mapping.

Key fields and control record fields

An IDoc mapplet includes a primary key (GPK) and a foreign key (GFK) in each segment. When you configure a mapping, integration template, or mapping task, map the primary key field, foreign key field, and any control record fields.

Note: You can enable control record fields when you import the IDoc metadata.

The Prepare transformation in the SAP IDoc Writer mapplet can have primary key and foreign key fields and other input fields, including control record fields.

The Prepare transformation has the following output fields:

- IDoc Data. Map this field to an IDoc target.
- Error IDoc Data. Map this field to see error messages about IDoc syntax/data conversion.

When you import IDoc metadata, you can add fields to a Prepare transformation. In the SAP Metadata utility, you can click Control Page and add the control record keys as key-value pairs. For example, you can add the following key-value pairs for the sender partner type and the sender partner number:

- Key: SNDPRT and Value: LS for Logical System
- Key: SNDPRN and Value: ICS

In an inbound mapping, you can pass the sender partner number to SAP. You can pass a value to the CONTROL_SNDPRN port in the control input group of the Prepare transformation. If you do not connect this port to an upstream transformation, the Secure Agent uses the partner number value of SNDPRN key you specify in the SAP Metadata utility.

IDoc primary and foreign keys

An IDoc message is organized hierarchically with one top-level parent segment and one or more second-level child segments. Second-level child segments can also have one or more third-level child segments.

To maintain the structure of the IDoc data, the Prepare transformation in the SAP IDoc Writer mapplet uses primary and foreign keys. The top-level parent segment has a primary key. Each child segment has a primary key and a foreign key. The foreign key of each child segment references the primary key of its parent segment. For example, the foreign key of a second-level child segment references the primary key of the top-level parent segment. Similarly, the foreign key of a third-level child segment references the primary key of the second-level child segment.

The Prepare transformation groups incoming IDoc data based on the values in the primary and foreign key fields. The Control Input group of the Prepare transformation represents the parent segment. All other groups of the Prepare transformation except the ErrorIDocData group represent second-level or third-level child segments. The ErrorIDocData group is used for processing invalid IDocs.

The following table shows the groups of the Prepare transformation and the fields used for the primary and foreign keys:

Groups	Field	Description
Control Input Group	GPK_DOCNUM	Primary key of the parent segment.
Child Segment 1	GPK_<Child1_name>	Primary key of Child Segment 1.
Child Segment 1	GFK_DOCNUM_<Child1_name>	Foreign key of Child Segment 1 references the primary key of the parent segment.
Child Segment A of Child Segment 1	GPK_<Child1A_name>	Primary key of Child Segment A of Child Segment 1.
Child Segment A of Child Segment 1	GFK_<Child1_name>_<Child1A_name>	Foreign key of Child Segment A of Child Segment 1 references the primary key of Child Segment 1.
Child Segment 2	GPK_<Child2_name>	Primary key of the IDoc child segment.
Child Segment 2	GFK_DOCNUM_<Child2_name>	Foreign key of Child Segment 2 references the primary key of the parent segment.

Groups	Field	Description
Child Segment B of Child Segment 2	GPK_<Child2B_name>	Primary key of Child Segment B of Child Segment 2.
Child Segment B of Child Segment 2	GFK_<Child2_name>_<Child2B_name>	Foreign key of Child Segment B of Child Segment 2 references the primary key of Child Segment 2.

Each value for the GPK_<name> field needs to be unique. Each GFK_<parent_name>_<group_name> field needs to reference the primary key of its parent segment.

For example, the following table shows the relationship of primary and foreign keys in an IDoc message named ABSEN1 with four child segments:

Group	Field	Primary/Foreign Keys
CONTROL_INPUT_ABSEN1	GPK_DOCNUM	P1
E2ABSE1	GPK_E2ABSE1	C1
-	GFK_DOCNUM_E2ABSE1	P1
E2ABSE2	GPK_E2ABSE2	C2
-	GFK_DOCNUM_E2ABSE2	P1
E2ABSE2A	GPK_E2ABSE2A	C2A
-	GFK_E2ABSE2_E2ABSE2A	C2
E2ABSE3	GPK_E2ABSE3	C3
-	GFK_DOCNUM_E2ABSE3	P1
E2ABSE3B	GPK_E2ABSE3B	C3B
-	GFK_E2ABSE2_E2ABSE2A	C3
E2ABSE4	GPK_E2ABSE4	C4
-	GFK_DOCNUM_E2ABSE4	P1

The Prepare transformation uses these primary and foreign key relationships to maintain the structure of the IDoc data. Any foreign key field that does not match the primary key of its parent segment results in an orphan row. Any primary key field that is not unique results in a duplicate row.

Verify that each IDoc message has a unique primary key for the top-level parent segment, each child segment, and that each foreign key matches the primary key of its parent.

Importing IDoc metadata

1. Navigate to the SAP Metadata utility installation directory and double-click the `SAPUtil.bat` file.
The Import SAP IDOC/BAPI/RFC wizard appears.
2. Select the SAP system to which you want to connect.
All systems specified in the `sapnwrfc.ini` file appear in the drop-down list.
3. Enter the SAP user name.
4. Enter the password associated with the SAP user.
5. Enter the client number.
6. Enter the language code.
7. Select IDoc and click **Connect**.
The connection to the SAP system is established.
8. Click **Next**.
The **Step 2: Select SAP IDoc Prepare Transformation** page appears.
9. Enter the message type and the IDoc type, and click **Fetch**.
You can view the segment details of the IDoc.
10. Select the transformation type. You can choose one of the following options:
 - To generate outbound mappings to read IDocs from an SAP system, select the Interpreter transformation.
 - To generate inbound mappings to write IDocs to an SAP system, select the Prepare transformation.
 - To generate outbound and inbound mappings, select Both.
11. Select the transformation scope. You can choose one of the following options:
 - Choose Transaction to apply the transformation logic to all rows in a transaction. Select Transaction when the results of the transformation depend on all rows in the same transaction, but not on rows in other transactions. When you select Transaction, associated mappings can run in real time. For outbound mappings, select Transaction.
 - Choose All Input to apply the transformation logic to all incoming data, and to drop the incoming transaction boundaries. Select All Input when the results of the transformation depend on all rows of data in the source.
12. Select the segments you want to include in the mapplet.
You can click **Select All Segments** to include all segments in the IDoc. Click **Deselect All Segments** to remove all selected segments except required segments from the IDoc.
13. To add other fields into the Control Record input group of a mapplet, perform the following steps:
 - a. Click **Control Page**. Add more control records if you have more than one logical system.
 - b. Select the checkbox for the field that you want to add, and then click **Partner Profile > New**.
 - c. Enter the key and value for the partner profile. The key is the field name, and the value is the partner type.
 - d. Optionally, to add a control record field to the mapplet, from the Control Record page, select the checkbox for the field you want to add. This will enable you to map the selected control record fields when you configure a mapping, integration template, or mapping task.
14. Select a directory for the output files and click **OK**.

15. Click **Finish**.

The mapplet for the specified IDoc is created in the output directory.

CHAPTER 11

Mapping and mapping tasks using IDocs

This chapter includes the following topics:

- [Mapping and mapping tasks using IDocs overview, 137](#)
- [IDoc reader sources in mappings, 138](#)
- [Importing an IDoc mapplet to Data Integration, 139](#)
- [Configuring an outbound mapping to read IDocs from SAP, 139](#)
- [Configuring an inbound mapping to write IDocs to SAP, 140](#)
- [Outbound mapping to read IDocs from SAP example, 141](#)
- [Inbound mapping to write IDocs to SAP example, 147](#)

Mapping and mapping tasks using IDocs overview

To send and read IDocs, Data Integration integrates with SAP applications using Application Link Enabling (ALE).

ALE is an SAP proprietary technology that enables data communication between SAP systems. ALE also enables data communication between SAP and external systems.

You can configure outbound mappings to read IDocs from SAP and inbound mappings to write IDocs to SAP.

To configure an outbound mapping to read IDocs from SAP, perform the following tasks:

1. Import the IDoc metadata from SAP and generate a mapplet using the SAP Metadata utility. Verify that you selected the segments and groups you want to include in the IDoc. In addition, select the Interpreter transformation.
2. Import the IDoc mapplet to Data Integration.
3. Configure an outbound mapping using the generated IDoc mapplet. Add a Source transformation to read data from the SAP system, configure the IDoc mapplet, and add a Target transformation to write the IDoc in the target object.

To configure an inbound mapping to write IDocs to SAP, perform the following tasks:

1. Import the IDoc metadata from SAP and generate a mapplet using the SAP Metadata utility. Verify that you selected the segments and groups you want to include in the IDoc. In addition, select the Prepare transformation.

2. Import the IDoc mapplet to Data Integration.
3. Configure an inbound mapping using the generated IDoc mapplet. Add a Source transformation to read data from the source system, configure the IDoc mapplet, and add a Target transformation to write the IDoc to the SAP system.

IDoc reader sources in mappings

To read IDocs from an SAP application, use an SAP IDoc Reader connection and configure the IDoc Reader source properties in the Source transformation in a mapping.

Specify the name and description of the IDoc Reader source. Configure the source and advanced properties for the source object.

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

Property	Description
Connection	Name of the source connection.
Source Type	Source type. Select Single for a single source object. When you select an SAP IDoc Reader as connection, the source type can be a single object and source object is the IDoc Reader Object. The source object has the generic structure of an IDoc message.
Object	Source object.

The following table describes the SAP IDoc Reader advanced source properties:

Property	Description
Idle Time	Indicates the number of seconds the Secure Agent waits for IDocs to arrive before it stops reading from the SAP source. For example, if you enter 30 seconds for idle time, the Secure Agent waits 30 seconds after reading from the SAP source. If no new IDocs arrive within 30 seconds, the Secure Agent stops reading from the SAP source. Default is 300.
Packet Count	Controls the number of packets the Secure Agent reads from SAP before stopping. For example, if you enter 10 for Packet Count, the Secure Agent reads the first 10 packets from the SAP source and then stops. The packet Size property in the ALE configuration determines the number of IDocs the Secure Agent receives in a packet. If you enter packet count as -1, you can read infinite number of packets. Default is -1.
Realtime Flush Latency	Determines, in seconds, how often the Secure Agent flushes data from the source.
Reader Time Limit	Sets a period of time, in seconds, during which the Secure Agent reads IDocs from the SAP source. For example, if you specify 10 as the reader time limit, the Secure Agent stops reading from the SAP source after 10 seconds. If you enter reader time limit as 0, the Security Agent continues to read IDocs from SAP for an infinite period of time. Default is 0.

Property	Description
Recovery Cache Folder	Specifies the location of the recovery cache folder.
Tracing Level	Sets the amount of detail that appears in the log file. You can choose terse, normal, verbose initialization or verbose data. Default is normal.

Importing an IDoc mapplet to Data Integration

- To create a mapplet, click **Data Integration > New > Mapplets > Mapplet - PC Import** and then click **Create**.
To edit a mapplet, on the **Explore** page, navigate to the mapplet. In the row that contains the mapplet, click **Actions** and select **Edit**.
- Enter an unique name for the IDoc mapplet.
- Optionally, enter a description for the IDoc mapplet you want to import.
- Select the mapplet type as **Active**.
All IDoc mapplets are active.
- Click **Upload** to navigate to the XML file you generated using the SAP Metadata utility.
The **Upload Metadata XML File** dialog box appears.
- Click **Choose File**.
By default, you can view the generated IDoc mapplets as XML files in the `<SAP Metadata Utility installation directory>/generatedMappings` directory.
- Select an XML file and click **Open**.
You can view the XML file details of the IDoc mapplet.
- Click **OK**.
You can view the imported mapplet in the **Mapplets** page.

Configuring an outbound mapping to read IDocs from SAP

- To create a mapping, click **Data Integration > New > Mappings**. Select **Mapping** and click **Create**.
- Enter a name and description for the mapping, and click **OK**.
You can use alphanumeric characters and underscores (_) in the mapping name.
- To configure an SAP source, on the **Transformation** palette, click **Source**.
- In the **Properties** panel, on the **General** tab, enter a name and description.
- Click the **Source** tab and select an SAP IDoc Reader connection.

When you select an SAP IDoc Reader as connection, the source type is a single object and source object is the IDoc Reader Object.

6. If required, configure the advanced source properties.
7. To add an IDoc mapplet transformation, on the **Transformation palette**, click **Mapplet**.
 - a. On the **General** tab, enter a name and description for the mapplet.
 - b. Draw a link to connect the previous transformation to the transformation.
 - c. On the **Mapplet** tab, click **Select**.

The **Select Mapplet** dialog box appears.
 - d. Specify an IDoc mapplet that you imported using the Interpreter transformation and click **OK**.
8. To add any other transformation, on the **Transformation palette**, click the transformation name. Or, drag the transformation onto the mapping canvas.
 - a. On the **General** tab, enter a name and description for the transformation.
 - b. Draw a link to connect the previous transformation to the transformation.

When you link transformations, the downstream transformation inherits the incoming fields from the previous transformation.
For a Joiner transformation, draw a master link and a detail link.
 - c. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.
 - d. Configure additional transformation properties, as needed.

The properties that you configure vary based on the type of transformation that you create.
 - e. To add another transformation, repeat these steps.
9. To add a Target transformation, on the **Transformation palette**, click **Target**.
 - a. On the **General** tab, enter a name and description.
 - b. Draw a link to connect the previous transformation to the Target transformation.
 - c. Click the **Target** tab and configure target details. If required, configure the advanced target properties.

Target details and advanced target properties appear based on the connection type.
 - d. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.
 - e. Click **Field Mapping** and map the fields that you want to write to the target.
 - f. To add another Target transformation, repeat these steps.
10. Save and run the mapping. or save and create a mapping task.

For information about the source and target transformations, see *Transformations*.

Configuring an inbound mapping to write IDocs to SAP

1. To create a mapping, click **Data Integration > New > Mappings**. Select **Mapping** and click **Create**.
2. Enter a name and description for the mapping, and click **OK**.

You can use alphanumeric characters and underscores (_) in the mapping name.
3. To configure a source, on the **Transformation palette**, click **Source**.

4. In the **Properties** panel, on the **General** tab, enter a name and description.
5. Click the **Source** tab and configure the source details.
6. To add an IDoc mapplet transformation, on the **Transformation palette**, click Mapplet.
 - a. On the **General** tab, enter a name and description for the mapplet.
 - b. Draw a link to connect the previous transformation to the transformation.
 - c. On the **Mapplet** tab, click **Select**.

The **Select Mapplet** dialog box appears.
 - d. Specify an IDoc mapplet that you imported using the Prepare transformation and click **OK**.
 - e. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.

Note: You must link the DOCNUM port of the mapplet to the source transformation. The DOCNUM port represents a unique number for each IDoc and the SAP system does not accept inbound IDocs without a unique document number.
7. To add any other transformation, on the **Transformation palette**, click the transformation name. Or, drag the transformation onto the mapping canvas.
 - a. On the **General** tab, enter a name and description for the transformation.
 - b. Draw a link to connect the previous transformation to the transformation.

When you link transformations, the downstream transformation inherits the incoming fields from the previous transformation.

For a Joiner transformation, draw a master link and a detail link.
 - c. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.
 - d. Configure additional transformation properties, as needed.

The properties that you configure vary based on the type of transformation that you create.
 - e. To add another transformation, repeat these steps.
8. To add a Target transformation, on the **Transformation palette**, click **Target**.
 - a. On the **General** tab, enter a name and description.
 - b. Draw a link to connect the previous transformation to the Target transformation.
 - c. Click the **Target** tab and configure SAP target details.
 - d. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.
 - e. Click **Field Mapping** and map the fields that you want to write to the target.
 - f. To add another Target transformation, repeat these steps.
9. Save and run the mapping or save and create a mapping task.

Outbound mapping to read IDocs from SAP example

You can read material master (MATMAS) IDocs from SAP and write it to a relational database object.

In this example to read the MATMAS IDocs, perform the following steps:

Step 1: Import MATMAS metadata using the SAP Metadata utility.

Perform the following steps to import the MATMAS IDoc:

1. Launch the SAP Metadata utility and specify the SAP connection properties to connect to the SAP system.
2. Verify that you select the IDoc option and then connect to the SAP system.
The **Next** button is enabled only after you establish a connection to the SAP system.
3. Enter the MATMAS as the message type and MATMAS04 as the IDoc type to fetch the IDoc segments and fields for MATMAS.
4. To read IDocs, select the Interpreter transformation.
5. Retain the default output directory for the generated mapplet.

Step 2: Import the generated mapplet to Data Integration.

Log in to Data Integration and import the MATMAS mapplet XML file from the output directory.

Step 3: Configure a mapping using the generated mapplet.

Perform the following steps to configure a mapping:

1. Configure an SAP source. Specify an SAP IDoc Reader connection.
2. Add the Mapplet transformation. Draw a link to connect the Source transformation to the Mapplet transformation.
3. Map the incoming IDoc Record field with the IDocData field in the mapplet
4. Configure the Mapplet transformation. Select the generated Mapplet from the output directory.
5. Configure a target database object to which you can write the material master details. Draw a link to connect the Control Output Group in the Mapplet transformation to the Target transformation.

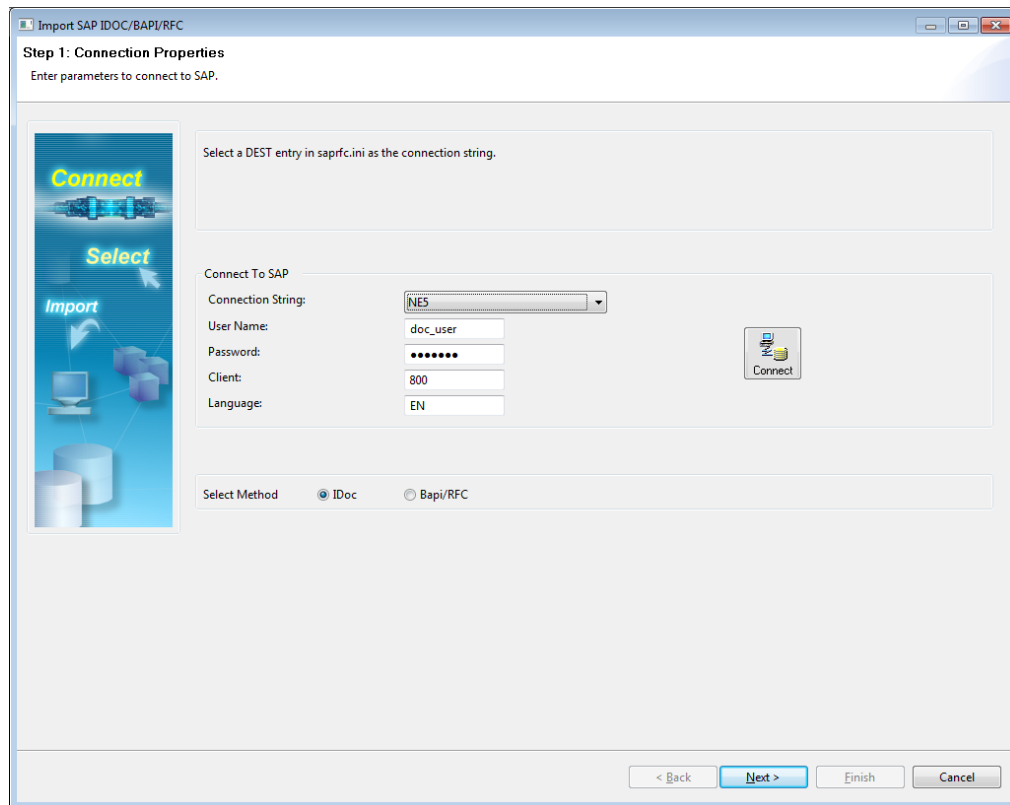
Note: Based on your requirement, you can choose to configure multiple target objects for each segment in the IDoc and for the IDoc_Interpreter_Error_Output_Group.

Step 1: Importing MATMAS IDoc metadata

1. Navigate to the SAP Metadata utility installation directory and double-click the `SAPUtil.bat` file.
The Import SAP IDOC/BAPI/RFC wizard appears.
2. Select the SAP system to which you want to connect.
All systems specified in the `sapnwrfc.ini` file appear in the drop-down list.
3. Enter the SAP user name.
4. Enter the password associated with the SAP user.
5. Enter the client number.
6. Enter the language code.
7. Select IDoc and click **Connect**.

The SAP Metadata utility establishes a connection to the SAP system.

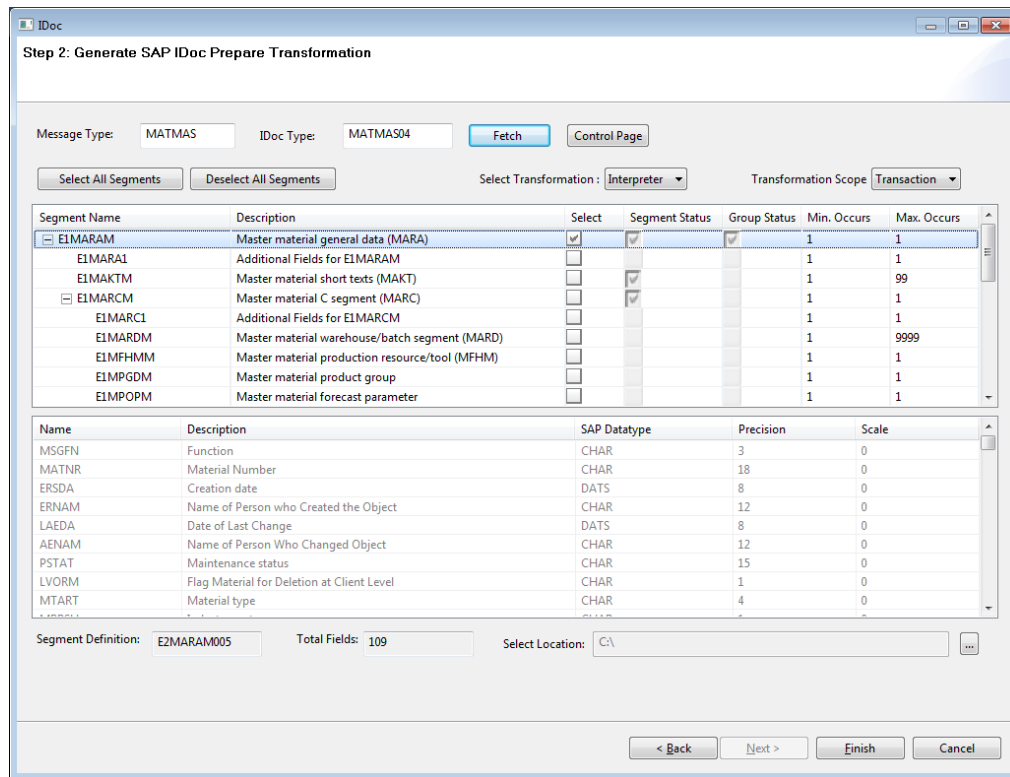
The following image shows the Connection Properties dialog box in the SAP Metadata utility:



8. Click **Next**.

The **Step 2: Select SAP IDoc Prepare Transformation** page appears.

9. Enter the message type as MATMAS and the IDoc type as MATMAS04, and click **Fetch**.
You can view the segment and field details of the IDoc.
10. Select the Interpreter transformation and the scope of the transformation as Transaction.
The following image shows the SAP IDoc specification dialog box:



11. Select the segments you want to include in the mapplet.

You can click **Select All Segments** to include all segments in the IDoc. You can click **Deselect All Segments** to remove all selected segments except required segments from the IDoc.

12. Retain the default directory for the output files and click **OK**.

13. Click **Finish**.

The MATMAS04_Interpreter_Mapping.xml mapplet for the MATMAS IDoc is created in the <SAP Metadata Utility installation directory>/generatedMappings directory.

Step 2: Importing the MATMAS04_Interpreter_Mapping mapplet to Data Integration

1. To create a mapplet, click **Data Integration > New > Mapplets > Mapplet - PC Import** and then click **Create**.

To edit a mapplet, on the **Explore** page, navigate to the mapplet. In the row that contains the mapplet, click **Actions** and select **Edit**.

2. Enter an unique name for the IDoc mapplet.

- Optionally, enter a description for the IDoc mapplet you want to import.

The following image shows the Mapplet Details:

Mapplet Details

Mapplet Name: ?

Location: Browse

Description:

Mapplet Type: ☒ Active ☐ Passive ?

Mapplet XML File: Upload... Download ?

- Select the mapplet type as **Active**.
- Click **Upload** to navigate to the XML file you generated using the SAP Metadata utility.
The **Upload Metadata XML File** dialog box appears.
- Click **Choose File**.
- Navigate to the <SAP Metadata Utility installation directory>/generatedMappings directory, select the MATMAS04_Interpreter_Mapping.xml file, and click **Open**.

The following image shows the input and output details of the MATMAS04_Interpreter_Mapping mapplet:

Mapplet XML File Details (MATMAS04_Interpreter_Mapping.xml)

Connection Reference	Type
There are no connections used by this mapplet.	

Input Fields			Output Fields		
Group	Info	Name	Group	Info	Name
IDoc_Interpreter_Input_Group_For_MATMAS04		IDocData	Control_Output_Group_For_IDoc_MATMAS04		CONTROL_TABNAM
					CONTROL_MANDT
					CONTROL_DOCNUM
					CONTROL_DOCREL
					CONTROL_STATUS
					CONTROL_DIRECT
					CONTROL_OUTMOD
					CONTROL_EXPRESS
					CONTROL_TEST
					CONTROL_IDOCTYP
					CONTROL_CIMTYP
					CONTROL_MESTYP
					CONTROL_MESCOD
					CONTROL_MESFCT
					CONTROL_STD
					CONTROL_STDVRS
					CONTROL_STDVMS
					CONTROL_SHDPOR
					CONTROL_SHDPRT

- Click **OK**.

You can view the imported mapplet in the **Mapplets** page.

Step 3: Configuring an outbound mapping with the MATMAS IDoc

- To create a mapping, click **Data Integration > New > Mappings**. Select **Mapping** and click **Create**.
- Enter a name and description for the mapping, and click **OK**.
- To configure an SAP source, on the **Transformation** palette, click **Source**.
- In the **Properties** panel, on the **General** tab, enter a name and description.
- Click the **Source** tab and select an SAP IDoc Reader connection.

When you select an SAP IDoc Reader as connection, the source type is a single object and source object is the IDoc Reader Object.

6. If required, configure the advanced source properties.

The following image shows the SAP source details:

The screenshot shows the 'Source' configuration window for an SAP IDoc Reader. The 'Source' tab is selected. Under the 'Details' section, the 'Connection' is set to 'conn_sap_idoc_reader (SAP)', 'Source Type' is 'Single Object', and 'Object' is 'IDoc_Reader_Object'. The 'Advanced' section contains several fields: 'Idle Time' (300), 'Packet Count' (-1), 'Realtime Flush Latency' (1), 'Reader Time Limit' (0), 'Recovery Cache Folder' (\$PMCacheDir/), and 'Tracing Level' (Normal).

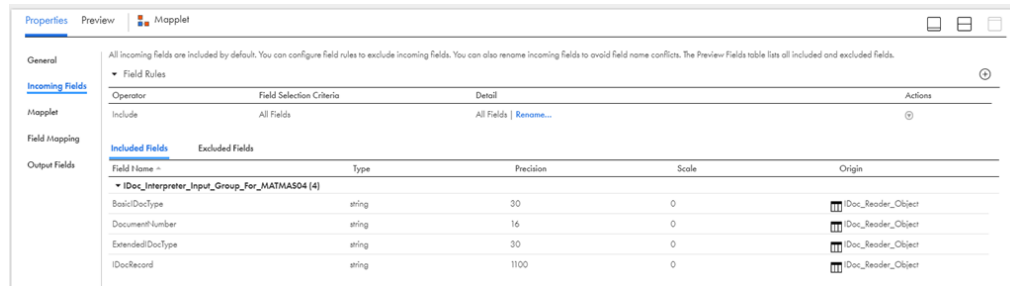
7. To add an IDoc mapplet transformation, on the **Transformation palette**, click Mapplet.
8. On the **General** tab, enter a name and description for the mapplet.
9. Draw a link to connect the Source transformation to the Mapplet transformation.
10. On the **Mapplet** tab, click **Select**.
The **Select Mapplet** dialog box appears.
11. Specify an IDoc mapplet that you imported using the Interpreter transformation and click **OK**.

The following image shows the MATMAS mapplet details:

The screenshot shows the 'Mapplet' configuration window for a MATMAS mapplet. The 'Mapplet' tab is selected. The 'Mapplet' field is set to 'Default\MATMAS04_Interpreter_Mapplet'. The 'Description' field is empty. The 'Type' is set to 'Active'.

12. To preview the incoming single IDoc Reader Object, click **Incoming Fields**.

The following image shows the incoming single IDoc Reader object:



13. Click **Field Mappings** to map the incoming IDoc Record field with the IDocData field in the mapplet.

14. To add a Target transformation, on the **Transformation palette**, click **Target**.

15. On the **General** tab, enter a name and description.

16. Click the **Target** tab, and configure the required target database details.

Note: When you use IDoc Listener as a source, you can specify only those targets that honor commit. Contact Global Customer Support for the list of supported targets.

17. Draw a link to connect the mapplet groups to the target database object.

18. Save and run the mapping.

Inbound mapping to write IDocs to SAP example

You can create material master (MATMAS) in SAP using MATMAS IDoc type.

In this example to write MATMAS IDoc to SAP, perform the following steps:

Step 1: Import MATMAS metadata using the SAP Metadata utility.

Perform the following steps to import the MATMAS IDoc:

1. Launch the SAP Metadata utility and specify the SAP connection properties to connect to the SAP system.
2. Verify that you select the IDoc option and then connect to the SAP system.
The **Next** button is enabled only after you establish a connection to the SAP system.
3. Enter the MATMAS as the message type and MATMAS03 as the IDoc type to fetch the IDoc segments and fields for MATMAS.
4. To write IDocs, select the Prepare transformation.
5. Retain the default output directory for the generated mapplet.

Step 2: Import the generated mapplet to Data Integration.

Log in to Data Integration and import the MATMAS mapplet XML file from the output directory.

Step 3: Configure a mapping using the generated mapplet.

Perform the following steps to configure a mapping:

1. Configure multiple flat file sources to provide data to the mapplet input fields.

2. Add the Mapplet transformation. Draw a link to connect the Source transformation to the Mapplet transformation.
3. Configure the Mapplet transformation. Select the generated mapplet from the output directory.
4. Configure an SAP object to write the material master details and a flat file object to write the error details. Draw a link to connect the IDoc_Prepare_Output_Group_For_MATMAS03 to the IDocWriter object. Draw another link to connect the IDoc_Prepare_Error_Output_Group_For_MATMAS03 to the Error_Output flat file object.

Step 1: Importing MATMAS IDoc metadata

1. Navigate to the SAP Metadata utility installation directory and double-click the `SAPUtil.bat` file.
The Import SAP IDOC/BAPI/RFC wizard appears.
2. Select the SAP system to which you want to connect.
All systems specified in the `sapnwrfc.ini` file appear in the drop-down list.
3. Enter the SAP user name.
4. Enter the password associated with the SAP user.
5. Enter the client number.
6. Enter the language code.
7. Select IDoc and click **Connect**.
The SAP Metadata utility establishes a connection to the SAP system.
8. Click **Next**.
The **Step 2: Select SAP IDoc Prepare Transformation** page appears.
9. Enter the message type as MATMAS and the IDoc type as MATMAS03, and click **Fetch**.
You can view the segment and field details of the IDoc.
10. Select the Prepare transformation and the scope of the transformation as All Input.
11. Select the segments you want to include in the mapplet.
You can click **Select All Segments** to include all segments in the IDoc. You can click **Deselect All Segments** to remove all selected segments except required segments from the IDoc.
12. To add other fields into the Control Record input group of a mapplet, perform the following steps:
 - a. Click **Control Page**. Add more control records if you have more than one logical system.
 - b. Select the checkbox for the field that you want to add, and then click **Partner Profile > New**.
 - c. Enter the key and value for the partner profile. The key is the field name, and the value is the partner type.
 - d. Optionally, to add a control record field to the mapplet, from the Control Record page, select the checkbox for the field you want to add. This will enable you to map the selected control record fields when you configure a mapping, integration template, or mapping task.
13. Retain the default directory for the output files and click **OK**.
14. Click **Finish**.

The `MATMAS03_Prepare_Mapping.xml` mapplet for the MATMAS IDoc is created in the `<SAP Metadata Utility installation directory>/generatedMappings` directory.

Step 2: Importing the MATMAS03_Prepare_Mapping mapplet to Data Integration

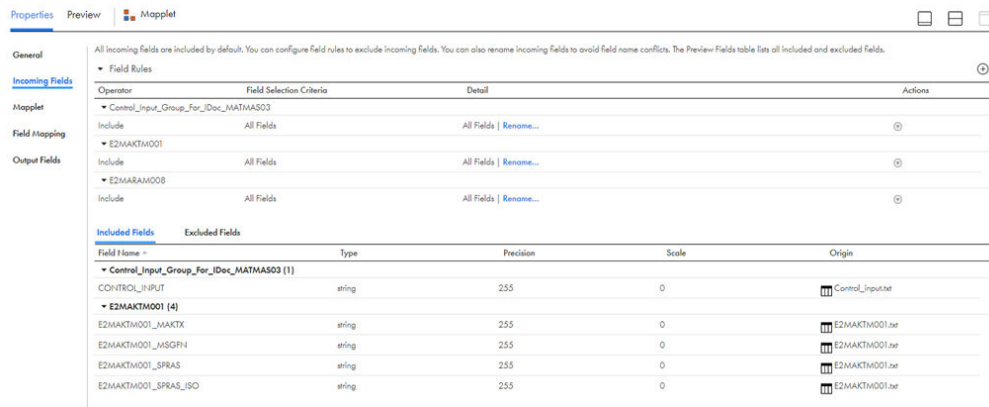
1. To create a mapplet, click **Data Integration > New > Mapplets > Mapplet - PC Import** and then click **Create**.
To edit a mapplet, on the **Explore** page, navigate to the mapplet. In the row that contains the mapplet, click **Actions** and select **Edit**.
2. Enter an unique name for the IDoc mapplet.
3. Optionally, enter a description for the IDoc mapplet you want to import.
4. Select the mapplet type as **Active**.
5. Click **Upload** to navigate to the XML file you generated using the SAP Metadata utility.
The **Upload Metadata XML File** dialog box appears.
6. Click **Choose File**.
7. Navigate to the `<SAP Metadata Utility installation directory>/generatedMappings` directory, select the `MATMAS03_Prepare_Mapping.xml` file, and click **Open**.
8. Click **OK**.
You can view the imported mapplet in the **Mapplets** page.

Step 3: Configuring an inbound mapping with the MATMAS IDoc

1. To create a mapping, click **Data Integration > New > Mappings**. Select **Mapping** and click **Create**.
2. Enter a name and description for the mapping, and click **OK**.
3. To configure a flat file source, on the **Transformation** palette, click **Source**.
4. In the **Properties** panel, on the **General** tab, enter a name and description.
5. Click the **Source** tab and select an flat file connection.
6. Add separate flat file sources for the control_input group and segments in the MATMAS IDoc.
7. To add an IDoc Mapplet transformation, on the **Transformation palette**, click Mapplet.
8. On the **General** tab, enter a name and description for the mapplet.
9. On the **Mapplet** tab, click **Select**.
The **Select Mapplet** dialog box appears.
10. Specify an IDoc mapplet that you imported using the Prepare transformation and click **OK**.
11. Draw a link to connect the Source transformations to the Mapplet transformation. For example, connect the Control_Input source object to the Control_Input_Group for the MATMAS IDoc.

12. To preview the incoming fields, click **Incoming Fields**.

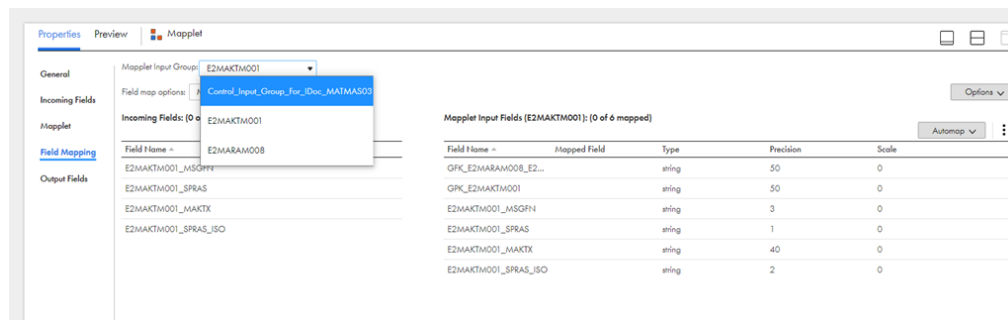
The following image shows the incoming fields:



Field Name	Type	Precision	Scale	Origin
Control_Input_Group_For_IDoc_MATMAS03	string	255	0	Control_Input.doc
E2MAKTM001	string	255	0	E2MAKTM001.doc
E2MAKTM001_MAKTX	string	255	0	E2MAKTM001.doc
E2MAKTM001_MSGFN	string	255	0	E2MAKTM001.doc
E2MAKTM001_SPRAS	string	255	0	E2MAKTM001.doc
E2MAKTM001_SPRAS_ISO	string	255	0	E2MAKTM001.doc

13. Click **Field Mappings** to map the incoming fields with the mapplet input fields.

The following image shows the field mapping in the mapplet:

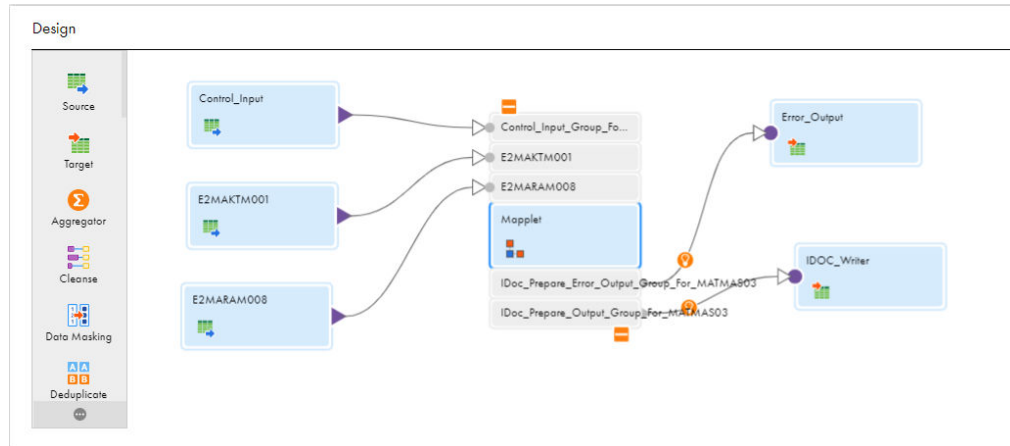


Field Name	Mapped Field	Type	Precision	Scale
Control_Input_Group_For_IDoc_MATMAS03	Control_Input_Group_For_IDoc_MATMAS03	string	50	0
E2MAKTM001	E2MAKTM001	string	50	0
E2MAKTM001_MSGFN	E2MAKTM001_MSGFN	string	3	0
E2MAKTM001_SPRAS	E2MAKTM001_SPRAS	string	1	0
E2MAKTM001_MAKTX	E2MAKTM001_MAKTX	string	40	0
E2MAKTM001_SPRAS_ISO	E2MAKTM001_SPRAS_ISO	string	2	0

14. To add a Target transformation for writing to SAP, on the **Transformation palette**, click **Target**.
- On the **General** tab, enter a name and description.
 - Click the **Target** tab and configure SAP target details.
15. To add a flat file Target transformation for the error output, on the **Transformation palette**, click **Target**.
- On the **General** tab, enter a name and description.
 - Click the **Target** tab and configure flat file target details.

16. Draw a link to connect the `IDoc_Prepare_Output_Group_For_MATMAS03` to the `IDocWriter` object. Draw another link to connect the `IDoc_Prepare_Error_Output_Group_For_MATMAS03` to the `Error_Output` flat file object.

The following image shows the mapping for the inbound mapping for the MATMAS IDoc:



17. Save and run the mapping.

Part VII: SAP BW Data Extraction

This part contains the following chapters:

- [Synchronization tasks with SAP BW, 153](#)
- [Mappings and Mapping tasks with SAP BW, 157](#)

CHAPTER 12

Synchronization tasks with SAP BW

This chapter includes the following topics:

- [Synchronization tasks with SAP BW overview, 153](#)
- [SAP BW sources in Synchronization tasks, 154](#)
- [Configuring a Synchronization task with a single SAP BW object as the source, 155](#)
- [Monitoring a Synchronization task, 156](#)

Synchronization tasks with SAP BW overview

You can configure a synchronization task to synchronize data between an SAP BW source and a target. You can use the Synchronization Task wizard to configure the synchronization task.

You can use SAP BW objects as sources. You can read data from InfoCubes, InfoSets, MultiProviders, and DataStore objects. You can use expressions to transform the data according to your business logic and use data filters to filter data before writing it to targets.

Note: You cannot perform a lookup on an SAP BW object.

When you create a task, you can associate it with a schedule to run it at specified times or at regular intervals. You can also manually run a task. You can monitor tasks and view logs about completed tasks.

SAP BW sources in Synchronization tasks

When you configure a synchronization task to use an SAP BW source, you can configure the source properties. The source properties appear on the **Source** page of the Synchronization Task wizard.

The following table describes the SAP BW source properties:

Property	Description
Connection	SAP BW Reader connection that you want to use to read data.
Source Type	Source type. You can read data from a single SAP BW object. You cannot edit this field.
Source Object	SAP BW source object from which you want to read data.
Display technical field names instead of labels	When selected, displays technical names instead of business names of the fields in the specified source object.
Display source fields in alphabetical order	When selected, displays source fields in alphabetic order. By default, fields appear in the order returned by the source system.
Data Preview	Displays the first 10 rows of the first five columns in the object, and the total number of columns in the object.
Preview All Columns	Previews all source columns in a file.

You can also configure advanced source properties when you schedule the synchronization task. Advanced source properties appear on the **Schedule** page of the Synchronization Task wizard.

The following table describes the SAP BW advanced source properties:

Property	Description
Packet Size in MB	Size of the HTTP packet that SAP sends to the Secure Agent. The unit is MB. Default is 10 MB.
Package Size in ABAP in Rows	Number of rows that are read and buffered in SAP at a time. Default is 1000 rows.
Enable Compression	When selected, the ABAP program compresses the data in the gzip format before it sends the data to the Secure Agent. If the Secure Agent and the SAP system are not on the same network, you might want to enable the compression option to optimize performance. Default is not selected.

Configuring a Synchronization task with a single SAP BW object as the source

1. To create a synchronization task, click **Data Integration > New > Tasks**. Select **Synchronization Task** and click **Create**.
2. Enter a name for the synchronization task.

The names of synchronization tasks must be unique within the organization. Synchronization task names are not case sensitive. Synchronization task names can contain alphanumeric characters, spaces, and the following special characters: _ . + -
3. Enter a description for the synchronization task.

The description can have a maximum length of 255 characters.
4. Select the task operation that you can perform on the target.

You can select one of the following options:

 - Insert
 - Update
 - Upsert
 - Delete
5. Click **Next** to enter the source details.
 - a. Select an SAP BW Reader connection from the list or create a new SAP BW Reader connection.
 - b. Select an SAP BW source object from the list or click **Select** to search for an SAP BW source object.

The **Select Source Object** dialog box appears. The dialog box displays up to 200 objects. If the objects that you want to use do not appear, enter a search string to search for the object based on its name, label, description, or type, and then click **Search**.
 - c. Select the SAP BW source object from which you want to read data, and then click **Select**.

The **Data Preview** area displays the first 10 rows of the first five columns in the SAP BW object, and the total number of columns in the object. To preview all source columns in a file, click **Preview All Columns**.
 - d. To display technical names instead of business names, select the **Display technical field names instead of labels** option.
 - e. To display source fields in alphabetic order, select the **Display source fields in alphabetical order** option.

By default, fields appear in the order returned by the source system.
6. Click **Next** to specify the target connection and target objects.
7. Click **Next** to specify the data filter criteria.
 - a. Click **New** to create a data filter. You can specify a simple data filter based on key characteristics.

Note: You cannot create an advanced data filter. You cannot specify a simple data filter based on key figures.
 - b. Select the source object, key characteristic source field, and operator.

You can select one of the following operators for the filter condition:

 - Equals

- Not Equals
 - Less Than
 - Less Than or Equals
 - Greater Than
 - Greater Than or Equals
- c. Enter the value based on which you want to filter the data and click **OK**.
8. Click **Next** to configure the field mappings. Perform any of the following steps based on your requirements:
- a. Click **Edit Types** in the Source column to edit the precision and scale of the SAP BW object.
 - b. Click **Automatch** to match source and target fields with similar names.
 - c. Click **Refresh Fields** to update the cache and view the latest field attributes.
 - d. Click **Edit Types** in the Target column to edit the data type, precision, and scale of the target object. Note that this option is not available for all target types.
 - e. Select a source field and drag it to the target field to map the source and target fields. Repeat for all the fields that you want to map.
 - f. Click the **Add or Edit Expression** icon to define a field expression to transform data.
 - g. Click **Validate Mapping** to validate all the field mappings.
 - h. Click **Clear Mapping** to clear all the field mappings.
9. Click **Next** to configure a schedule and advanced options. Perform any of the following steps based on your requirements:
- a. Click **Run this task on schedule** and specify the schedule that you want to use. Alternatively, you can click **Do not run this task on a schedule** to run the task manually.
 - b. Configure the email notification options.
 - c. Configure a parameter file, if needed.
 - d. Configure the advanced source properties.
 - e. Specify the execution mode.
10. Save the synchronization task. You can choose one of the following save options:
- Click **Save and Close** to save and close the task.
 - Click **Save and Continue** to save the task and continue with configuring the task.
 - Click **Save and Run** to save and run the task immediately.

Monitoring a Synchronization task

After you run a synchronization task, you can monitor the task and view the logs.

In **Monitor**, you can monitor the status of the logs after you run the task.

You can also monitor the progress of the task by calling Transaction SM37 from SAP. You can view the actual job duration in SAP. The job duration listed in the Data Integration activity log is a higher value because it also includes time required to complete processing in Data Integration.

You can view the HTTP and HTTPS log files in the SMICM transaction. Optionally, you can increase trace level to 3 to view the detailed logs.

CHAPTER 13

Mappings and Mapping tasks with SAP BW

This chapter includes the following topics:

- [Mappings and Mapping tasks with SAP BW overview , 157](#)
- [SAP BW sources in mappings, 158](#)
- [Configuring a mapping with a single SAP BW source, 158](#)
- [Creating a Mapping task, 160](#)
- [Monitoring a Mapping task, 161](#)
- [Rules and guidelines for SAP BW sources, 161](#)

Mappings and Mapping tasks with SAP BW overview

Use a mapping to define data flow logic that is not available in synchronization tasks, such as specific ordering of logic. Use the Data Integration Mapping Designer to configure mappings.

You can create a mapping to read data from an SAP BW source. You cannot perform a lookup on an SAP BW object.

When you configure a mapping to describe the flow of data from a source to a target, you can also add transformations to transform data. A transformation includes field rules to define incoming fields. Links visually represent how data moves through the data flow.

After you create a mapping, you can run the mapping or you can deploy the mapping in a mapping task. You can use the Mapping application to process data based on the data flow logic that you defined in the mapping.

Use the Mapping Task wizard to create a mapping task. When you create a mapping task, you can select the mapping based on which you want to create the task.

If you configured parameters, which are placeholders for information, in a mapping, you can define the parameters in the mapping task. You can define parameters for additional flexibility and to use the same mapping in multiple mapping tasks. For example, you can use a parameter for a source connection in a mapping, and then define the source connection when you configure the mapping task.

When you create a mapping task, you can associate the task with a schedule to run it at specified times or at regular intervals. Or, you can run it manually. You can also configure advanced session properties. You can monitor tasks and view details about completed tasks.

SAP BW sources in mappings

To read data from an SAP BW source, configure an SAP BW object as the Source transformation in a mapping.

Specify the name and description of the SAP BW source. Configure the source and advanced properties for the source object.

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

Property	Description
Connection	SAP BW Reader connection that you want to use to read data.
Source Type	Source type. Select one of the following types: <ul style="list-style-type: none">- Single. Select to specify a single SAP BW object.- Parameter. Select to specify a parameter name. You can configure the source object in a mapping task associated with a mapping that uses this source transformation.
Object	SAP BW source object from which you want to read data.

The following table describes the SAP BW advanced source properties:

Property	Description
Packet Size in MB	Size of the HTTP packet that SAP sends to the Secure Agent. The unit is MB. Default is 10 MB.
Package Size in ABAP in Rows	Number of rows that are read and buffered in SAP at a time. Default is 1000 rows.
Enable Compression	When selected, the ABAP program compresses the data in the gzip format before it sends the data to the Secure Agent. If the Secure Agent and the SAP system are not on the same network, you might want to enable the compression option to optimize performance. Default is not selected.
Tracing Level	Amount of detail that appears in the log file. You can select one of the following options: <ul style="list-style-type: none">- Terse- Normal- Verbose Initialization- Verbose Data Default is normal.

Configuring a mapping with a single SAP BW source

Use the Data Integration Mapping Designer to configure a mapping.

1. To create a mapping, click **Data Integration > New > Mappings**. Select **Mapping** and click **Create**.

2. Enter a name and description for the mapping, and click **OK**.
You can use alphanumeric characters and underscores (_) in the mapping name.
3. To configure an SAP BW source, on the **Transformation** palette, click **Source**.
4. In the **Properties** panel, on the **General** tab, enter a name and description for the SAP BW source.
5. Click the **Source** tab and configure the SAP BW source details.
6. Select an SAP BW Reader connection from the list or click **New Connection** to create a new SAP BW Reader connection.
You can also parameterize the connection.
7. Specify the source type. You can choose one of the following options:
 - Select **Single Object** to select a single SAP BW object.
 - Select **Parameter** to configure the SAP BW source objects in a mapping task associated with this mapping.
8. Enter the SAP BW object name or click **Select** to search for an object based on its name, label, description, or type.
9. Select the SAP BW object from which you want to read data and click **OK**.
10. Click **Query Options** in the **Source** tab to specify data filters for the SAP BW object.
You can specify a simple data filter based on key characteristic fields.
Note: You cannot create an advanced data filter.
 - a. Click **Configure** and then click the **+** icon to add a data filter.
 - b. Select the source object, key characteristic source field, and operator.
You can select one of the following operators for the filter condition:
 - Equals
 - Not Equals
 - Less Than
 - Less Than or Equals
 - Greater Than
 - Greater Than or Equals
 - c. Enter the value that you want to use and click **OK**.
You can also parameterize the filter condition.
11. Click **Advanced** to specify the advanced source properties.
12. To add or remove source fields, update field metadata, or synchronize fields with the source, click the **Fields** tab.
13. To add a transformation, on the **Transformation palette**, click the transformation name. Or, drag the transformation onto the mapping canvas.
 - a. On the **General** tab, you can enter a name and description for the transformation.
 - b. Draw a link to connect the previous transformation to the transformation.
When you link transformations, the downstream transformation inherits the incoming fields from the previous transformation.
For a Joiner transformation, draw a master link and a detail link.
 - c. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.

- d. Configure additional transformation properties, as needed.
The properties that you configure vary based on the type of transformation you create.
- e. To add another transformation, repeat these steps.
14. To add a Target transformation, on the **Transformation palette**, click **Target**.
 - a. On the **General** tab, enter a name and description for the target.
 - b. Draw a link to connect the previous transformation to the Target transformation.
 - c. Click the **Target** tab and configure target details. If necessary, configure the advanced target properties.
Target details and advanced target properties appear based on the connection type. For more information, see *Transformations*.
 - d. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.
 - e. Click **Field Mapping** and map the fields that you want to write to the target.
 - f. To add another Target transformation, repeat these steps.
15. Save the mapping. You can choose one of the following save options:
 - Click **Save and Close** to save and close the mapping.
 - Click **Save and Run** to save and run the mapping immediately.
 - Click **Save and New Mapping Task** to save and create a mapping task.

Creating a Mapping task

You can create a mapping task based on a valid mapping.

1. To create a mapping task, click **Data Integration > New > Tasks** and then complete one of the following steps:
 - To create a mapping task based on a mapping, select **Mapping Task** and click **Create**.
 - To create a mapping task using a template, expand the appropriate template category and select the template you want to use, and then click **Create**.

To edit a mapping task, on the **Explore** page, navigate to the mapping task. In the row that contains the task, click **Actions** and select **Edit**.

2. Enter a name for the task.
Task names must be unique within the organization. Task names are not case sensitive. Task names can contain alphanumeric characters, spaces, and the following special characters: `_ . + -`
3. Select the runtime environment that contains the Secure Agent that you want to use to access the SAP BW objects.
4. Select **Mapping** as the task based on which you want to create the mapping task.
5. Click **Select** to specify a mapping.
The **Select a Mapping** dialog box appears.
6. Select a mapping. You can also search for a mapping based on its name and description.
7. Click **OK**.
The image of the selected mapping appears.

8. Click **Next**.
If you specified any parameters in the source or target details in the mapping, the **Source** or **Target** page appears. If not, the **Schedule** page appears.
9. Configure a schedule and advanced options. Perform any of the following steps based on your requirements:
 - a. Click **Run this task on schedule** and specify the schedule that you want to use.
 - b. Configure the email notification options.
 - c. Configure advanced options for the task.
 - d. Specify the execution mode.
10. Optionally, add advanced session properties.
 - a. Click **Add**.
 - b. Select a session property.
 - c. Configure the value of the session property.
11. Save the mapping task. You can choose one of the following save options:
 - Click **Save and Close** to save and close the task.
 - Click **Save and Continue** to save the task and continue with configuring the task.
 - Click **Save and Run** to save and run the task immediately.

Monitoring a Mapping task

After you run a mapping task, you can monitor the task and view the logs.

In **Monitor**, you can monitor the status of the logs after you run the task.

You can also monitor the progress of the task by calling Transaction SM37 from SAP. You can view the actual job duration in SAP. The job duration listed in the Data Integration activity log is a higher value because it also includes time required to complete processing in Data Integration.

You can view the HTTP and HTTPS log files in the SMICM transaction. Optionally, you can increase trace level to 3 to view the detailed logs.

Rules and guidelines for SAP BW sources

To establish communication from the SAP system with the Secure Agent using the IP address of the NAT gateway, you must include the DTM property named SapTableReaderNatIpAddress for the Secure Agent and specify the NAT IP address as the value.

Part VIII: Data Integration using SAP ODP Extractor

This part contains the following chapters:

- [SAP ODP, 163](#)
- [Mappings and mapping tasks with SAP ODP Extractor, 165](#)

CHAPTER 14

SAP ODP

This chapter includes the following topics:

- [SAP ODP sources, 163](#)
- [Rules and guidelines for SAP ODP sources, 164](#)

SAP ODP sources

You can connect to SAP ODPs using SAP ODP Extractor Connector.

Use SAP ODP Extractor Connector to connect to ODPs available in the following contexts or providers:

Providers/Context	Source SAP System and ODPs
SAP Service Application Programming Interface (S-API)	SAP Data Sources/Extractors without Enterprise Search (ESH)
HANA	SAP HANA Information View
BW	SAP NetWeaver Business Warehouse
ABAP_CDS	ABAP Core Data Services

SAP ODP Extractor Connector identifies the different contexts available based on the SAP system that you want to use. Identified contexts appear as packages in the **Select Object** dialog box. You can select any of the packages to get the list of the available activated ODPs for that context. You can filter by the ODP name when you connect to the SAP system.

Data Integration imports the following SAP ODP information:

- ODP name
- Business descriptions
- ODP type
- ODP transfer structure fields
- Field information such as the name, type, description, filterable, precision, scale, SAP type, SAP length, SAP output length, and SAP decimals.

Rules and guidelines for SAP ODP sources

Use the following rules and guidelines when you configure SAP ODP sources:

- Only the available contexts in the selected SAP system appear as packages.
- Ensure that the required ODP is activated in the SAP system before you can use in Data Integration. Only the activated ODPs appear in the browser list of the SAP ODP Extractor Connector.
- If the ODP name contains namespace (" / ") characters at the beginning, the Secure Agent replaces those characters with T___. Every subsequent namespace character in the ODP name is replaced by "__". For example, if the ODP name is /IMO/CMSD17, it appears in the browser list as T___IMO__CMSD17.
- If the field name of the selected ODP has a namespace character (" / "), that character is replaced with an underscore (_) character.
- Do not edit the field metadata as it might corrupt the extracted data.
- Partitioning is not supported with filters and hierarchal data sources.
- You can read delta data for ODPs that are supported in the SAP system. If you try to run the delta mode for ODPs where the ODQ is not maintained in the SAP system, a runtime error occurs. If the ODQ is not supported for contexts such as HANA and ABAP CDS views, delta data fetch modes are not applicable.
- You can apply filters only for the selected fields of the ODPs. You can identify those fields with the attribute Filterable marked as Y. If you apply filters on any other fields, it results in a runtime error.
- Sorting of data is not supported.
- The default packet size to write data is 8 MB. When you set the packet size value equal to greater than 8 MB and you encounter out-of-memory issues, you can increase the Java heap memory for the Secure Agent. In the **System Configuration Details** section of the Secure Agent properties, select **DTM** and set the **JVMOption1** property to the following value: *Xmx512m*. Click **OK** to save the change and then restart the Secure Agent. Adjust the value for the JVMOption1 property based on the amount of records you want to write and the available memory on the Secure Agent machine.

CHAPTER 15

Mappings and mapping tasks with SAP ODP Extractor

This chapter includes the following topics:

- [Mapping and mapping tasks overview, 165](#)
- [SAP ODP sources in mappings, 166](#)
- [Delta extraction for SAP ODP Extractor mappings, 168](#)
- [Fixed partitioning for SAP ODP sources, 168](#)
- [Configuring a mapping with an SAP ODP source, 169](#)
- [Creating a mapping task, 170](#)

Mapping and mapping tasks overview

Use a mapping to define the data flow logic. Use the Data Integration Mapping Designer to configure mappings.

When you configure a mapping to describe the flow of data from source and target, you can also add transformations to transform data. A transformation includes field rules to define incoming fields. Links visually represent how data moves through the data flow.

After you create a mapping, you can run the mapping or you can deploy the mapping in a mapping task. The Mapping Configuration application allows you to process data based on the data flow logic defined in a mapping or integration template.

Use the Mapping task wizard to create a mapping task. When you create a mapping task, you select the mapping or integration template for the task to use.

If you configured parameters, which are placeholders for information, in a mapping, you can define the parameters in the mapping task. Defining parameters provides additional flexibility and allows you to use the same mapping in multiple mapping tasks. For example, you can use a parameter for a source connection in a mapping, and then define the source connection when you configure the mapping task.

When you create a mapping task, you can associate the task with a schedule to run it at specified times or on regular intervals. Or, you can run it manually. You can also configure advanced session properties. You can monitor tasks that are currently running and view details about completed tasks.

SAP ODP sources in mappings

To read data from an SAP S/4HANA application, configure an SAP ODP object as the Source transformation in a mapping.

Specify the name and description of the SAP ODP source. Configure the source and advanced properties for the source object.

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

Property	Description
Connection	Name of the source connection.
Source Type	The source type. Select from one of the following types: <ul style="list-style-type: none">- Single. Select to specify a single SAP ODP object.- Parameter. Select to specify the SAP ODP object as a parameter.
Source Object	Source object for the task. Click Select to select the source object.
Preview Data	Not applicable

The following table describes the SAP ODP Extractor advanced source properties:

Property	Description
Data Fetch Mode	<p>The data fetch mode used while reading records from ODP.</p> <p>You can select from the following options:</p> <p>0-Full</p> <p>Reads all the records for the selected ODP.</p> <p>1-Delta Plus</p> <p>Reads all records of the ODP from the SAP system and also initializes the Operational Delta Queue (ODQ) for the selected ODP in the subscriber that you defined in the SAP system when you run the mapping for the first time using this mode. Subsequently, use this mode to read delta data of the ODP from the SAP system.</p> <p>2-Delta Only</p> <p>Initializes the Operational Delta Queue (ODQ) for the selected ODP in the subscriber that you defined in the SAP system when you run the mapping for the first time using this mode. Subsequently, when you use this mode and run the mapping, the Secure Agent reads delta data of the ODP from the SAP system.</p> <p>3-Repetitive</p> <p>Extracts delta records of the last delta run.</p> <p>For example, use this mode when the mapping with the Delta Plus or Delta Only option fails, and you want to read the last delta again.</p> <p>Parameter</p> <p>Use this option when you want to parameterize the data fetch mode values. Specify a valid data fetch mode value in the Parameter Name for Data Fetch Mode field.</p>
Parameter Name for Data Fetch Mode	<p>The parameter name that you defined for the Data Fetch Mode property in the parameter file.</p> <p>You can specify the following values for the data fetch mode:</p> <ul style="list-style-type: none"> - 0 for Full - 1 for Delta Plus - 2 for Delta Only - 3 for Repetitive <p>If you pass any other value, the jobs fail when you run the mapping,</p>
Job Timeout	<p>Defines the maximum amount of time, in seconds, while processing the mapping during which the Secure Agent must wait before it receives communication from SAP and get the data packets.</p> <p>The timeout applies only when the Secure Agent waits for SAP to send the data packets. Do not modify the default value.</p>
Packet size in MB	<p>The packet size of each SAP data packet while reading data from SAP S/4HANA.</p> <p>Default value is 8 MB.</p>
Tracing	<p>Sets the amount of detail that appears in the log file.</p> <p>You can choose terse, normal, verbose initialization or verbose data.</p> <p>Default is normal</p>

Delta extraction for SAP ODP Extractor mappings

You can use the SAP ODP Extractor to extract delta data from ODPs that are enabled for delta. SAP maintains Operation Data Queue (ODQ) for delta-enabled ODPs. For contexts such as HANA and ABAP CDS views, SAP does not maintain ODQ at the source and therefore you cannot extract delta data from the ODPs of these contexts.

When you configure a mapping, use the following sequence to extract data from ODPs:

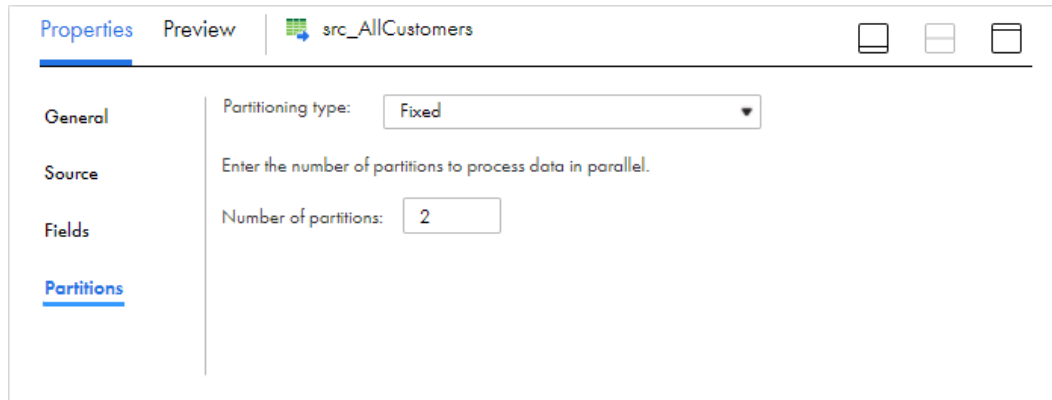
1. Run the mapping using Full as the data fetch mode to extract all the records of the ODP to create the initial setup.
2. Run the job in Delta Only mode to initialize ODQ for the selected ODP for your subscriber in the SAP system. SAP starts tracking for any changes of data in ODQ.
3. Alternatively, combine operations 1 and 2 to run the job in the Delta Plus data fetch mode. Using this option, you can extract all the records from the ODP and initialize ODQ for the ODPs from your defined subscriber.
4. Subsequently, you can run the mapping with either Delta Only or Delta Plus mode to extract delta data for the selected SAP system.
5. At any time, if you want to extract the last delta data, run the mapping in the Repetitive data fetch mode.

Fixed partitioning for SAP ODP sources

You can configure fixed partitioning in a mapping that reads data from SAP ODP sources.

Enable partitioning when you configure the Source transformation in the Mapping Designer.

On the **Partitions** tab for the Source transformation, you select fixed partitioning and enter the number of partitions, as shown in the following image:



The screenshot shows the SAP ODP Extractor Mapping Designer interface. At the top, there are tabs for 'Properties' (selected), 'Preview', and a source icon labeled 'src_AllCustomers'. Below the tabs, on the left, is a vertical list of tabs: 'General', 'Source', 'Fields', and 'Partitions' (which is highlighted with a blue underline). The main area on the right is for the 'Partitions' tab. It contains a 'Partitioning type:' dropdown menu with 'Fixed' selected. Below this, there is a text prompt 'Enter the number of partitions to process data in parallel.' followed by a 'Number of partitions:' label and a text input field containing the value '2'.

The mapping task distributes rows of data based on the number of partitions that you specify. You can specify up to 64 partitions.

Configuring a mapping with an SAP ODP source

Use the Data Integration Mapping Designer to configure a mapping.

1. To create a mapping, click **Data Integration > New > Mappings**. Select **Mapping** and click **Create**.
2. Enter a name and description for the mapping, and click **OK**.
You can use alphanumeric characters and underscores (_) in the mapping name.
3. To configure a source, on the **Transformation palette**, click **Source**.
4. In the **Properties** panel, on the **General** tab, enter a name and description.
5. Click the **Source** tab and configure source details.
6. Specify the source type. You can choose one of the following options:
 - Select **Single Object** to select a single SAP object.
 - Select **Parameter** to configure the source objects in a mapping task associated with this mapping.
7. Click **Query Options** in the **Source** tab to specify any filter for the SAP ODP object.
8. Click **Advanced** to specify the advanced source properties.
Note: You cannot add or remove source fields or edit the field metadata.
9. To add a transformation, on the **Transformation palette**, click the transformation name. Or, drag the transformation onto the mapping canvas.
 - a. On the **General** tab, you can enter a name and description for the transformation.
 - b. Draw a link to connect the previous transformation to the transformation.
When you link transformations, the downstream transformation inherits the incoming fields from the previous transformation.
For a Joiner transformation, draw a master link and a detail link.
 - c. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.
 - d. Configure additional transformation properties, as needed.
The properties that you configure vary based on the type of transformation you create.
 - e. To add another transformation, repeat these steps.
10. To add a Target transformation, on the **Transformation palette**, click **Target**.
 - a. On the **General** tab, you can enter a name and description.
 - b. Draw a link to connect the previous transformation to the Target transformation.
 - c. Click the **Target** tab and configure target details. If necessary, configure the advanced target properties.
Target details and advanced target properties appear based on the connection type. For more information, see *Transformations*.
 - d. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.
 - e. Click **Field Mapping** and map the fields that you want to write to the target.
 - f. To add another Target transformation, repeat these steps.
11. Click the **Field Mapping** to map the Source and Target fields.
You can use the Automatic option if the fields are similar between the source and target.
12. Save and run the mapping or save and create a mapping task.

Creating a mapping task

You can create a mapping task based on a valid mapping or integration template on the Mappings page.

1. To create a mapping task, click **Data Integration > New > Tasks**.
2. Enter a name for the task.

Task names must be unique within the organization. Task names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Task names are not case sensitive.
3. Select the runtime environment that contains the Secure Agent that you want to use to access the SAP ODP Extractor connection.
4. Select **Mapping** as the task based on which you want to create the mapping task.
5. Click **Select** to specify a mapping.

The **Select a Mapping** dialog box appears.
6. Select a mapping or search for the required mapping and select **OK**.

The image of the selected mapping appears.
7. Click **Next**.

If you specified any parameters in the source or target details in the mapping, the Source or Target page appears. If not, the Schedule page appears.
8. Click **Next** to configure a schedule and advanced options. Perform any of the following steps based on your requirements.
 - a. Click **Run this task on schedule** and specify the schedule you want to use.
 - b. Configure the email notification options.
 - c. Configure advanced options for the task.
 - d. Configure the advanced source properties and advanced target properties.
 - e. Specify the execution mode.
9. Optionally, add the advanced session properties.
 - a. Click **Add**.
 - b. Select a session property.
 - c. Configure the value of the session property.
10. Save and run the mapping task.

Part IX: Data Integration for SAP ADSO

This part contains the following chapters:

- [Data Integration for SAP ADSO sources using SAP Table Reader, 172](#)
- [Data Integration for SAP ADSO targets using SAP ADSO Writer, 174](#)
- [Mappings and mapping tasks with SAP ADSO Writer, 176](#)

CHAPTER 16

Data Integration for SAP ADSO sources using SAP Table Reader

This chapter includes the following topics:

- [SAP ADSO sources, 172](#)
- [Importing an SAP ADSO object, 173](#)

SAP ADSO sources

You can use SAP Table Reader Connector to connect to the SAP BW/4HANA application and read from SAP ADSOs.

SAP Advanced DataStore Object (ADSO) is the central object for data storage and data consolidation in the SAP BW system. ADSO is the primary persistent object in BW/4HANA and simplifies the modeling and support environment. ADSOs are commonly stored in 2-dimensional transparent database tables.

You can use SAP Table Reader Connector in Data Integration to read large volumes of data from the SAP BW/4HANA application.

Data Integration imports the following SAP ADSO information:

- ADSO name
- Description
- Type
- Info area
- Transfer structure
- Field information such as the name, type, description, precision, scale, SAP type, SAP length, SAP output length, and SAP decimals.

Importing an SAP ADSO object

To read from an SAP ADSO, use SAP Table Reader Connector. Import an ADSO object from SAP as a source in Data Integration mappings.

The naming convention of an ADSO is: /BIC/A<technical_name of ADSO>*, where * represents the table number associated with an ADSO.

When you import an ADSO into Cloud Data Integration, the Secure Agent imports the following five tables associated with each ADSO:

- /BIC/A<technical_name of ADSO>1. Inbound table for data store <technical_name of ADSO>.
- /BIC/A<technical_name of ADSO>2. Active data table for data store <technical_name of ADSO>.
- /BIC/A<technical_name of ADSO>3. Change log for data store <technical_name of ADSO>.
- /BIC/A<technical_name of ADSO>6. View for extraction from data store <technical_name of ADSO>.
- /BIC/A<technical_name of ADSO>7. View for reporting for datastore <technical_name of ADSO>.
- /BIC/A<technical_name of ADSO>8. View for external access (introduced in BW/4HANA 2.0 <technical_name of ADSO>.

The following image shows the five tables of an ADSO with technical name ZDELTA that you can import from BW/4HANA 1.0 into Cloud Data Integration:

The screenshot shows the 'Select Source Object' dialog in Informatica Data Integration. The search bar contains the query '/BIC/*|ZDELTA*'. Below the search bar, a table lists the results:

Select	Name	Label	Type
<input type="radio"/>	/BIC/AZDELTA2	Active Data Table for Data...	TRANSP
<input type="radio"/>	/BIC/AZDELTA3	Change Log for DataStore ...	TRANSP
<input type="radio"/>	/BIC/AZDELTA6	Generated Table for View	VIEW
<input type="radio"/>	/BIC/AZDELTA7	Generated Table for View	VIEW
<input type="radio"/>	/BIC/AZDELTA1	Inbound Table for DataSto...	TRANSP

CHAPTER 17

Data Integration for SAP ADSO targets using SAP ADSO Writer

This chapter includes the following topics:

- [SAP ADSO targets, 174](#)
- [Rules and guidelines for SAP ADSO targets, 174](#)

SAP ADSO targets

You can use SAP ADSO Writer Connector to connect to the SAP BW/4HANA application and write to ADSOs.

SAP Advanced DataStore Object (ADSO) is the central object for data storage and data consolidation in the SAP BW system. ADSO is the primary persistent object in BW/4HANA and simplifies the modeling and support environment. ADSOs are commonly stored in 2-dimensional transparent database tables.

You can use SAP ADSO Writer Connector in Data Integration to load large volumes of data to the target ADSO objects in the SAP BW/4HANA application.

Data Integration imports the following SAP ADSO information:

- ADSO name
- Description
- Type
- Info area
- Transfer structure
- Field information such as the name, type, description, precision, scale, SAP type, SAP length, SAP output length, and SAP decimals.

Rules and guidelines for SAP ADSO targets

Use the following rules and guidelines when you configure SAP ADSO targets:

- Only the activated ADSOs appear in the browser list of the SAP ADSO Writer Connector. Ensure that the required ADSO is activated in the SAP system before you can use in Data Integration.

- If the ADSO name has namespace (" / ") characters at the beginning, the Secure Agent replaces those characters with T___. Every subsequent namespace character in the ADSO name is replaced by " __ ". For example, if the ADSO name is /IMO/CMSD17, it appears in the browser list as T__IMO__CMSD17.
- Do not edit the field metadata as it might corrupt the extracted data.
- If the field name of the selected ADSO has a namespace character (" / "), the Secure Agent replaces it with an underscore " _ " character.
- When you define a mapping, you must select the operation as Insert. While activating, SAP BW/4HANA uses its algorithm to handle loaded data. Operations such as update and delete are handled at the BW/4HANA layer itself.
- Ensure that data with the different data types that you load to BW/4HANA is correct. The activation of the loaded packet might fail if the inserted data is incorrect.
- The Secure Agent does check the validity of the data according to the supported transformation data type. However, if the data is incorrect, the Secure Agent loads the data to SAP BW/4HANA, but fails during the data activation. Ensure that the data is valid according to the data type of the fields.
- The default packet size to write data is 8 MB. When you set the packet size value equal to greater than 8 MB and you encounter out-of-memory issues, you can increase the Java heap memory for the Secure Agent. In the **System Configuration Details** section of the Secure Agent properties, select **DTM** and set the **JVMOption1** property to the following value: *Xmx512m*. Click **OK** to save the change and then restart the Secure Agent. Adjust the value for the JVMOption1 property based on the amount of records you want to write and the available memory on the Secure Agent machine.
- The default precision for variable length data types such as STRING and RAWSTRING is set to a higher value of 1333. To manage the optimal record length, you must, however, set the length for these data types in the Edit Metadata Section of the mapping based on the expected length of the actual data.

CHAPTER 18

Mappings and mapping tasks with SAP ADSO Writer

This chapter includes the following topics:

- [Mapping and mapping tasks overview, 176](#)
- [SAP ADSO Extractor targets in mappings, 177](#)
- [Fixed partitioning for SAP ADSO targets, 178](#)
- [Configuring a mapping with an SAP ADSO target, 179](#)
- [Creating a mapping task, 180](#)

Mapping and mapping tasks overview

Use a mapping to define the data flow logic. Use the Data Integration Mapping Designer to configure mappings.

When you configure a mapping to describe the flow of data from source and target, you can also add transformations to transform data. A transformation includes field rules to define incoming fields. Links visually represent how data moves through the data flow.

After you create a mapping, you can run the mapping or you can deploy the mapping in a mapping task. The Mapping Configuration application allows you to process data based on the data flow logic defined in a mapping or integration template.

Use the Mapping task wizard to create a mapping task. When you create a mapping task, you select the mapping or integration template for the task to use.

If you configured parameters, which are placeholders for information, in a mapping, you can define the parameters in the mapping task. Defining parameters provides additional flexibility and allows you to use the same mapping in multiple mapping tasks. For example, you can use a parameter for a target connection in a mapping, and then define the target connection when you configure the mapping task.

When you create a mapping task, you can associate the task with a schedule to run it at specified times or on regular intervals. Or, you can run it manually. You can also configure advanced session properties. You can monitor tasks that are currently running and view details about completed tasks.

SAP ADSO Extractor targets in mappings

To write data to an SAP BW/4HANA application, configure an SAP ADSO object as the Target transformation in a mapping.

Specify the name and description of the SAP ADSO target. Configure the target and advanced properties for the target object.

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

Property	Description
Connection	Name of the source connection.
Target Type	The source type. Select from one of the following types: <ul style="list-style-type: none">- Single Object. Select to specify a single SAP ADSO object.- Parameter. Select to specify the SAP ADSO object as a parameter.
Object	Target object for the task. Click Select and then select the target object.
Operation	The type of operation for the task. Only Insert is applicable.
Preview Data	Not applicable.

The following table describes the SAP ADSO Writer advanced target properties:

Property	Description
Activate Option Mode	Loads the data into the target ADSO object and then sends data activation requests to SAP BW/4HANA based on the activate options you select. You can select from the following activate options: <ul style="list-style-type: none">- 0-Do Not Activate. Does not send an activate request.- 1-Activate. Creates a single activation request for all load requests in the queue.- 2-Activate Request by Request. Creates a separate activation request for each of the load requests in the queue.- Parameter. Use this option to parameterize the activate options. Specify a valid activate option value in the Parameter Name for Activate Option Mode field. Default is Do Not Activate.
Parameter Name for Activate Option Mode	The parameter name that you defined for the Activate Option Mode in the parameter file. You can specify the following values for the data fetch mode: <ul style="list-style-type: none">- 0 for Do Not Activate- 1 for Activate- 2 for Activate Request by Request If you pass any other value, the jobs fail when you run the mapping,

Property	Description
Packet size in MB	The packet size of each SAP data packet while writing data to SAP BW4/HANA. Default value is 10 MB.
Tracing	Sets the amount of detail that appears in the log file. You can choose terse, normal, verbose initialization, or verbose data. Default is normal

Activate option mode for SAP ADSO Writer mappings

You can select the activate option mode when you load data to the ADSO target in SAP BW/4HANA.

When you specify the activate mode, the Secure Agent first loads the data into the target ADSO object and then sends the data activation requests to SAP BW/4HANA based on the following activate options you select:

- **0-Do Not Activate.** Does not send an activate request and the activation preprocessing does not occur.
- **1-Activate.** Creates a single activation request for all load requests in the queue.
- **2-Activate Request by Request.** Creates a separate activation request for each of the load requests in the queue.

The activation request activates all the previous load requests in the queue that are pending for activation. Activation occurs per load request in a chronological sequence, starting from the earliest pending request to the most recent load request. The Secure Agent waits for the activation to be fully processed in SAP BW/4HANA system. The wait time depends upon the number of load requests in the queue that were available earlier to the load request associated with the current mapping.

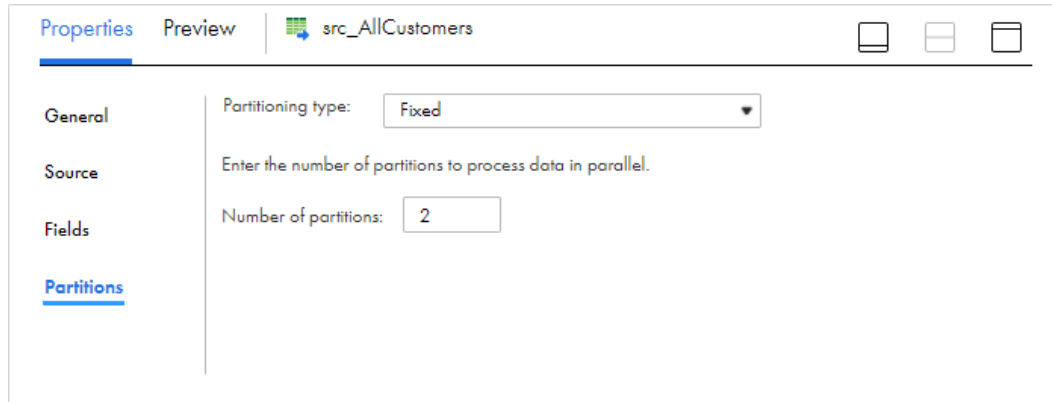
During the activation process, if the activation of a specific load request fails, the whole activation process fails and the rest of the load requests are also not activated. In such cases, the mapping fails even though the Secure Agent loaded the data correctly based on the enabled activate mode.

Fixed partitioning for SAP ADSO targets

You can configure fixed partitioning in a mapping that writes to SAP ADSO targets.

Enable partitioning when you configure the Source transformation in the Mapping Designer. You do not have to enable fixed partitioning in the Target transformation. The Secure Agent considers the same number of partitions you specified for the source as the target partition number.

On the **Partitions** tab for the Source transformation, you select fixed partitioning and enter the number of partitions, as shown in the following image:



When you run the mapping, the Secure Agent distributes rows of data for the target based on the number of partitions that you specify in the Source transformation. You can specify up to 64 partitions.

Configuring a mapping with an SAP ADSO target

Use the Data Integration Mapping Designer to configure a mapping.

1. To create a mapping, click **Data Integration > New > Mappings**. Select **Mapping** and click **Create**.
2. Enter a name and description for the mapping, and click **OK**.
You can use alphanumeric characters and underscores (_) in the mapping name.
3. To configure a source, on the **Transformation palette**, click **Source**.
4. In the **Properties** panel, on the **General** tab, enter a name and description.
5. Click the **Source** tab and configure source details.
6. Specify the source type. You can choose one of the following options:
 - Select **Single Object** to select a single SAP object.
 - Select **Parameter** to configure the source objects in a mapping task associated with this mapping.
7. Click **Query Options** in the **Source** tab to specify any filter for the SAP ADSO object.
8. Click **Advanced** to specify the advanced source properties.
Note: You cannot add or remove source fields or edit the field metadata.
9. To add a transformation, on the **Transformation palette**, click the transformation name. Or, drag the transformation onto the mapping canvas.
 - a. On the **General** tab, you can enter a name and description for the transformation.
 - b. Draw a link to connect the previous transformation to the transformation.
When you link transformations, the downstream transformation inherits the incoming fields from the previous transformation.
For a Joiner transformation, draw a master link and a detail link.
 - c. To preview fields, configure the field rules, or rename fields, click **Incoming Fields**.

- d. Configure additional transformation properties, as needed.
The properties that you configure vary based on the type of transformation you create.
- e. To add another transformation, repeat these steps.
10. To add an ODSO object to the Target transformation, on the **Transformation palette**, click **Target**.
 - a. On the **General** tab, you can enter a name and description.
 - b. Draw a link to connect the previous transformation to the Target transformation.
 - c. Click the **Target** tab, configure the target details. Specify the target type:
 - Select **Single Object** to select an ADSO object.
 - Select **Parameter** to configure the target objects in a mapping task associated with this mapping.
 - Select **Operation** as **Insert**.
 - Click **Advanced** and specify the advanced target properties.
 - d. Click **Field Mapping** and map the fields that you want to write to the target.
 - e. To add another Target transformation, repeat these steps.
11. Click the **Field Mapping** to map the Source and Target fields.
You can use the Automatic option if the fields are similar between the source and target.
12. Save and run the mapping or save and create a mapping task.

Creating a mapping task

You can create a mapping task based on a valid mapping or integration template on the Mappings page.

1. To create a mapping task, click **Data Integration > New > Tasks**.
2. Enter a name for the task.
Task names must be unique within the organization. Task names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Task names are not case sensitive.
3. Select the runtime environment that contains the Secure Agent that you want to use to access the SAP ADSO Writer connection.
4. Select **Mapping** as the task based on which you want to create the mapping task.
5. Click **Select** to specify a mapping.
The **Select a Mapping** dialog box appears.
6. Select a mapping or search for the required mapping and select **OK**.
The image of the selected mapping appears.
7. Click **Next**.
If you specified any parameters in the source or target details in the mapping, the Source or Target page appears. If not, the Schedule page appears.
8. Click **Next** to configure a schedule and advanced options. Perform any of the following steps based on your requirements.
 - a. Click **Run this task on schedule** and specify the schedule you want to use.

- b. Configure the email notification options.
 - c. Configure advanced options for the task.
 - d. Configure the advanced target properties.
 - e. Specify the execution mode.
- 9. Optionally, add the advanced session properties.
 - a. Click **Add**.
 - b. Select a session property.
 - c. Configure the value of the session property.
- 10. Save and run the mapping task.

APPENDIX A

SAP data type reference

This appendix includes the following topics:

- [SAP data type reference overview, 182](#)
- [SAP and transformation data types, 183](#)
- [SAP BW and transformation data types, 185](#)

SAP data type reference overview

Data Integration uses the following data types in mappings, synchronization tasks, and mapping tasks with SAP:

Native data types

Native data types are data types specific to the source and target databases or flat files. They appear in non-SAP sources and targets in the mapping.

SAP data types

SAP data types appear in the Fields tab for Source and Target transformations when you choose to edit metadata for the fields. SAP performs any necessary conversion between the SAP data types and the native data types of the underlying source database tables.

Transformation data types

Set of data types that appear in the remaining transformations. They are internal data types based on ANSI SQL-92 generic data types, which Data Integration uses to move data across platforms.

Transformation data types appear in all remaining transformations in a mapping, synchronization task, or mapping task.

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.

SAP and transformation data types

The following table lists the SAP data types that SAP Table Connector and SAP IDocs and RFCs/BAPI Connector support along with the corresponding transformation data types:

SAP Data Type	Transformation Data Type	Range for Transformation Data Type
ACCP	Date/time	Jan 1, 0001 A.D. to Dec 31, 9999 A.D.
CHAR	String	1 to 104,857,600 characters Fixed-length or varying-length string.
CLNT	String	1 to 104,857,600 characters Fixed-length or varying-length string.
CUKY	String	1 to 104,857,600 characters Fixed-length or varying-length string.
CURR	Decimal	Precision 1 to 28 digits, scale 0 to 28
DATS	Date/time	Jan 1, 0001 A.D. to Dec 31, 9999 A.D. Precision to the nanosecond.
DEC	Decimal	Precision 1 to 28 digits, scale 0 to 28
DF16_DEC	Decfloat16	Range of 1-15 and scaling of maximum 14. Decimal floating point number stored in BCD format. You can use the DF16_DEC data type in the following scenarios: <ul style="list-style-type: none"> - When you read data from and write data to SAP tables - When you configure SAP BAPI Connector as a business service within a mapping or a mapping task to integrate with SAP - When you use SAP BAPI/RFC mapplets to integrate with SAP
DF34_DEC	Decfloat34	Range of 1-31 and scaling of maximum 30. Decimal floating point number stored in BCD format. You can use the DF34_DEC data type in the following scenarios: <ul style="list-style-type: none"> - When you read data from and write data to SAP tables - When you configure SAP BAPI Connector as a business service within a mapping or a mapping task to integrate with SAP
DF16_RAW	Double	Maximum of 16 positions with floating decimal. Decimal floating point number stored in binary format. You can use the DF34_DEC data type in the following scenarios: <ul style="list-style-type: none"> - When you read data from and write data to SAP tables - When you configure SAP BAPI Connector as a business service within a mapping or a mapping task to integrate with SAP - When you use SAP BAPI/RFC mapplets to integrate with SAP
DF34_RAW	Double	Maximum of 34 positions with floating decimal. Decimal floating point number stored in binary format. You can use the DF34_DEC data type in the following scenarios: <ul style="list-style-type: none"> - When you read data from and write data to SAP tables - When you configure SAP BAPI Connector as a business service within a mapping or a mapping task to integrate with SAP - When you use SAP BAPI/RFC mapplets to integrate with SAP

SAP Data Type	Transformation Data Type	Range for Transformation Data Type
FLTP	Double	Precision 15, scale 0
INT1	Small Integer	Precision 5, scale 0
INT2	Small Integer	Precision 5, scale 0
INT4	Integer	Precision 10, scale 0
INT8	Int8	8-byte integer between -9,223,372,036,854,775,808 and +9,223,372,036,854,775,807. The length is set at 19 positions. Use the INT8 data type when you read data from and write data to SAP tables.
LANG	String	1 to 104,857,600 characters Fixed-length or varying-length string.
LCHR	String	1 to 104,857,600 characters Fixed-length or varying-length string.
LRAW	Binary	Uninterrupted sequence of bytes with a maximum length of 255 positions.
NUMC	String	1 to 104,857,600 characters Fixed-length or varying-length string.
PREC	Binary	Uninterrupted sequence of bytes with a maximum length of 255 positions.
QUAN	Decimal	Precision 1 to 28 digits, scale 0 to 28
RAW	Binary	Uninterrupted sequence of bytes with a maximum length of 255 positions.
RAWSTRING	Binary	Uninterrupted byte string. You can use the RAWSTRING data type in the following scenarios: <ul style="list-style-type: none"> - When you read data from and write data to SAP tables - When you use IDocs to integrate with SAP - When you use SAP BAPI/RFC mapplets to integrate with SAP
SSTRING	String	Small Character string. You can use the SSTRING data type in the following scenarios: <ul style="list-style-type: none"> - When you read data from and write data to SAP tables - When you use SAP BAPI/RFC mapplets to integrate with SAP
STRING	String	Character string. You can use the STRING data type in the following scenarios: <ul style="list-style-type: none"> - When you read data from and write data to SAP tables - When you use SAP BAPI/RFC mapplets to integrate with SAP - When you use IDocs to integrate with SAP
TIMS	Date/time	Jan 1, 0001 A.D. to Dec 31, 9999 A.D. Precision to the nanosecond.

SAP Data Type	Transformation Data Type	Range for Transformation Data Type
UNIT	String	1 to 104,857,600 characters Fixed-length or varying-length string.
VARC	String	1 to 104,857,600 characters Fixed-length or varying-length string.

Rules and guidelines for SSTRING, STRING, and RAWSTRING data types

When you import metadata that contains a SSTRING, STRING or RAWSTRING data type with precision that is not defined in SAP, you must set the **SapTableReaderPrecision** custom property for the Secure Agent and specify the required precision.

Perform the following steps to configure the custom property for the Secure Agent:

1. Log on to Informatica Intelligent Cloud Services.
2. Click **Administrator**.
3. In the navigation bar, select the **Runtime Environments** tab.
4. In the Runtime Environments page, select the Secure Agent used for running the SAP task.
5. Select **Edit** on the top right-hand corner.
6. In the **System Configuration Details** section, add a custom property.
7. Select **Service** as **Data Integration Service**, and then select **Type** as **Tomcat**.
8. In the **Name** field, specify **SapTableReaderPrecision**, and in the **Value** field, set the required precision.
9. Click **Save**.

SAP BW and transformation data types

The following table lists the SAP data types that SAP BW Connector supports along with the corresponding transformation data types:

SAP Data Type	Transformation Data Type	Range for Transformation Data Type
CHAR	String	1 to 104,857,600 characters Fixed-length or varying-length string.
CUKY	String	1 to 104,857,600 characters Fixed-length or varying-length string.
CURR	Decimal	Precision 1 to 28 digits, scale 0 to 28
DATS	Date/time	Jan 1, 0001 A.D. to Dec 31, 9999 A.D. Precision to the nanosecond.

SAP Data Type	Transformation Data Type	Range for Transformation Data Type
DEC	Double	Precision 1 to 28 digits, scale 0 to 28
FLTP	Double	Precision 15, scale 0
INT4	Integer	Precision 10, scale 0
LANG	String	1 to 104,857,600 characters Fixed-length or varying-length string.
NUMC	String	1 to 104,857,600 characters Fixed-length or varying-length string.
QUAN	Decimal	Precision 1 to 28 digits, scale 0 to 28
TIMS	Date/time	Jan 1, 0001 A.D. to Dec 31, 9999 A.D. Precision to the nanosecond.
UNIT	String	1 to 104,857,600 characters Fixed-length or varying-length string.

INDEX

A

ADSO targets
rules and guidelines in mapping tasks [174](#)

B

BAPI/RFC
configuring mappings [120](#)
map error output [118](#)
mapping example [121](#)
nested structure [116](#)
BAPI/RFC mappings
configuring [120](#)
configuring mapping example [124](#)
example [121](#)
generate mapplet example [123](#)
overview [119](#)
BAPI/RFC mapplets
integration ID [117](#)
overview [114](#)
parameters [115](#)
rules and guidelines [118](#)
BAPI/RFC parameter
properties [115](#)
system variables [117](#)

C

certificate
converting to PSE format [28](#)
importing to SAP [28](#)
Cloud Application Integration community
URL [9](#)
Cloud Developer community
URL [9](#)
configuring key range
partitioning for SAP table sources [104](#)
connections
SAP ADSO Writer [61](#), [62](#)
configuration for SAP ADSO Writer connections [48](#)
configuration for SAP IDoc and RFC/BAPI connections [30](#)
configuration for SAP ODP Extractor connections [43](#)
configuration for SAP table connections [17](#), [18](#), [31](#)
SAP [56](#)
SAP ADSO Writer [61](#), [62](#)
SAP ADSO Writer configuration requirements [49](#)
SAP BW Reader [59](#)
SAP configuration requirements [25](#), [44](#), [49](#)
SAP IDoc Reader [58](#)
SAP IDoc Writer [58](#)
SAP ODP Extractor [66](#)
SAP ODP Extractor configuration requirements [44](#)
SAP RFC/BAPI Interface [57](#)

connections (*continued*)
SAP Table [55](#)
creating
SAP Table connections [70](#)

D

Data Integration community
URL [9](#)
data types
SAP [182](#)
defining logical system
configuration for SAP IDoc connections [35](#)

H

HTTPS
configuring [26](#)
HTTPS configuration
enable service on SAP [28](#)
overview [26](#)
prerequisites [26](#)

I

IDoc mappings
overview [137](#)
read example [141](#), [147](#)
IDoc mapplets
importing [139](#)
importing example [144](#), [149](#)
overview [128](#)
IDoc Reader mappings
sources [138](#)
IDocs
importing metadata [135](#)
importing metadata example [142](#), [148](#)
mapping read example [141](#), [147](#)
primary and foreign keys [133](#)
properties [130](#)
importing certificate
SAP trust store [28](#)
importing IDocs
MATMAS example [142](#), [148](#)
inbound mappings
configuring to write IDocs [140](#)
configuring to write IDocs example [149](#)
Informatica Global Customer Support
contact information [10](#)
Informatica Intelligent Cloud Services
web site [9](#)

L

libraries

- to read from and write to SAP tables [18](#)
- to read from SAP ODP [47](#), [51](#)
- to read from SAP tables [18](#)
- to write to SAP tables [19](#)

load balancing connection

- entry in sapnwrfc.ini [22](#), [33](#)

logical system

- creating for SAP Connector [36](#)
- defining SAP Connector [35](#)
- SAP, program ID [36](#)

M

maintenance outages [10](#)

mapping example

- SAP Table source [107](#)

mapping tasks

- creating [160](#)
- rules and guidelines for SAP ADSO targets [174](#)
- rules and guidelines for SAP ODP sources [164](#)

Mapping tasks

- creating [106](#), [170](#), [180](#)
- overview [95](#), [165](#), [176](#)

mappings

- IDoc Reader sources [138](#)
- overview [95](#), [165](#), [176](#)
- SAP ADSO targets [177](#)
- SAP ODP sources [166](#)
- SAP Table lookups [104](#)
- SAP Table source example [107](#)
- SAP Table sources [96](#)

mapplet

- outbound [131](#)

mapplets

- BAPI/RFC [114](#)
- inbound [132](#)

O

ODP sources

- rules and guidelines in mapping tasks [164](#)

OpenSSL certificate

- converting to PSE format [28](#)
- creating [26](#)

organization ID

- finding [78](#)

organizations

- finding your organization ID [78](#)

outbound mappings

- configuring to read IDocs [139](#)
- configuring to read IDocs example [145](#)

outbound mapplet

- map error output [132](#)
- ports [131](#)

P

Partitioning

- key range partitioning for SAP table sources [103](#), [168](#), [178](#)

partner profile

- creating outbound and inbound parameters [37](#)
- SAP ALE integration [37](#)

program ID

- ALE integration [36](#)
- SAP, logical system [36](#)
- sapnwrfc.ini file [22](#), [33](#)

R

RFC destination

- creating tRFC port [36](#)

RFC server program connection

- entry in sapnwrfc.ini [22](#), [33](#)

rules and guidelines

- BAPI/RFC mapplets [118](#)

S

SAP

- additional configuration for SAP ADSO Writer connections [48](#)
- additional configuration for SAP ODP Extractor connections [43](#)
- additional configuration for SAP table connections [17](#), [18](#), [31](#)
- data types [182](#)
- installing transport files for processing SAP ADSO [49](#)
- installing transport files for processing SAP ODPs [44](#)
- installing transport files for processing table data [25](#)
- installing transport files for reading SAP ODPs [44](#), [49](#)

SAP ADSO Writer

- connection properties [62](#)
- to load data to SAP ADSO [48](#)

SAP ADSO Writer connection

- creating [74](#)

SAP ADSO Writer connections

- overview [61](#)

SAP ADSO Writer Connector administration

- licenses for SAP ADSO Writer Connector [48](#)

SAP ADSO Writer mappings

- configuring [179](#)

SAP BW Connector administration

- licenses for SAP BW Connector [40](#)

SAP BW mappings

- configuring [158](#)

SAP BW Reader

- connection properties [59](#)

SAP BW Reader connection

- creating [73](#)

SAP configuration requirements

- whitelisting the Secure Agent for reading SAP table data [29](#)

SAP connections

- IDoc and BAPI/RFC [57](#)
- overview [54](#)
- rules and guidelines [56](#)

SAP Connector

- communication interfaces [15](#)
- integration methods [12](#)
- overview [12](#)
- user authorizations [38](#), [43](#)

SAP Connector administration

- overview [17](#)

SAP IDoc Reader

- connection properties [58](#)

SAP IDoc Reader connection

- creating [71](#)

SAP IDoc Writer

- connection properties [58](#)

SAP IDoc Writer connection

- creating [72](#)

- SAP IDocs and RFCs/BAPI Connector administration
 - licenses for SAP IDocs and RFCs/BAPI Connector [30](#)
- SAP integration methods
 - overview [12](#)
 - using BAPI/RFC functions [13](#)
 - using IDocs [13](#)
 - using SAP ADSO Writer [14](#)
 - using SAP ODP Extractor [14](#)
 - using SAP Table [13](#)
- SAP libraries
 - for SAP IDoc and RFC/BAPI connections [18](#), [31](#)
 - to read from and write to SAP tables [18](#)
 - to read from SAP ODP [47](#), [51](#)
 - to read from SAP tables [18](#)
 - to write to SAP tables [19](#)
- SAP Metadata utility
 - installation and configuration [39](#)
 - installing and configuring [39](#)
 - overview [15](#)
 - prerequisites [39](#)
- SAP notes
 - to read from SAP ODPs [44](#)
 - to write to SAP ADSO [48](#)
- SAP ODP
 - configuring [45](#)
 - user authorization [45](#)
- SAP ODP Extractor connection
 - creating [76](#)
- SAP ODP Extractor connections
 - overview [66](#)
- SAP ODP Extractor Connector administration
 - licenses for SAP ODP Extractor Connector [43](#)
- SAP ODP Extractor mappings
 - configuring [169](#)
- SAP RFC/BAPI connection
 - creating [72](#)
- SAP RFC/BAPI Interface
 - connection properties [57](#)
- SAP sources
 - ODP [163](#)
 - tables and views [81](#)
- SAP sources and targets
 - rules and guidelines in Synchronization tasks [82](#)
- SAP Table
 - connection properties [55](#)
- SAP table connections
 - troubleshooting [79](#)
- SAP Table connections
 - creating [70](#)
 - overview [55](#)
- SAP Table Connector administration
 - licenses for SAP Table Connector [18](#)

- SAP Table mapping example
 - defining the mapping [107](#)
- SAP Table mappings
 - configuring [105](#)
- SAP targets
 - ADSO [172](#), [174](#)
- SAP user authorization
 - configuring to process table data [24](#)
- sapnwrfc.ini
 - connections [22](#), [33](#)
- segments and groups
 - overview [128](#)
 - status [129](#)
- specific application server connection
 - entry in sapnwrfc.ini [22](#), [33](#)
- status
 - Informatica Intelligent Cloud Services [10](#)
 - segments and groups [129](#)
- Synchronization tasks
 - example [90](#)
 - monitoring [90](#)
 - multiple SAP object sources [88](#)
 - overview [84](#)
 - rules and guidelines for SAP sources and targets [82](#)
 - SAP Table lookups [86](#)
 - SAP Table sources [84](#)
 - single SAP BW source [155](#)
 - single SAP object source [86](#)
 - system status [10](#)

T

- tRFC port
 - configuring for IDoc connections [36](#)
- trust site
 - description [10](#)

U

- upgrade notifications [10](#)

W

- web site [9](#)
- whitelisting the Secure Agent for reading SAP table data
 - SAP configuration requirements [29](#)