Oracle® Identity Manager

Connector Guide for SAP Employee Reconciliation - HCM

9.1.2
E11210-24
March 2021

ORACLE

Oracle Identity Manager Connector Guide for SAP Employee Reconciliation - HCM, 9.1.2

E11210-24

Primary Author: Gowri.G.R

Contributing Authors: Alankrita Prakash

Contents

2 Deploying the Connector

3 Using the Connector

List of Figures

List of Tables

Preface

This guide describes the connector that is used to onboard applications for flat files, exported from various enterprise target systems, to Oracle Identity Governance.

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For information about installing and using Oracle Identity Manager, visit the following Oracle Help Center page:

http://docs.oracle.com/cd/E52734_01/index.html

For information about Oracle Identity Manager Connectors documentation, visit the following Oracle Help Center page:

http://docs.oracle.com/cd/E22999_01/index.htm

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in this Guide?

This chapter provides an overview of the updates made to the software and documentation for release 9.1.2.7 of the SAP Employee Reconciliation - HCM connector.

The updates discussed in this chapter are divided into the following categories:

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

  These include major changes made to the connector documentation. These changes are not related to software updates.

Software Updates

The following are software updates and issues resolved in release 9.1.2.7.1 and 9.1.2.7.0:

The following are software updates and issues resolved in release 9.1.2.7.1:

Bug Number	Issue	Resolution
25603451	Receiving error in the scheduler after parsing of IDoc XML is the connector	This issue has been resolved.
18669492	Mechanism needed to track IDoc numbers against employee numbers of users.	This issue has been resolved.
13520610	Requirement to remove a SAP connection to process IDoc flat files.	This issue has been resolved.
26246139	Missing resource in the connector resource bundle for UDF attribtes.	This issue has been resolved.
26035915	Batch reconciliation implemented for the SAP ER connector.	This issue has been resolved.
18668482	IDocs are picked up by the SAP HRMS listener but stay in data received state for long.	This issue has been resolved.
30703415	Update connector name SAP Employee Reconciliation to SAP Employee Reconcilation - HCM connector.	This issue has been resolved.

The following are software updates and issues resolved in release 9.1.2.7.0:

Bug Number	Issue	Resolution
16941269	Wrong Manager Id was updated to the user	This issue has been resolved.
17047491	Update Manager Scheduled Task is not working	This issue has been resolved.
16989933	Update Manager Scheduled Task is throwing invalid DataFormat Exception	This issue has been resolved.
16772203	Error loggers should be changed to Info logger for HRMS Listener	This issue has been resolved.
16793231	Install SAP ER 9.1.2.5 Connector Unable to edit GTC Connector	This issue has been resolved.
17211711	Update Manager scheduled task not working properly when the "update users with empty manger id only" parameter is set to YES	This issue has been resolved.
17796698	SAP ER connector creates multiple events for same change	This issue has been resolved.
19319985	SAP ER connector 9.1.2.6.5 is not able to create deferred events for changes on identites which are not classified as HIRE, REHIRE or TERMINATE	This issue has been resolved.
23482998	SAP ER connector fail to read it, when "Middle Name" field value is only 1 character long in the IDOC	This issue has been resolved.
23344445	SAP ER connector support for IDOC in XML format	This issue has been resolved.
23320012	SAP ER connector fails to connect to SAP Gateway and Message Server	This issue has been resolved.

Documentation-Specific Updates

The following are documentation-specific updates in release 9.1.2.7.1 and 9.1.2.7.0:

The following are documentation-specific updates in release 9.1.2.7.1:

The following documentation-specific updates have been made for revision "24" of this guide:

- The "Target Systems" row of Table 1-1 has been modified to include support for SAP S/4HANA 2020 with component S4CORE 105 SP 0000.

The following documentation-specific updates have been made for revision "23" of this guide:

- The "Target Systems" row of Table 1-1 has been modified to include support for SAP S/4HANA 1909 with component S4CORE 104 SP 0000.
- Creating a Target System User Account for Connector Operations has been updated.

The following documentation-specific updates have been made for revision "22" of this guide:

- The connector name has been changed from SAP Employee Reconciliation to SAP Employee Reconciliation - HCM throughout the guide.
- Several values present in Creating a Target System User Account for Connector Operations have been modified.
- A screenshot present in Registering the Listener with the SAP Gateway (tRFC) has been updated.
- Added an entry for Code key parameter Idoc Number to Table 1-5 of Predefined Lookup Definitions.
- Added entries for Code key parameters Sub Type Field and Begin Date field to Table 2-2 of Setting Up the Lookup.SAP.HRMS.Configuration Lookup Definition in Oracle Identity Manager.
- Updated the contents of the SAP-ER_fr.properties file listed in Copying Resource Bundle Entries for UDFs.

The following are documentation-specific updates in release 9.1.2.7.0:

The following documentation-specific update has been made for revision "21" of this guide:

The following sections have been added:

- Checking Whether a Sender Logical System Already Exists
- Defining the Sending and Receiver Logical Systems
- Assigning a Client to the Sender Logical System
- Defining the Distribution Model
- Creating the File Port
- Defining the Partner Profile
- Registering the Listener with the SAP Gateway (tRFC)
- Creating the tRFC Port
- Generating IDocs
- Specifying the Mode of Reconciliation in the Partner Profile
- Scheduling Jobs on the Target System for Incremental Reconciliation

The following documentation-specific updates have been made for revision "20" of this guide:

- The "Target Systems" row of Table 1-1 has been modified to include support for SAP S/4HANA 1809 with component S4CORE 103 SP 0000.
- The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to include support for Oracle Identity Governance 12c (12.2.1.4.0).
- Usage Recommendation has been modified to include support for Oracle Identity Governance 12c (12.2.1.4.0).
- Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System has been modified.
- A "Note" has been added to Files and Directories on the Installation Media.
- The solution documented for an issue related to connecting to SAP through SNC has been modified in Common SNC Errors.

The following documentation-specific updates have been made for revision "19" of this guide:

- The "Oracle Identity Manager" row of Table 1-1 has been renamed as "Oracle Identity Governance or Oracle Identity Manager" and updated to certify Oracle Identity Governance 12c (12.2.1.3.0).
- Usage Recommendation has been updated to include support for Oracle Identity Governance 12c (12.2.1.3.0).
- Setting Up the Lookup.SAP.HRMS.Configuration Lookup Definition in Oracle Identity Manager has been modified to include steps about setting or modifying a decode value in the lookup deifnition for OIM 11.1.2.1.0 or later.
- Step 2 of Verifying Segment Details in Lookup Definitions has been modified to include steps for verifying segment details in OIM 11.1.2.1.0 or later.
- Step 3 of Mapping New Connection Properties has been modified to include steps for creating a mapping between the connection property and the IT resource parameter in OIM 11.1.2.1.0 or later.
- Configuring the Target System to Resend IDocs and Manually Sending IDocs have been added.
- Step 2 of Adding Attribute Mapping has been modified to include steps for adding the attribute mapping in the Lookup.SAP.HRMS.AttributeMapping lookup in OIM 11.1.2.1.0 or later.
- Adding Attribute Mapping has been modified to inlcude steps for modifying the field lengths on the OIM user form in OIM 11.1.2.1.0 or later.

The following documentation-specific updates have been made for revision "18" of this guide:

- Oracle Identity Manager 9.*x* content has been removed throughout the document.
- The JDK, Target System, and External Code rows in Table 1-1 have been updated.
- Usage Recommendation has been modified to remove support to 9.0.4.x version of the connector with OIM 11g.
- Information pertaining to procedures performed on the target system has been replaced with a high-level summary in the following sections:
  - Reconciliation of the Manager ID Attribute
  - Creating a Target System User Account for Connector Operations
  - Downloading and Installing the SAP JCo
  - Verifying Segment Details in Lookup Definitions
  - Configuring Reconciliation of Effective-Dated Target System Events
  - Adding Attribute Mapping
- SAP ER Connector Support for IDoc in XML Format has been added.
- Section "Determining the Release Number of the Connector" has been removed as it is related to OIM 9.*x*.
- Creating a Backup of the Existing Common.jar File has been modified.
- The following rows have been added to Table 2-2:
  - Is Future Dated Event Handling Enabled

  - Is IDOC File Format in XML
  - Recon Rule Attribute Lookup
- The description for the parameter "Gateway host" of Table 2-6 has been updated.
- Common SNC Errors has been updated to include SNC issues.
- Known Issues has been updated to include bug 18668482.

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. This guide discusses the connector that enables you to use SAP HRMS as an authoritative (trusted) source of identity data for Oracle Identity Manager.

In the identity reconciliation (trusted source) mode of the connector, identities are created or modified only on the target system and data about these identities is reconciled into Oracle Identity Manager. The user data reconciled from the target system is used to create or update OIM Users.

> **Note:**
>
> At some places in this guide, SAP HRMS is referred to as the **target system**.
> This chapter contains the following sections:

- Certified Components
- Usage Recommendation
- Certified Languages
- Connector Architecture
- Features of the Connector
- Connector Objects Used During Reconciliation

> **Note:**
>
> In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed. At some places in this guide, SAP HRMS has been referred to as the target system.

1.1 Certified Components

Table 1-1 lists the certified components for the connector.

Table 1-1 Certified Components

Component	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* release 1 (11.1.1.3.0) and any later BP in this release track **Note**: In this guide, Oracle Identity Manager release 11.1.1 has been used to denote Oracle Identity Manager release 11g release 1 (11.1.1) and future releases in the 11.1.1.*x* series that the connector will support. • Oracle Identity Manager 11*g* release 1 PS1 (11.1.1.5.0) and any later BP in this release track • Oracle Identity Manager 11*g* release 1 PS2 (11.1.1.7.0) and any later BP in this release track • Oracle Identity Manager 11*g* release 2 BP04 (11.1.2.0.4) and any later BP in this release track. **Note**: In this guide, Oracle Identity Manager release 11.1.2 has been used to denote Oracle Identity Manager release 11*g* release 2 BP04 (11.1.2.0.4) and future releases in the 11.1.2.*x* series that the connector will support. • Oracle Identity Manager 11*g* release 2 PS1 (11.1.2.1.0) and any later BP in this release track • Oracle Identity Manager 11*g* release 2 PS2 (11.1.2.2.0) and any later BP in this release track • Oracle Identity Manager 11*g* release 2 PS3 (11.1.2.3.0) and any later BP in this release track The connector does not support Oracle Identity Manager running on Oracle Application Server. For detailed information about certified components of Oracle Identity Manager, see the certification matrix on Oracle Technology Network at http://www.oracle.com/technetwork/documentation/oim1014-097544.html **Note**: If Oracle Identity Manager is running on Oracle WebLogic Server and using JRockit, then the scheduled task configured as a listener on Oracle Identity Manager might fail. It is recommended that you use SUN JVM. The listener is described later in this chapter.

Table 1-1 (Cont.) Certified Components

Component	Requirement
JDK	For Oracle Identity Manager release 11.1.*x* and 11.1.2.*x*, Sun/IBM JDK 1.6 update 18 or later. **Note**: JRockit is not supported because it is incompatible with the SAP JCo libraries.
Target system	The target system can be any one of the following: • SAP R/3 4.7 SP 45 (running on WAS 6.20) BASIS SP 48 or later • mySAP ERP 2004 (ECC 5.0 running on WAS 6.40) BASIS SP 22 or later • mySAP ERP 2005 (ECC 6.0 running on WAS 7.00) BASIS SP 13 or later • SAP ERP 6.0 (running on SAP NetWeaver 7.0 or later) with EHP 1 to 6 • SAP ERP 6.0 (running on SAP NetWeaver 7.4 or later) with EHP7 • SAP ERP 6.0 (running on SAP NetWeaver 7.5 or later) with EHP 8 • SAP S/4HANA 1809 with component S4CORE Release 103 SP 0000 • SAP S/4HANA 1909 with component S4CORE Release 104 SP 0000 • SAP S/4HANA 2020 with component S4CORE Release 105 SP 0000 **Note**: From version 6.40 onward, SAP WAS is also known as "SAP NetWeaver."
External Code	The connector works with SAP JCo 3.0.2 or later. The following SAP custom code files are required: • sapjco3.jar version 3.0.2 or later • sapidoc3.jar version 3.0.12 or later • Additional file for Microsoft Windows: sapjco3.dll version 3.0.2 • Additional file for AIX, Solaris, and Linux: libsapjco3.so version 3.0.2 **Note**: There are different distribution packages (JCo) 3.0.2 available for various supported platforms and processors. See, JCo documentation for more information about using JCo 3.0.2 packages as per your environment.

1.2 Usage Recommendation

If you are using any of the following versions of Oracle Identity Manager, then you must use the 9.1.2.*x* version of this connector:

- Oracle Identity Governance 12*c* (12.2.1.4.0) and any later BP in this release track
- Oracle Identity Governance 12*c* (12.2.1.3.0) and any later BP in this release track

- Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) or later
- Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) or later
- Oracle Identity Manager 11*g* Release 2 PS1 (11.1.2.1.0) or later
- Oracle Identity Manager 11*g* Release 2 BP04 (11.1.2.0.4) or later
- Oracle Identity Manager 11*g* Release 1 PS2 (11.1.1.7.0) or later
- Oracle Identity Manager 11*g* Release 1 PS1 (11.1.1.5.0) or later
- Oracle Identity Manager 11*g* Release 1 (11.1.1.3.0) or later

1.3 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- English
- French
- German
- Italian
- Japanese
- Portuguese (Brazilian)
- Korean
- Spanish

1.4 Connector Architecture

> **Note:**
>
> This guide provides only an overview of the SAP data components and processes that are used during reconciliation with the target system. For detailed information about ALE, see the SAP Help documentation at http://help.sap.com.

The target system is configured as a trusted source of identity data for Oracle Identity Manager. In other words, identity data that is created and updated on the target system is fetched into Oracle Identity Manager and used to create and update OIM Users.

IDocs (interchange documents) are the medium of data interchange between SAP HRMS and Oracle Identity Manager. IDocs are ASCII-based flat files containing lines of text that are ordered into data fields. A typical IDoc contains a header line (control record) followed one or many data lines (data records). In the Oracle Identity Manager

context, IDocs are used to transfer user data from the target system to Oracle Identity Manager. You can set the number of user records that must be recorded in an IDoc.

An IDoc type defines the structure of data in an IDoc. All IDocs adhere to the structural requirements imposed by their IDoc type. In other words, individual IDocs can be seen as instances of an IDoc type. The connector supports all IDoc types that are associated with the HRMD_A message type. A message type is a definition of the type of data generated and sent out from the target system.

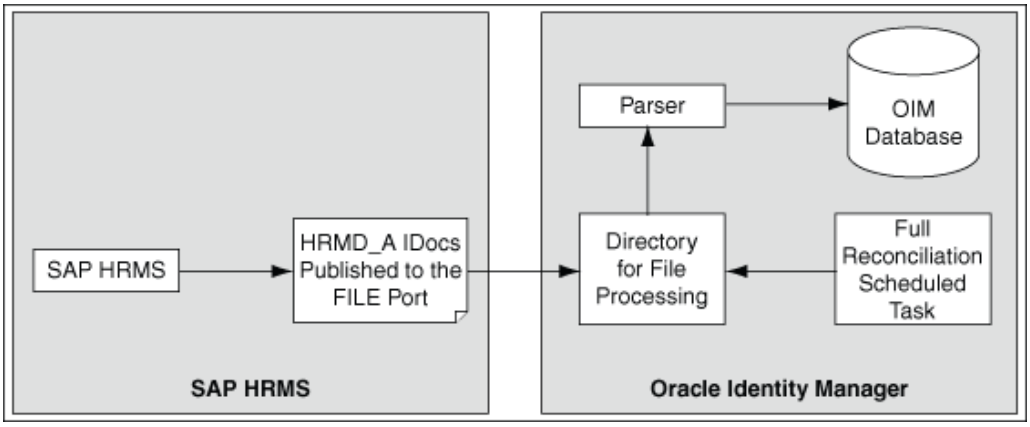
> **See Also:**
>
> Structure of a Sample IDoc

The method by which IDocs reach Oracle Identity Manager depends on the type of reconciliation that you configure:

Full Reconciliation

Figure 1-1 shows the flow of data during full reconciliation.

Figure 1-1 Data Flow During Full Reconciliation



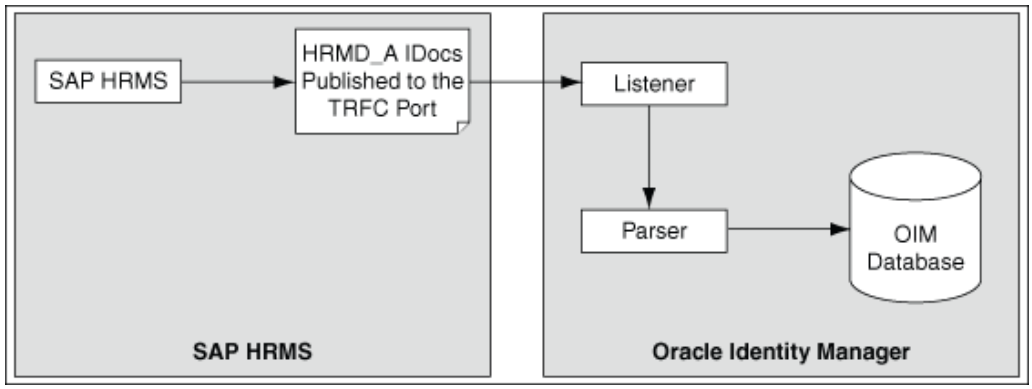
In full reconciliation, you run a transaction that generates IDocs for all existing target system users. These IDocs are captured in flat files and sent to a file port that you configure. You copy these flat files to a directory on the Oracle Identity Manager host computer and then run a scheduled task. A parser program called by the scheduled task converts the IDocs into reconciliation events.

> **Note:**
>
> After you deploy the connector, you first perform full reconciliation to create OIM Users for all existing target system users.

Incremental reconciliation

Figure 1-2 shows the flow of data during incremental reconciliation.

Figure 1-2 Data Flow During Incremental Reconciliation



In incremental reconciliation, a change doc is created whenever a user record is created or updated. An IDoc is created for each change doc generated by the system. Scheduled tasks that you configure on the target system send these IDocs to a transactional remote function call (tRFC) port.

A scheduled task that you configure on Oracle Identity Manager acts as a listener and accepts IDocs from the tRFC port. The listener then calls the parser, which converts the IDocs into reconciliation events.

> **Note:**
>
> You configure the listener scheduled task to run continuously on Oracle Identity Manager. Configuring the Listener on Oracle Identity Manager provides information about this scheduled task.

Whenever required, you can switch from incremental to full reconciliation and then switch back to incremental reconciliation.

1.5 Features of the Connector

The following are features of the connector:

- Dedicated Support for Trusted Source Reconciliation
- IDoc-Based Reconciliation
- Configurable Attribute Mapping
- Reconciliation of Effective-Dated Lifecycle Events
- Setting the Start Date and End Date Values Based on the Life Cycle Events of the Target System User Record
- Synchronization of Employee Type Data and Reconciliation by Employee Type
- Reconciliation of the Manager ID Attribute
- Reconciliation of Person Record Deletion
- Support for Both Unicode and Non-Unicode Modes

- Validation and Transformation of User Datas
- SAP ER Connector Support for IDoc in XML Format

1.5.1 Dedicated Support for Trusted Source Reconciliation

The connector provides all the features required for setting up SAP HRMS a trusted (authoritative) source of identity data for Oracle Identity Manager.

The connector cannot be used for setting up SAP HRMS as a target resource. In other words, the connector does not support provisioning operations and target resource reconciliation with SAP HRMS. This is because person records maintained in SAP HRMS are not accounts that users can use to log in to the system and perform business-related work.

1.5.2 IDoc-Based Reconciliation

The connector supports IDoc-based reconciliation. Both tRFC and file ports can be used as modes of communication between the target system and Oracle Identity Manager. The following are features of IDoc-based reconciliation:

- Standard BAPIs provided by the target system are used for reconciliation.
- Reconciliation is in real time. Changes made on the target system can be immediately sent to Oracle Identity Manager.
- You can specify the infotypes that must be fetched from the target system during reconciliation. You can also specify custom infotypes that have been added on the target system by extending IDoc types.
- The connector processes only person records. In the SAP context, this means that the connector processes only records of the P (person) object type. IDocs of all other object types, such as organization and position, are ignored even if they are sent to Oracle Identity Manager.

1.5.3 Configurable Attribute Mapping

You can specify the segments from which you want to reconcile changes.

In addition, you can customize attribute mappings between the target system and Oracle Identity Manager. During reconciliation, only changes to infotypes in segments that you specify are used to create IDocs. When an IDoc is processed by Oracle Identity Manager, attribute mappings are applied to filter out attributes that are used to create reconciliation events.

Extended IDoc types can be used for reconciliation. This means that you can add both standard and custom target system attributes can be added for reconciliation.

See sections Configuring Segment Filtering and Removing or Adding Attributes for Reconciliation for more information:

1.5.4 Reconciliation of Effective-Dated Lifecycle Events

The connector can distinguish between hire events and other events in the life cycle of a user record on the target system.

These events may be either current dated or future-dated (in other words, effective-dated). A current-dated event is one in which the date of the event is less than or equals the current date. A future-dated event is one in which the date the event takes effect is set in the future. For example, if the current date is 30-Jan-09 and if the date set for an event is 15-Feb-09, then the event is future dated. During reconciliation, the manner in which an event is processed depends on the type of the event:

- If both the hire event and changes to other infotypes are current dated, then the OIM User is created by using information from all infotypes.
- If the hire event is current dated and some other infotypes are future dated, then the OIM User is created by using only information from the current-dated infotype attributes. Future-dated infotype attributes are stored in reconciliation events to which the Event Deferred state is applied in the reconciliation manager.
- If the hire event is future dated, then depending on the value of the Create deferred event for future dated hire entry in the Lookup.SAP.HRMS.Configuration lookup definition, one of the following actions are performed:
  - If the Create deferred event for future dated hire entry is set to Yes, then no OIM User is created. However, in the reconciliation manager, a reconciliation event (containing the future-dated infotype attributes) is created and the Event Deferred state is applied.
  - If the Create deferred event for future dated hire entry is set to No, then an OIM User is created and the Start Provisioning date is set to the future date in the Action infotype in the target system record.

  > **See Also:**
  >
  > Structure of a Sample IDoc for the location of the Action infotype in an IDoc.

- If the future-dated event is not a hire event, then it is set to the Event Deferred state.

The Process Deferred Recon Events scheduled task is used to process reconciliation events that are in the Event Deferred state. For each event in the Event Deferred state, the scheduled task compares the event date with the system date. If the Start Provisioning date is less than or equals the system date, then the event is forwarded to the Reconciliation Manager in Oracle Identity Manager.

1.5.5 Setting the Start Date and End Date Values Based on the Life Cycle Events of the Target System User Record

The Start date and End date process form fields are optional on Oracle Identity Manager. However, in the target system, the attributes corresponding to the Start date and End date process form fields are mandatory. Depending on whether you want to populate values for the Start date and End date process form fields, you set values for the OIM start date field and OIM end date field entries in the Lookup.SAP.HRMS.Configuration lookup definition.

The values for the Start date and End date process form fields are populated depending on the events in the life cycle of a user record on the target system. The Lookup.SAP.HRMS.HireEvents, Lookup.SAP.HRMS.TerminateEvents, and Lookup.SAP.HRMS.RehireEvents lookup definitions are used to determine values

for the Start date and End date process form fields. See Predefined Lookup Definitions for more information about these lookup definitions.

If you set the values of the OIM start date field and OIM end date field entries in the Lookup.SAP.HRMS.Configuration lookup definition to None, then no values are populated in the Start date and End date process form fields.

If you set the values of the OIM start date field and OIM end date field entries in the Lookup.SAP.HRMS.Configuration lookup definition to Start date and End date respectively, then the following scenarios explain how these values are populated:

- For a particular target system user record, if IDoc contains information about both Hire or Re-hire event and Terminate events, then:
  The value for the Start date field is the start date of the corresponding Hire or Re-hire event, which is determined from the Lookup.SAP.HRMS.HireEvents or Lookup.SAP.HRMS.RehireEvents lookup definitions.

  The value for the End date field is the start date of the corresponding Terminate event, which is determined from the Lookup.SAP.HRMS.TerminateEvents lookup definition.
- For a particular target system user record, if IDoc contains events other than the Terminate event, then:
  The value of the Start date field is the start date of the corresponding Hire or Re-hire event, which is determined from the Lookup.SAP.HRMS.HireEvents or Lookup.SAP.HRMS.RehireEvents lookup definitions.

  The value of the End date field is the end date of the last event created for the user record.

1.5.6 Synchronization of Employee Type Data and Reconciliation by Employee Type

The Lookup.SAP.HRMS.EmployeeType lookup definition enables you to specify mappings between the following items:

- Employee Group and Employee Subgroup combinations on the target system
- Employee types defined in Oracle Identity Manager

You use the SAP HRMS EmployeeType Lookup Recon scheduled task to synchronize this lookup definition with changes made on the target system. See Lookup.SAP.HRMS.EmployeeType for more information.

In addition, you can use the Employee Type Query attribute of the SAP HRMS User Recon scheduled task to specify the employee types for which you want to fetch data for reconciliation. This additional filter is applied during the reconciliation process.

1.5.7 Reconciliation of the Manager ID Attribute

> **Note:**
>
> Configuring Reconciliation of Manager ID Attribute Values provides information about implementing this feature. The target system also provides the Supervisor attribute, which is a free-text field on the target system UI. If you want to bring values from this attribute into Oracle Identity Manager, first create a UDF for this attribute and then follow the instructions given in Adding Attribute Mapping.

Managers are not defined for individual users on the target system. Instead, managers are defined for organizations and users are members of these organizations. The Manager ID attribute is one of the predefined OIM User form attributes.

Summary of the Manager ID Reconciliation Process

The following is a summary of the steps involved in reconciling the manager ID value for a particular OIM User:

1. The organization ID of the OIM User is determined from the user's record on the target system and populated in the Org Unit attribute.
2. The personnel number of the manager for that organization is determined from the Lookup.SAP.HRMS.OrgManager lookup definition. This lookup definition holds information about the managers for each organization.
   If it is determined that the user is also the manager of the organization or if the position of the user's manager is currently vacant, then:
   a. The parent organization of the user's organization is determined from the Lookup.SAP.HRMS.OrgHierarchy lookup definition.
   b. The personnel number of the manager for the parent organization is determined from the Lookup.SAP.HRMS.OrgManager lookup definition.
3. The manager's personnel number determined in Step 2 is populated in the Manager ID attribute of the OIM User form.

> **Note:**
>
> If the manager of the organization is changed, then the change is not automatically propagated to individual OIM User records. This is because the connector only fetches changes to person records, and not organization records. Running the SAP HRMS Update Manager Scheduled Task describes how you can reconcile Manager ID values in this scenario.

The sequence of steps can be illustrated by the following example:

Suppose Richard is a user belonging to organization 50000147 on the target system. Drew is the manager of this organization. During reconciliation of Richard's user record:

1. The organization ID of Richard's organization is determined from his user record.

2. The personnel number of Richard's manager (Drew) is determined from Lookup.SAP.HRMS.OrgManager lookup definition.
3. Drew's personnel number is used to populate the Manager ID attribute of Richard's OIM User form.

During reconciliation of Drew's user record:

1. The organization ID of Drew's organization is determined from her user record.
2. From the Lookup.SAP.HRMS.OrgManager lookup definition, it is determined that Drew is the manager of the organization to which she belongs.
3. The parent organization of Drew's organization is determined from the Lookup.SAP.HRMS.OrgHierarchy lookup definition.
4. The personnel number of the manager for the parent organization is determined from the Lookup.SAP.HRMS.OrgManager lookup definition.
5. The personnel number of the manager is populated in the Manager ID attribute of Drew's OIM User form.

Detailed Steps of the Manager ID Reconciliation Process

To determine the manager ID of a particular target system user, the following approach is applied during reconciliation:

1. The organization ID of the OIM User is determined from the user's record on the target system and populated in the Org Unit attribute.
2. The personnel number of the manager for that organization is determined from the Lookup.SAP.HRMS.OrgManager lookup definition.
   If it is determined that the user is also the manager of the organization, then:
   a. The parent organization of the user's organization is determined from the Lookup.SAP.HRMS.OrgHierarchy lookup definition. The Code Key column of this lookup definition holds the ID of an organization and the Decode column holds the ID of the corresponding parent organization.
   Table 1-2 shows sample entries in this lookup definition.

Table 1-2 Sample Entries in the Lookup.SAP.HRMS.OrgHierarchy Lookup Definition

Code Key	Decode
00000001	00000001
00000100	00000001
00001001	00000100
50000147	00001001
50000148	00001001
50000149	00001001

There can be multiple organization hierarchies on the target system. The Code Key and Decode entries are the same for the topmost organization in a particular organization hierarchy. The first row in the preceding table is an entry for a topmost organization.

   b. The personnel number of the manager for the parent organization is determined from the Lookup.SAP.HRMS.OrgManager lookup definition. The Code Key column of this lookup definition holds the ID of an organization

and the Decode column holds the personnel number of the organization's manager.
Table 1-3 shows sample entries in this lookup definition.

Table 1-3 Sample Entries in the Lookup.SAP.HRMS.OrgManager Lookup Definition

Code Key	Decode
00000001	00001009
00000100	00001017
00001001	00001018
50000147	00001019
50000148	00001020
50000149	00001021

3. The personnel number of the manager is populated in the Manager ID attribute of the OIM User form.

1.5.8 Reconciliation of Person Record Deletion

The connector can process IDocs that bring data about deleted person records to Oracle Identity Manager. The details of the target system attribute that provides information about deleted person records are stored in the Delete Indicator entry of the Lookup.SAP.HRMS.Configuration lookup definition.

See Setting Up the Lookup.SAP.HRMS.Configuration Lookup Definition in Oracle Identity Manager for information about this lookup definition.

1.5.9 Support for Both Unicode and Non-Unicode Modes

An SAP application can be run in either Unicode or non-Unicode mode.

The connector supports both modes. You use the Unicode mode parameter of the IT resource to specify whether the target SAP application is running in Unicode or non-Unicode mode. Configuring the IT Resource provides more information about this parameter.

1.5.10 Validation and Transformation of User Datas

You can configure validation and transformation of user data that is brought into Oracle Identity Manager during reconciliation.

See the following sections for more information:

- Configuring Validation of Data During Reconciliation
- Configuring Transformation of Data During User Reconciliation

1.5.11 SAP ER Connector Support for IDoc in XML Format

The Connector supports processing of IDocS in xml format. This feature works similar to a flat file IDoc processing. XML IDoc (Standard IDoc/Extended IDoc/Custom IDoc)

is parsed and the values are retrieved using JCo parser. Once IDoc is parsed, then the post processing is performed similar to a flat file.

To accomplish this feature, you must enter the value "yes" in the configuration lookup for the entry "Is IDoc File Format in XML."

Xml IDoc files must be placed at a defined folder location in the schedule task which can be accessed by IDM. SAP ER Connector reads these files from this location and parses the contents of the files. The connector creates reconciliation events for each record in IDM.

1.6 Connector Objects Used During Reconciliation

This section discusses the following topics:

- User Fields for Reconciliation
- Reconciliation Rule
- Reconciliation Action Rules
- Predefined Lookup Definitions

1.6.1 User Fields for Reconciliation

Predefined attribute mappings for reconciliation between the target system and Oracle Identity Manager are stored in the Lookup.SAP.HRMS.AttributeMapping lookup definition. See Lookup.SAP.HRMS.AttributeMapping for more information.

1.6.2 Reconciliation Rule

The Personnel Number attribute of the target system can hold only numeric values. The User ID attribute of the OIM User form can hold alphanumeric values. If you use the target system as a trusted source, then all User ID values would have to be numeric values. This restriction might not be compatible with other target systems of Oracle Identity Manager in your operating environment.

To work around this restriction, the Personnel Number attribute of the target system is mapped to the following attributes on the OIM User form:.

- User ID attribute
- Personnel Number UDF

In addition, a two-component reconciliation rule is applied to reconciliation events:

Rule name: SAP HRMS Recon Rule

Rule element: (Personnel Number Equals Personnel Number) OR (User Login Equals User ID)

In the first component:

- The Personnel Number attribute to the left of "Equals" represents the Personnel Number UDF created on the OIM User form.
- The Personnel Number attribute to the right of "Equals" represents the Personnel Number attribute of the target system.

In the second component:

- The User Login attribute represents the User ID attribute on the OIM User form.
- The User ID attribute represents the Personnel Number attribute of the target system.

When an OIM User is created during a reconciliation run, the Personnel Number value from the target system is used to populate both the User ID attribute and the Personnel Number UDF on the OIM User form. You are allowed to change the User ID value according to your requirements, but you cannot change the Personnel Number value on the OIM User form. The advantage of this feature is illustrated by the following example:

Suppose you have configured SAP HRMS as a trusted source and Microsoft Active Directory as a target resource. During reconciliation with SAP HRMS, the Personnel Number and User ID attributes are populated with Personnel Number values. For OIM User John Doe, you can manually change the User ID value to the samAccountName value of John's account on Microsoft Active Directory. During subsequent reconciliation runs with Microsoft Active Directory, the User ID attribute of the OIM User is used for matching purposes.

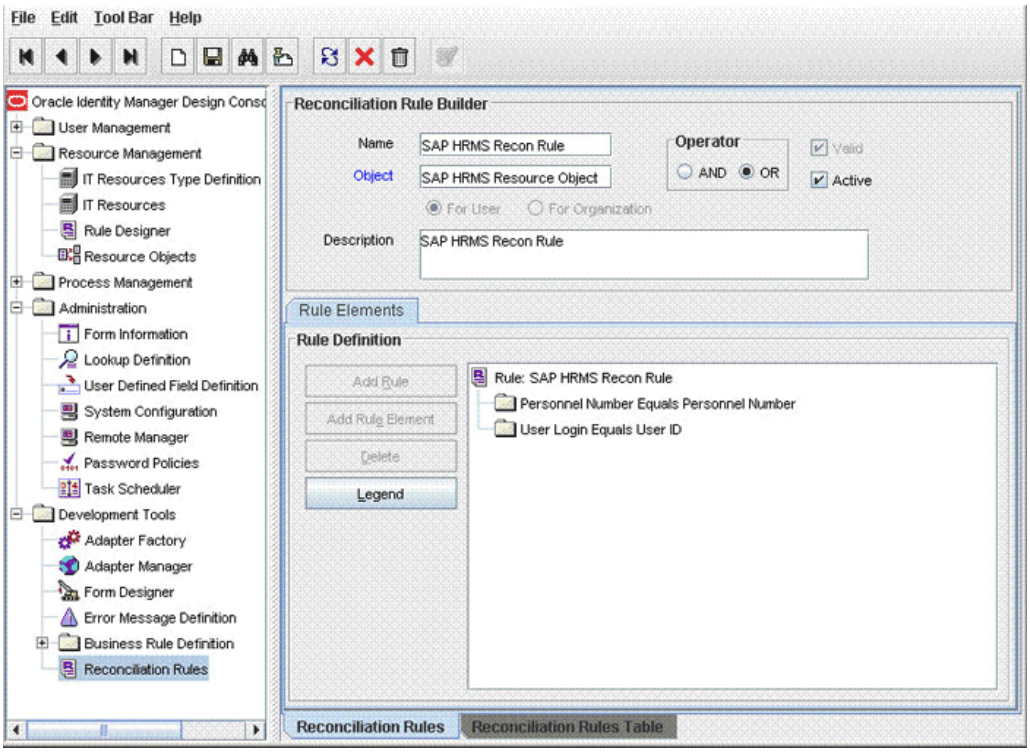
If you create an OIM User and then perform reconciliation with SAP HRMS, then the second component of the rule is used to determine a match between the OIM User and an existing account for the same individual on the target system.

After you deploy the connector, you can view the reconciliation rule for trusted source reconciliation as follows:

> **Note:**
>
> Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **SAP HRMS Recon Rule**. The following screenshot shows the reconciliation rule:

Figure 1-3 Reconciliation Rules



1.6.3 Reconciliation Action Rules

Application of the matching rule on reconciliation events would result in one of multiple outcomes. The action rules for reconciliation define actions to be taken for these outcomes. Table 1-4 lists the action rules for reconciliation.

Table 1-4 Action Rules for Trusted Source Reconciliation

Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link

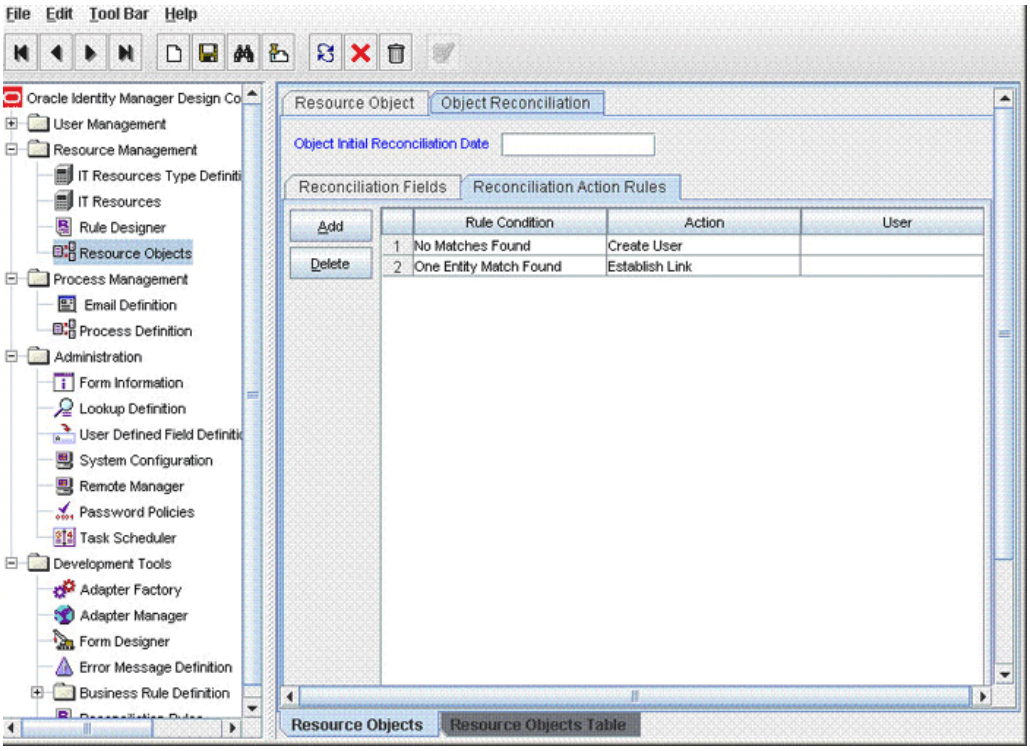
> **Note:**
>
> No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See Setting a Reconciliation Action Rule in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about modifying or creating a reconciliation action rule.

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.

2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **SAP HRMS Resource Object** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. The following screenshot shows the reconciliation action rules:

Figure 1-4 Reconciliation Action Rules



1.6.4 Predefined Lookup Definitions

The following are predefined lookup definitions:

Lookup.SAP.HRMS.ITResourceMapping

The IT resource for this connector contains the connection properties required to establish a connection with the target system. The entries listed in the Lookup.SAP.HRMS.ITResourceMapping lookup definition are mappings between:

- Code Key: Some of the connection properties defined for the ServerDataProvider and DestinationDataProvider interfaces of SAP JCo 3.0
- Decode: Parameters of the IT resource

The SAP JCo API recognizes only values assigned to the connection properties. The mappings in the lookup definition are used to forward values of the IT resource parameters to the appropriate SAP JCo connection properties.

> **See Also:**
>
> The Javadocs shipped with SAP JCo 3.0 for detailed information about these connection properties. See Specifying Values for the Connection Properties (IT Resource Configuration) for information about modifying this lookup definition.

Lookup.SAP.HRMS.AttributeMapping

The Lookup.SAP.HRMS.AttributeMapping lookup definition holds default attribute mappings between the target system and Oracle Identity Manager. Table 1-5 lists the default attribute mappings stored in this lookup definition. The following is the format of values stored in this table:

- Code Key: Name of the OIM User field
- Decode: Combination of the following elements:

```
SEGMENT_NAME;SUB_TYPE;SAP_ATTRIBUTE_NAME;START_POSITION;END_POSITION;[Text|Date]
```

Table 1-5 Entries in the Lookup.SAP.HRMS.AttributeMapping Lookup Definition

Code Key	Decode	Comments
First Name	E2P0002001;NONE;VORNA_40;790;829;Text	Default OIM User attribute
Middle Name	E2P0002001;NONE;NACHN_40;670;709;Text	Default OIM User attribute
Last Name	E2P0002001;NONE;NACHN;148;172;Text	Default OIM User attribute
Personnel Number	E2PLOGI001;NONE;OBJID;68;75;Text	UDF
Org Unit	E2P0001001;NONE;ORGEH;189;196;Text	UDF
City	E2P0006003;NONE;ORT01;197;221;Text	UDF
Street	E2P0006003;NONE;STRAS;167;196;Text	UDF
Country	E2P0006003;NONE;LAND1;257;258;Text	UDF
District	E2P0006003;NONE;ORT02;222;246;Text	UDF
Postal Code	E2P0006003;NONE;PSTLZ;247;256;Text	UDF
Telephone Number	E2P0006003;NONE;TELNR;259;272;Text	UDF
Department	E2P0030001;NONE;ORGEH;142;149;Text	UDF
Email Id	E2P0105002;NONE;USRID_LONG;172;412;Text	Default OIM User attribute
Linked User Id	E2P0105002;0001;USRID;142;171;Text	UDF
Cost Center	E2P0001001;NONE;KOSTL;179;188;Text	UDF

Table 1-5 (Cont.) Entries in the Lookup.SAP.HRMS.AttributeMapping Lookup Definition

Code Key	Decode	Comments
Idoc Number	EDI_DC40;NONE;DOCNUM;14;29;Text	Tracking the Idoc Number
Position	E2P0001001;NONE;PLANS;197;204;Text	UDF

Lookup.SAP.HRMS.HireEvents, Lookup.SAP.HRMS.TerminateEvents, and Lookup.SAP.HRMS.RehireEvents

You use the Lookup.SAP.HRMS.HireEvents, Lookup.SAP.HRMS.TerminateEvents, and Lookup.SAP.HRMS.RehireEvents lookup definitions to hold the target system event IDs for Hire, Terminate, and Rehire events, respectively. When you deploy the connector, these lookup definitions are created without any entries. You add event IDs for Hire, Terminate, and Re-hire events as entries in these lookup definitions by performing the procedure described in the Configuring Reconciliation of Effective-Dated Target System Events.

> **Note:**
>
> On Oracle Identity Manager, the status of a terminated employee is set to Disabled and the status of a deleted employee (record) is set to Deleted.

Lookup.SAP.HRMS.EmployeeType

On the target system, there is no direct equivalent for the Employee Type attribute of the OIM User. As a workaround, a combination of the Employee Group and Employee Subgroup attributes can be used for each employee type defined in Oracle Identity Manager.

You run the SAP HRMS EmployeeType Lookup Recon scheduled task to populate the Lookup.SAP.HRMS.EmployeeType lookup definition. After the scheduled task is run, the Code Key column of this lookup definition is populated with a concatenated combination of Employee Group and Employee Subgroup values from the target system. The tilde (~) character is used as the delimiter. The following are sample Code Key entries:

1~DZ

1~Q5

1~Q4

1~Q6

2~M6

OIM Employee Type is one of the Code Key values in the Lookup.SAP.HRMS.Configuration lookup definition. The value of this entry is "End User." When the scheduled task is run, the Decode column of the Lookup.SAP.HRMS.EmployeeType lookup definition is populated with "End User." After the scheduled task has run, you manually modify the employee type for each

employee group and subgroup combination to individual employee types of your choice.

See Configuring the Scheduled Job for Lookup Field Synchronization for instructions on configuring the SAP HRMS EmployeeType Lookup Recon scheduled task.

Lookup.SAP.HRMS.Configuration

The Lookup.SAP.HRMS.Configuration lookup definition is used to capture information about the following items:

- Message type and IDoc type used for communication between the target system and Oracle Identity Manager
- Connector components used during reconciliation

See Setting Up the Lookup.SAP.HRMS.Configuration Lookup Definition in Oracle Identity Manager for a listing of the entries in this lookup definition.

Lookup.SAP.HRMS.Constants

The Lookup.SAP.HRMS.Constants lookup definition is used to store constants that are used by the connector. You must not modify the entries in this lookup definition.

Lookup.SAP.HRMS.CustomQueryMapping

You can configure limited reconciliation to specify the subset of target system records that must be fetched into Oracle Identity Manager. This subset is defined on the basis of attribute values that you specify in a query condition, which is then applied during reconciliation.

The Lookup.SAP.HRMS.CustomQueryMapping lookup definition maps resource object fields with OIM User form fields. It is used during application of the query condition that you create. See Limited Reconciliation for more information.

Lookup.SAP.HRMS.ReconValidation

This lookup definition is used to configure validation of user attribute values fetched from the target system during reconciliation.

You have to manually create entries in this lookup definition.

See Configuring Validation of Data During Reconciliation for more information.

Lookup.SAP.HRMS.ReconTransformation

This lookup definition is used to configure transformation of user attribute values that are fetched from the target system during reconciliation.

You have to manually create entries in this lookup definition. See Configuring Transformation of Data During User Reconciliation for more information.

2
Deploying the Connector

Deploying the connector involves the following steps:

- Preinstallation
- Installation
- Postinstallation
- Upgrading the Connector

> **Note:**
>
> Some of the procedures described in this chapter must be performed on the target system. To perform these procedures, you must use an SAP administrator account to which the SAP_ALL and SAP_NEW profiles have been assigned.

2.1 Preinstallation

Preinstallation information is divided across the following sections:

- Preinstallation on Oracle Identity Manager
- Preinstallation on the Target System

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- Files and Directories on the Installation Media
- Creating a Backup of the Existing Common.jar File

2.1.1.1 Files and Directories on the Installation Media

Table 2-1 lists the files and directories that are bundled in the deployment package on the installation media.

Table 2-1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
configuration/SAPHRMS-CI.xml	This XML file contains configuration information that is used during connector installation.

Table 2-1 (Cont.) Files and Directories on the Installation Media

File in the Installation Media Directory	Description
lib/Common.jar	This JAR file contains the class files that are common to all connectors. During connector deployment, this file is copied to the Oracle Identity Manager database of Oracle Identity Manager release 11.1.*x*.
lib/SAPCommon.jar	This JAR file contains the class files that are common to all SAP connectors. During connector deployment, this file is copied to the Oracle Identity Manager database of Oracle Identity Manager release 11.1.*x*.
lib/SAPER.jar	This JAR file contains the class files that are specific to the SAP Employee Reconciliation connector. During connector deployment, this file is copied to the Oracle Identity Manager database of Oracle Identity Manager release 11.1.*x*.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, this file is copied to the Oracle Identity Manager database of Oracle Identity Manager release 11.1.*x*. **Note**: A **resource bundle** is a file containing localized versions of the text strings that include GUI element labels and messages.
xml/SAPHRMS-ConnectorConfig.xml	This XML file contains definitions for the connector components. These components include the following: • Resource objects • IT resource types • Process form • Process definition • Lookup definitions • Scheduled tasks

> **Note:**
>
> If you are using Oracle Identity Manager 12cPS4 (12.2.1.4.0) or later with the SAP Employee Reconciliation 9.1.2.x connector, you must create the **ServiceAccount.API.EncryptedParamsValue** system property. This property is not available out of the box and must be created from the **Configuration Property** option in Oracle Identity System Administration console. This system property is used to control the functionality of the `tcITResourceInstanceOperationsBean.getITResourceInstanceParameters(long plITResourceInstanceKey)` API.
>
> By default, this API masks the value of encrypted fields making your deployment more secure.
>
> Oracle recommends creating this property only if a legacy connector or an old custom code requires the legacy behavior of the above API.
>
> When the value is set to **False**, the encrypted parameter values are masked. When the value is set to **True**, the encrypted parameter values are returned by the above API.

2.1.1.2 Creating a Backup of the Existing Common.jar File

The Common.jar file is in the deployment package of each release 9.1.x connector. With each new release, code corresponding to that particular release is added to the existing code in this file. For example, the Common.jar file shipped with Connector Y on 12-July contains:

- Code specific to Connector Y
- Code included in the Common.jar files shipped with all other release 9.1.*x* connectors that were released before 12-July.

If you have already installed a release 9.1.x connector that was released after current release of the SAP Employee Reconciliation connector, back up the existing Common.jar file, install the SAP Employee Reconciliation connector, and then restore the Common.jar file. The steps to perform this procedure are as follows:

> **Caution:**
>
> If you do not perform this procedure, then your release 9.1.*x* connectors might not work.

1. Determine the release date of your existing release 9.1.*x* connector as follows:

   If you are using Oracle Identity Manager release 11.1.*x* or later, then run the Oracle Identity Manager Download JARs utility to download the Common.jar file to the Oracle Identity Manager database.

   a. Extract the contents of the following file in a temporary directory:
   On the installation media for the connector, extract the contents of the lib directory/lib/Common.jar

> **Note:**
>
> On Oracle Identity Manager release 11.1.*x*, use either DownloadJars utility to download the common.jar file from the database, and then extract the contents of this file into a temporary directory. See Download JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed instructions.

b. Open the Manifest.mf file in a text editor.

c. Note down the Build Date and Build Version values.

2. Determine the release date of the SAP Employee Reconciliation release 9.1.1 connector as follows:

   a. On the installation media for the connector, extract the contents of the lib/Common.jar and then open the Manifest.mf file in a text editor.

   b. Note down the Build Date and Build Version values.

3. If the Build Date and Build Version values for the SAP Employee Reconciliation connector are less than the Build Date and Build Version values for the connector that is already installed, then for Oracle Identity Manager release 11.1.*x* or later, run the Oracle Identity Manager Upload JARs utility to post the Common.jar file to the Oracle Identity Manager database. This utility is copied to the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use this utility, verify that the `WL_HOME` environment variable is set to the directory in which Oracle WebLogic Server is installed.

   For Microsoft Windows:

   OIM_HOME/server/bin/UploadJars.bat

   For UNIX:

   OIM_HOME/server/bin/UploadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

   > **See Also:**
   >
   > See Download JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about the Upload JARs utility.

2.1.2 Preinstallation on the Target System

Preinstallation on the target system involves performing the following procedures:

- Creating a Target System User Account for Connector Operations
- Downloading and Installing the SAP JCo

2.1.2.1 Creating a Target System User Account for Connector Operations

The connector uses a target system account to connect to the target system during reconciliation. This target system account must be a CPIC user to whom you assign a customized role with the S_IDOC_ALL profile, S_RFC authorization object, and PLOG authorization object.

Create user of type CPIC with the following privileges:

1. Assign `S_IDOC_ALL` profile.
2. Assign authorization object S_RFC with values:
   - ACTVT: `16`
   - RFC_NAME: *
   - RFC_TYPE: `FUGR, FUNC`
3. Assign authorization object PLOG with values:
   - INFOTY: *
   - ISTAT: *
   - OTYPE: `$$,O,P,S`
   - PLVAR: `01, RS`
   - PPFCOD: *
   - SUBTYP: *
4. Assign authorization object P_ORGIN with values:
   - AUTHC: `R`
   - INFTY: `0000-0003, 0006, 0105`
   - PERSA: *
   - PERSG: *
   - PERSK: *
   - SUBTY: *
   - VDSK1: *
5. Assign authorization object P_ORGINCON with values:
   - AUTHC: `R`
   - INFTY: `0000-0003, 0006, 0105`
   - PERSA: *
   - PERSG: *

- PERSK: *
- SUBTY: *
- VDSK1: *
- PROFL: *

6. Assign authorization object P_PERNR with values:
   - AUTHC: `R`
   - PSIGN: `E, I`
   - INFTY: `0000-0003, 0006, 0105`
   - SUBTY: *
7. Assign authorization object B_ALE_RECV with values:
   - EDI_MES : `HRMD_A`

> **Note:**
>
> You must configure the PLOG authorization object so that the values assigned to this object match the ones shown in Step 2 through 6. Only the Plan Version (PLVAR) object can be set according to your requirements.

2.1.2.2 Downloading and Installing the SAP JCo

> **Note:**
>
> To download files from the SAP Web site, you must have access to the SAP service marketplace with Software Download authorization.
>
> In an Oracle Identity Manager cluster, copy the JAR files and the contents of the connectorResources directory to the corresponding directories on each node of the cluster.

To download and copy the external code files to the required locations:

1. Download and extract the contents of the SAP Java connector file from the SAP website
2. Copy the sapjco3.jar and sapidoc3.jar files into the OIM_HOME/server/ThirdParty directory.

   If sapjco3.jar and sapidoc3.jar is not detected, copy the sapjco3.jar and sapidoc3.jar file into the OIM_HOME/server/ThirdParty directory. Then, add its path to the DOMAIN_HOME\bin\startWebLogic file as follows:

   - On Microsoft Windows:
     In a text editor, open the DOMAIN_HOME\bin\startWebLogic.cmd file and add the following path:

CLASSPATH=MIDDLEWARE_HOME_PATH\Oracle_IDM1\server\ThirdPartysapjco3.jar:MIDDLEWARE_HOME_PATH\Oracle_IDM1\server\ThirdParty\sapidoc3.jar;%SAVE_CLASSPATH%

Save and close the file. Restart the server for the changes in the CLASSPATH variable to take effect.

- On Linux:
  In a text editor, open the DOMAIN_HOME/bin/startWebLogic.sh file and add the following path:

  CLASSPATH=MIDDLEWARE_HOME_PATH/Oracle_IDM1/server/ThirdParty/sapjco3.jar:/MIDDLEWARE_HOME_PATH/Oracle_IDM1/server/ThirdParty/sapidoc3.jar "${SAVE_CLASSPATH}"

  For example,

  CLASSPATH=/home/shareuser/Middleware/Oracle_IDM1/server/ThirdParty/sapjco3.jar:/home/shareuser/Middleware/Oracle_IDM1/server/ThirdParty/sapidoc3.jar"${SAVE_CLASSPATH}"

  Save and close the file. Restart the server for the changes in the CLASSPATHvariable to take effect.

> **Note:**
>
> Ensure that you are using version 3.0.2 or later of the sapjco3.jar and sapidoc3.jar files.
> In an Oracle Identity Manager cluster, copy these JAR files to each node of the cluster.

3. Copy the RFC files into the required directory on the Oracle Identity Manager host computer, and then modify the appropriate environment variable so that it includes the path to this directory:
   - On Microsoft Windows:
     Copy the sapjco3.dll into the WINDOWS_HOME\system32 directory. Alternatively, you can copy these files into any directory and then add the path to the directory in the java.library.path environment variable.
   - On Solaris and Linux:
     Copy the sapjco3.so file into the /usr/local/jco directory, and then add the path to this directory in the LD_LIBRARY_PATH environment variable.
4. On a Microsoft Windows platform, ensure that the msvcr80.dll and msvcp80.dll files are in the c:\WINDOWS\system32 directory. If required, both files can be downloaded from various sources on the Internet.
5. If you are using IBM WebSphere Application Server, perform the following steps:
   a. Copy the following files to WEBSPHERE_HOME/AppServer/lib:
      - libsapjco3.so
      - sapidoc3.jar
      - sapjco3.jar

      For example, copy the preceeding files to /home/shareuser/R2PS1ST1WAS/IBM/WebSphere/AppServer/lib

b. Update the *PROFILE_HOME*/bin/setupCmdLine.sh file as shown in the following example:

```
WAS_CLASSPATH="$WAS_HOME"/properties:"$WAS_HOME"/lib/
startup.jar:"$WAS_HOME"


/lib/bootstrap.jar:"$WAS_HOME"/lib/lmproxy.jar:"$WAS_HOME"/lib/
urlprotocols.jar:"$WAS_HOME"


/lib/sapjco3.jar:"$WAS_HOME"/lib/sapidoc3.jar:"$JAVA_HOME"/lib/
tools.jar
```

6. Restart the server for the changes in the environment variable to take effect.

> **Note:**
>
> You can either restart the server now or after the connector is installed.

7. To check if SAP JCo is correctly installed, in a command window, run one of the following commands:

```
java –jar JCO_DIRECTORY/sapjco3.jar
java –classpath JCO_DIRECTORY/sapjco3.jar com.sap.conn.jco.rt.About
```

2.2 Installation

> **Note:**
>
> In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.

Installing the connector involves running the connector installer, see Running the Connector Installer.

2.2.1 Running the Connector Installer

To run the Connector Installer for Oracle Identity Manager 11.1.*x*:

1. Copy the contents of the connector installation media into the following directory:

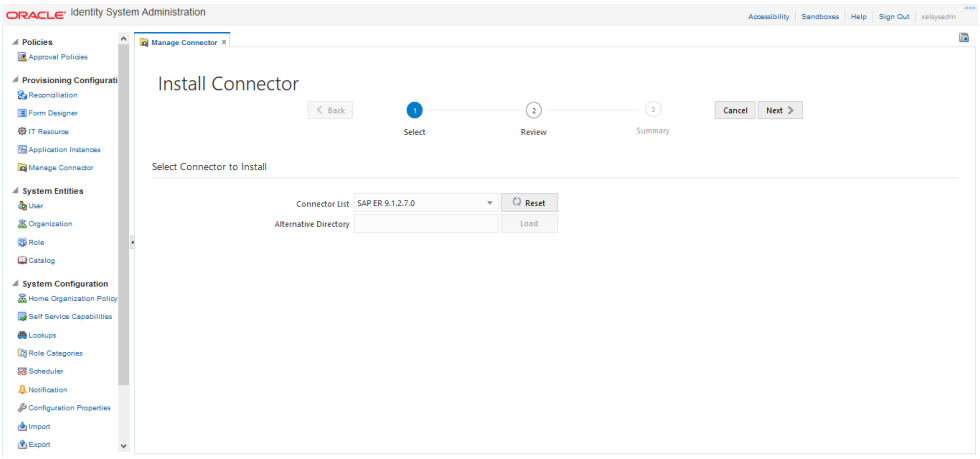
   OIM_HOME/server/ConnectorDefaultDirectory

> **Note:**
>
> In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster.

2. Perform the following steps:

   a. Log in to Oracle Identity System Administration by using the user account described in Creating the User Account for Installing Connectors of *Oracle Fusion Middleware Administering Oracle Identity Manager*.

   b. In the left pane, under System Management, click **Manage Connector**.



3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - For Oracle Identity Manager release 11.1.1:
     On the Welcome to Identity Manager Advanced Administration page, under the System Management section, click **Install Connector**.
   - For Oracle Identity Manager release 11.1.2 or later:
     In the Manage Connector page, click **Install**.

4. From the Connector List list, select **SAP ER *RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   For Oracle Identity Manager release 11.1.*x*:

   OIM_HOME/server/ConnectorDefaultDirectory

   If you have copied the installation files into a different directory, then:

   a. In the **Alternative Directory** field, enter the full path and name of that directory.

   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

   c. From the Connector List list, select **SAP ER *RELEASE_NUMBER***.

5. Click **Load**.

6. To start the installation process, click **Continue**.

   The following tasks are performed in sequence:

   a. Configuration of connector libraries

   b. Import of the connector XML files (by using the Deployment Manager)

   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are

displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

- Retry the installation by clicking **Retry**.
- Cancel the installation and begin again from Step 3.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed.

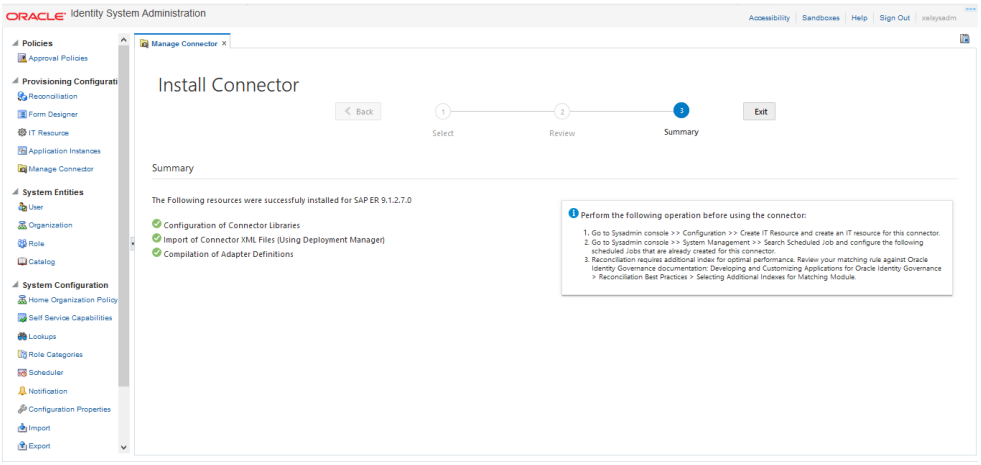
   In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed

> **Note:**
>
> At this stage, run the PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. Refer to Clearing Content Related to Connector Resource Bundles from the Server Cache for information about running the PurgeCache utility. There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector
   Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled tasks that are created when you installed the connector
   Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.



8. Restart Oracle Identity Manager.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 2-1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a cluster, copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on

each node of the cluster. Then, restart each node. See Files and Directories on the Installation Media for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

Restoring the Common.jar File

If required, restore the Common.jar file that you had backed up by following the procedure described in Creating a Backup of the Existing Common.jar File

2.3 Postinstallation

Postinstallation steps are divided across the following sections:

- Setting Up the Lookup.SAP.HRMS.Configuration Lookup Definition in Oracle Identity Manager
- Verifying Segment Details in Lookup Definitions
- Configuring Reconciliation of Manager ID Attribute Values
- Configuring the Target System for Generation of IDocs
- Changing to the Required Input Locale on Oracle Identity Manager
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Copying Resource Bundle Entries for UDFs
- Managing Logging
- Configuring Reconciliation of Effective-Dated Target System Events
- Recovering from Failed Communication Between the Target System and Oracle Identity Manager
- Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System
- Specifying Values for the Connection Properties (IT Resource Configuration)
- Creating an Authorization Policy
- Displaying UDFs in Oracle Identity Manager 11.1.2 or Later

2.3.1 Setting Up the Lookup.SAP.HRMS.Configuration Lookup Definition in Oracle Identity Manager

The Lookup.SAP.HRMS.Configuration lookup definition is used to capture information about the following items:

- Message type and IDoc type used for communication between the target system and Oracle Identity Manager
- Connector components used during reconciliation

Table 2-2 lists the entries in this lookup definition. The procedure to set or modify a Decode value is given after this table.

Table 2-2 Entries in the Lookup.SAP.HRMS.Configuration Lookup Definition

Code Key	Description	Decode
Message Type	Message type to be used for person record **Note**: You must not change the Decode value.	HRMD_A
Class Name	Name of the parser class **Note**: If you develop your own parser, then you can replace the default value of the Class Name entry with the name of your custom parser class.	oracle.iam.connectors.sap.common.parser.HRMDAParser
IDoc Type	IDoc type that you want to use You can specify either a predefined IDoc type or the name of a custom IDoc type.	HRMD_A05
IDoc Type Extension	If you have extended a predefined IDoc type, then enter the name of the IDoc type extension.	NONE
Sub Type Field	Stores the sub-type information You can specify a maximum length of 4 characters.	000076,000079
Begin Date Field	Stores the start date information You can specify a maximum length of 8 characters.	000091,000098

Note:

The entries listed in the remaining rows of this table must be changed only if you use a custom IDoc type. The default Decode values are correct for all predefined HRMD_A* IDoc types.

Code Key	Description	Decode
Root Segment	Root segment in IDoc, which will be used to identify new employees **Note**: You must not change the Decode value.	E2PLOGI001
Segment Name Length	Number of characters in the file that denotes the segment name	30
Object Type	Segment details of object type The Decode value is used to filter person records.	E2PLOGI001;OTYPE;66;67;P

Code Key	Description	Decode
User ID	Object ID that indicates the personnel number in a person record	E2PLOGI001;OBJID;68;75
Delete Indicator	Segment details of the indicator that identifies whether or not the employee is deleted	E2PLOGI001;OPERA;77;77;D
Event Begin Date	Segment details for the begin date of events (hire, terminate, and other events)	E2P0000001;BEGDA;91;98
Event End Date	Segment details for the end date of events (hire, terminate, and other events)	E2P0000001;ENDDA;83;90
Actions Event	Segment to indicate actions	E2P0000001
Event	Segment details for event	E2P0000001;MASSN;138;139
Group	Segment details for employee group	E2P0001001;PERSG;146;146
Sub Group	Segment details for employee subgroup	E2P0001001;PERSK;147;148
Group Segment	Infotype containing Employee Group and Employee Subgroup attributes	E2P0001001

Information about connector components

Code Key	Description	Decode
Employee Type Lookup	Name of the lookup definition that is used to map combinations of Employee Group and Employee Subgroup of the target system with the employee type in Oracle Identity Manager	Lookup.SAP.HRMS.EmployeeType
Hire Events Lookup	Name of the lookup definition that is used to store the list of all Hire events For example, name of the lookup definition that stores event IDs corresponding to employees joining the company for the first time.	Lookup.SAP.HRMS.HireEvents
Terminate Events Lookup	Name of the lookup definition that is used to store the list of all Terminate events For example, name of the lookup definition that stores events IDs corresponding to employees on long leave or terminated employees.	Lookup.SAP.HRMS.TerminateEvents

Code Key	Description	Decode
Rehire Events Lookup	Name of the lookup definition that is used to store the list of all Rehire events For example, name of the lookup definition that stores events IDs corresponding to employees who re-join the company.	Lookup.SAP.HRMS.RehireEvents
Transform Lookup For Recon	Name of the lookup definition that is used to configure transformation of user attribute values fetched from the target system during reconciliation	Lookup.SAP.HRMS.ReconTransformation
Validation Lookup For Recon	Name of the lookup definition that is used to configure validation of user attribute values fetched from the target system during reconciliation	Lookup.SAP.HRMS.ReconValidation
Organization	Default organization in Oracle Identity Manager	Xellerate Users
Employee Type	Default employee type in Oracle Identity Manager **Note**: The Decode value is used as the default user type in the Lookup.SAP.HRMS.EmployeeType lookup definition.	Full-time
User Type	Enter the role that must be set for OIM Users created through reconciliation. You must select one of the following values: • End-User • End-User Administrator Default value: `End-User`	End-User
IT Resource Mapping	Name of the lookup definition that holds mappings between the connection properties accepted by the SAP JCo API and the names of IT resource parameters	Lookup.SAP.HRMS.ITResourceMapping

Miscellaneous Variables

Code Key	Description	Decode
Batch Size	Enter the number of lines that you want the parser to process at a time from the flat file containing IDocs. This flat file is generated when you perform the procedure described in the Performing Full Reconciliation.	5

Code Key	Description	Decode
Remove Leading Zero from Personnel Number	Enter yes if you want leading zeros to be removed from personnel numbers fetched from the target system. Enter no if you do not want leading zeros to be removed.	no
Reconcile First Time Disabled Users	Enter yes to specify that you want to reconcile records that are currently in the Disabled state and that have not been reconciled earlier. Otherwise, enter no.	yes
Constants Lookup	Name of the lookup definition that holds constants	Lookup.SAP.HRMS.Constants
Manager Lookup Name	Name of the lookup definition in which manager IDs of managers of the various target system organizations must be populated	Lookup.SAP.HRMS.OrgManager
Create deferred event for future dated hire	Enter Yes if you want the connector to create a reconciliation event (containing the future-dated infotype attributes) and apply the Event Deferred state in the reconciliation manager. Note that the OIM User will be created only when the future date matches the current date. Enter No if you want the connector to create an OIM User and set the Start Provisioning date to the future date in the Action infotype in the target system record. Note that this OIM User remains in the Disabled until start date status until the current date matches the future-dated hire event date.	No
Create deferred event for terminate event	Enter Yes if you want the connector to create for the terminate event a separate recon event to which the Event Deferred state is applied in the reconciliation manager. Otherwise, enter No. **Note**: If you set the value of this entry to Yes, then the OIM start date field and OIM end date field entries (which are described later in this table) must contain the values Start date and End date, respectively.	No

Code Key	Description	Decode
OIM start date field	Enter `Start Date` if you want to reconcile the start date value from the target system into the Start date process form field in Oracle Identity Manager. Otherwise, enter `None`.	Start Date
OIM end date field	Enter `End Date` if you want to reconcile the end date value from the target system into the End date process form field in Oracle Identity Manager. Otherwise, enter `None`	End date
Use Validation For Recon	Enter `Yes` if you want to configure validation of user attributes that are brought into Oracle Identity Manager during reconciliation. Otherwise, enter `No`. See Configuring Validation of Data During Reconciliation for more information about this feature.	No
Use Transformation For Recon	Enter `Yes` if you want to configure transformation of user attributes that are brought into Oracle Identity Manager during reconciliation. Otherwise, enter `No`. See Configuring Transformation of Data During User Reconciliation for more information about this feature.	No
Organization Hierarchy Lookup Name	Name of the lookup definition containing details of organization hierarchies on the target system	Lookup.SAP.HRMS.OrgHierarchy
Get Manager ID During Recon	Enter `Yes` if you want to reconcile the Manager ID attribute values along with other user records. Otherwise, enter `No`.	No
Is Future Dated Event Handling Enabled	Enter `Yes` if you want the connector to handle future dated events as current dated events. Otherwise, enter `No`.	Yes
Is IDOC File Format in XML	Enter `Yes` if you want to parse the XML format IDOC. Otherwise, enter `No`.	No

Code Key	Description	Decode
Recon Rule Attribute Lookup	This entry will be used only to customize the reconciliation Rule. We must add an entry in the Lookup.SAP.HRMS.ReconRuleAttrMap. Field_Label as code key and UserForm_Field_Name in the decode. Example: `Code key: Employee ID` Decode: `USR_UDF_EMPLOYEEID` **Note**: Any updates done to Reconciliation Rules requires the 'Create Reconciliation Profile' option in Resource Object to be run once for the rule to take effect.	Lookup.SAP.HRMS.ReconRuleAttrMap

Depending on the OIM version, do the following to set or modify a Decode value in the lookup definition:

For Oracle Identity Manager prior to 11.1.2.1.0:

1. On the Design Console, expand **Administration**, and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.SAP.HRMS.Configuration** lookup definition.
3. In the **Decode** column for the Code Key, enter a value.
4. Click the Save icon.

For Oracle Identity Manager 11.1.2.1.0 or later:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Configuration, click **Lookups**.
3. Search for and open the **Lookup.SAP.HRMS.Configuration** lookup definition.
4. Click **Edit Lookup Type**.
5. In the Meaning column for the Code Key, enter a value.
6. Click the Save icon.

2.3.2 Verifying Segment Details in Lookup Definitions

The Lookup.SAP.HRMS.Configuration and Lookup.SAP.HRMS.AttributeMapping lookup definitions hold segment details of target system attributes. Segment details are in the following format:

```
E2P<INFO_TYPE><SEGMENT_VERSION>
```

For example, in the E2P0000001 segment, `0000` is the infotype and `001` is the version of the segment.

> **See Also:**
>
> Structure of a Sample IDoc

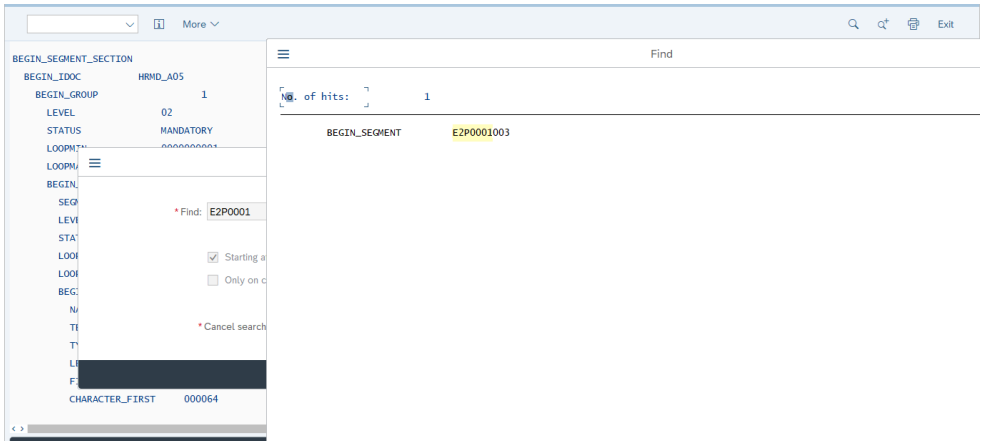
The segment version is different for different versions of the target system. For the HRMD_A05 IDoc type, E2P0001001 is the segment name in SAP R/3 4.7 and E2P0001002 is the segment name in ECC 6.0.

You must verify and, if required, correct segment details in the Lookup.SAP.HRMS.Configuration and Lookup.SAP.HRMS.AttributeMapping lookup definitions.

To determine and if required change the segment version:

1. Run transaction WE60 on the target system.
2. In the Find dialog box, enter `E2P0001` and then click the Search icon.

   In the results that are displayed, if the version component of the segment is 001, then you need not perform the remaining steps of this procedure. The following screenshot shows this page:



3. If the version component of the segment is anything other than `001`, then:
   a. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
   b. Search for and open the lookup definition.
   c. For values in the Decode column that contain segment details, change the segment version (last three digits) to the version that you determined in the preceding step.
   d. Click the Save icon after you modify all relevant Decode values.

2.3.3 Configuring Reconciliation of Manager ID Attribute Values

> **See Also:**
>
> Reconciliation of the Manager ID Attribute for information about the sequence of steps involved in this process.

To configure reconciliation of manager ID attribute values:

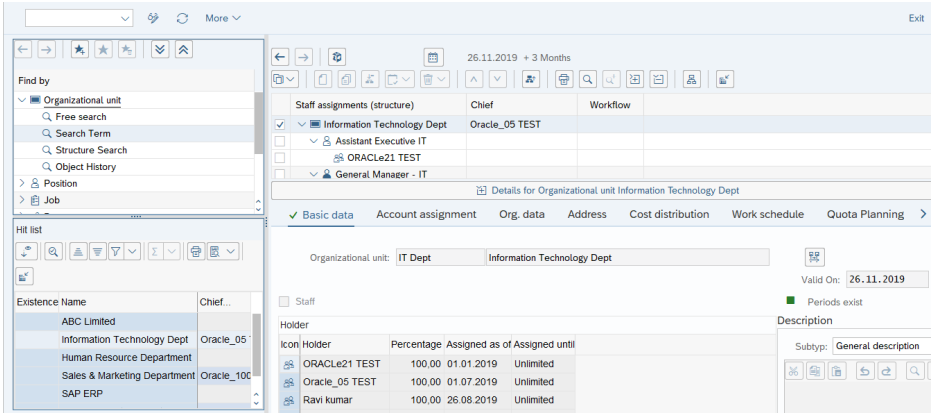
1. In the Lookup.SAP.HRMS.TopmostOrganization lookup definition, enter details of the top-most organization for each organization hierarchy.

   There may be multiple organization hierarchies defined on the target system. Each hierarchy has one top-most organization and other member organizations. In the Lookup.SAP.HRMS.TopmostOrganization lookup definition, you must manually create entries for all top-most organizations.

> **Note:**
>
> The value of this lookup definition is specified as the value of the Top most organization lookup entry in the Lookup.SAP.HRMS.Configuration lookup definition.

   To create entries for the top-most organizations:

   - On the target system:
     a. Run transaction PPOSE.
     b. For each hierarchy displayed in the list of hierarchies on the left pane:
        i. Double-click the hierarchy.
        ii. In the Staff Assignments region, the first organization is the topmost organization. Write down the ID of the organization.



   - On Oracle Identity Manager:
     a. Open the Lookup.SAP.HRMS.TopmostOrganization lookup definition.
     b. For each topmost organization that you identify:
        i. Click **Add**.
        ii. In the Code Key and Decode columns, enter the organization ID of the topmost organization.
        The following table shows sample entries in the Lookup.SAP.HRMS.TopmostOrganization lookup definition:

Code	Decode
00000001	00000001

Code	Decode
00000100	00000100

Both sample entries represent topmost organizations defined on the target system.

iii. After you create entries for all topmost organizations, click the Save icon.

2. Configure and run the SAP HRMS Manager Lookup Recon scheduled task.

Configure and run the SAP HRMS Manager Lookup Recon scheduled task.

This scheduled task performs the following functions:

- Reads entries for the topmost organization defined in the Lookup.SAP.HRMS.TopmostOrganization lookup definition.
- Populates the Lookup.SAP.HRMS.OrgHierarchy lookup definition with entries representing the other organizations within each hierarchy on the target system. In the entries created by the scheduled task, the Code Key column is the ID of an organization and the Decode column is the ID of the corresponding parent organization.
- Populates the Lookup.SAP.HRMS.OrgManager lookup definition with organization and manager mappings. The Code Key column holds the IDs of organizations and the Decode column holds the personnel numbers of the corresponding managers.

Table 2-3 describes the attributes of this scheduled task.

Table 2-3 Attributes of the SAP HRMS Manager Lookup Recon Scheduled Task

Attribute	Description
Schedule Task Name	This attribute holds the name of the scheduled task. Default value: `SAP HRMS Manager Lookup Recon` **Note**: For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that scheduled task as the value of the attribute in that scheduled task.
IT Resource	Enter the name of the IT resource that you configure by performing the procedure described in Configuring the IT Resource. Default value: `SAP HR IT Resource`

Table 2-3 (Cont.) Attributes of the SAP HRMS Manager Lookup Recon Scheduled Task

Attribute	Description
Configuration Lookup	This attribute holds the name of the lookup definition that holds configuration data for the connector. Default value: `Lookup.SAP.HRMS.Configuration` **Note**: You must not change this value for this instance of the connector. However, if you create a copy of the Lookup.SAP.HRMS.Configuration lookup definition, then you can specify the name of that lookup definition as the value of the Configuration Lookup attribute.
Top Most Organization Lookup	This attribute holds the name of the lookup definition that stores the organization IDs of top-most organizations in each organization hierarchy on the target system. Default value: `Lookup.SAP.HRMS.TopmostOrganization` **Note**: You must not change this value for this instance of the connector. However, if you create a copy of the Lookup.SAP.HRMS.TopmostOrganization lookup definition, then you can specify the name of that lookup definition as the value of the Top Most Organization Lookup attribute.

2.3.4 Configuring the Target System for Generation of IDocs

User data is moved from the target system to Oracle Identity Manager through "push" technology. The Application Link Enabling (ALE) feature of SAP is the foundation of this mode of data transfer.

This section describes procedures involved in configuring the target system. You may need the assistance of an SAP Basis administrator to perform some of these procedures.

The following link describes procedures to create the ALE components that are used during generation of IDocs:

- Checking Whether a Sender Logical System Already Exists
- Defining the Sending and Receiver Logical Systems
- Assigning a Client to the Sender Logical System
- Defining the Distribution Model
- Creating the File Port
- Defining the Partner Profile
- Registering the Listener with the SAP Gateway (tRFC)

- Creating the tRFC Port
- Activating Change Pointers
- Configuring Segment Filtering
- Configuring SAP Ports for Communication with Oracle Identity Manager

For more information on procedures to create ALE components, see the following link: https://wiki.scn.sap.com/wiki/display/ABAP/7+Steps+For+ALE+Configuration

> **Note:**
>
> - Select either the Transfer IDocs immediately or the Collect IDocs.
>   - For incremental reconciliation, select Transfer IDocs immediately Instead, the job that you schedule on the target system will be used to transfer IDocs in flat-file format to the port.
>   - For full reconciliation, select the Collect IDocs option. By selecting this option, you specify that IDocs must not be transferred to the port as and when they are created.
> - While performing the procedure described in Configuring the IT Resource , you specify the same program ID as the value of the Program ID parameter of the IT resource.

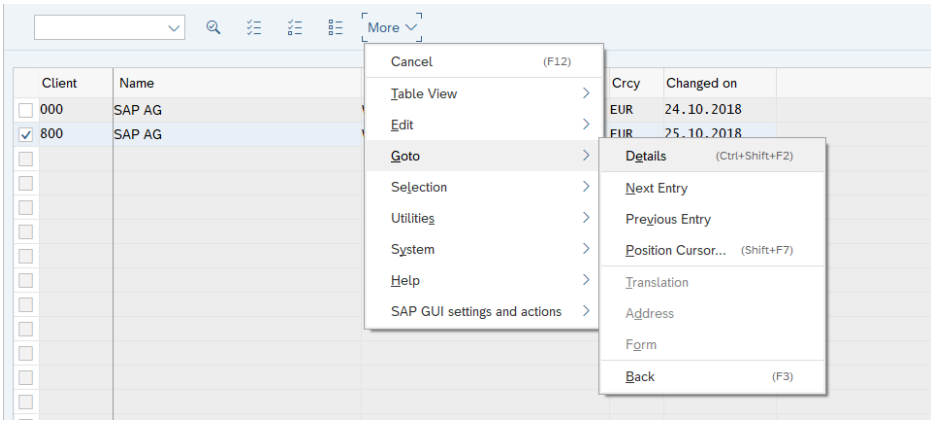
2.3.4.1 Checking Whether a Sender Logical System Already Exists

You must create a sender logical system to represent SAP and a receiver logical system to represent Oracle Identity Manager.

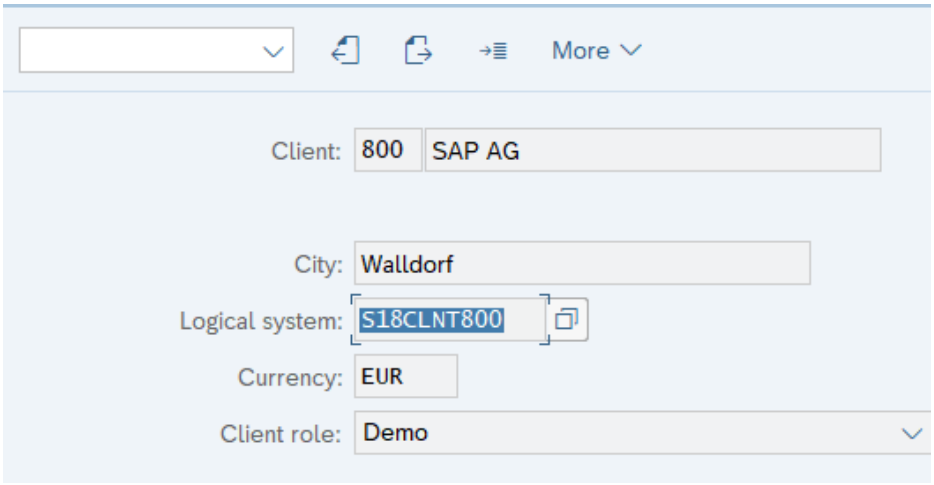
If there is an existing sender logical system to represent SAP, then you need not define another sender logical system. Similarly, if a client is assigned to the existing sender logical system, then you need not assign another client.

To check if the sender logical system has been defined and if a client has been associated with it:

1. Run transaction SCC4.
2. Use the Table View menu to switch to the change mode.
3. For each client in the list of clients displayed:
   a. Select the client.
   b. From the Goto menu, click **Details**. The details of the client are displayed.



c. In the Logical System field, check if a logical system has been selected. If a logical system is selected for a particular client, then you know that a sender logical system with a client associated with it already exists. You need not define a sender logical system, and you need not associate a client with the sender logical system.



2.3.4.2 Defining the Sending and Receiver Logical Systems

You must create a sender logical system to represent SAP and a receiver logical system to represent Oracle Identity Manager

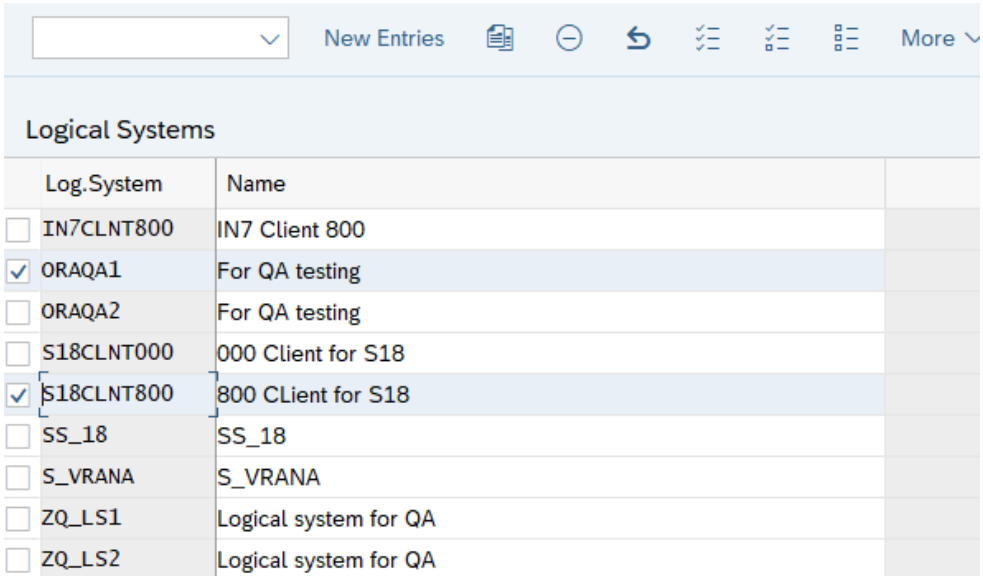
If there is an existing sender logical system to represent SAP, then you need not define another sender logical system. Similarly, if a client is assigned to the existing sender logical system, then you need not assign another client.

If you determined that a sender logical system does not exist, then you must create the sender logical system. In addition, you must create the receiver logical system.

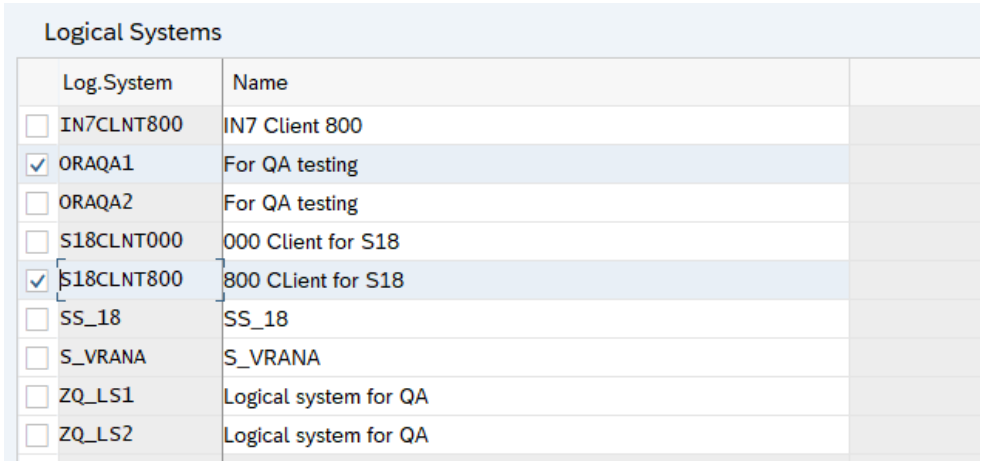
To create the sending or receiver logical system:

1. Run transaction BD54.
2. Click **New Entries**. A new row is added.
3. Enter a name for the logical system

   To specify a name for the sender logical system, you can use the <SYSTEM_ID>CLNT<CLIENT_NUMBER> format, for example, S18CLNT800.



To specify a name for the receiver logical system, you can use a name like ORAQA1. This is to help distinguish between the receiver logical system created for Oracle Identity Manager and other receiver logical systems.



4. Click the Save icon.

   If the sender logical system has been created, then repeat the procedure to create the receiver logical system.

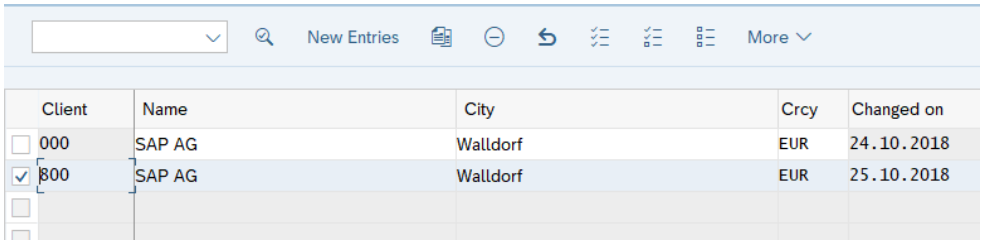
2.3.4.3 Assigning a Client to the Sender Logical System

The sender logical system must have a client associated with it. If there is an existing client associated with the sender logical system, then you need not associate another client.

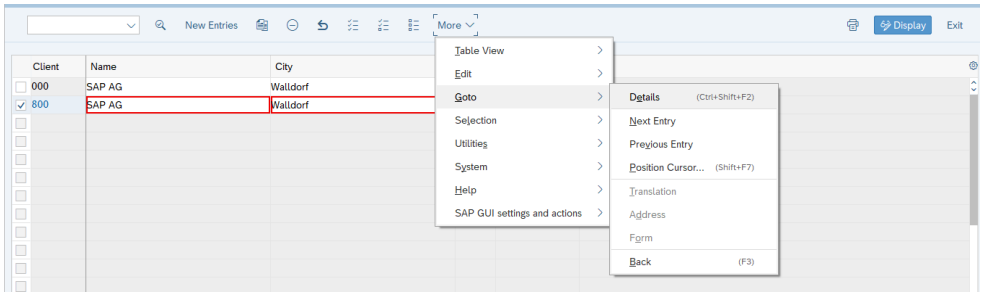
> **Note:**
>
> A logical system can have only one client associated with it.

To associate a client with the sender logical system:

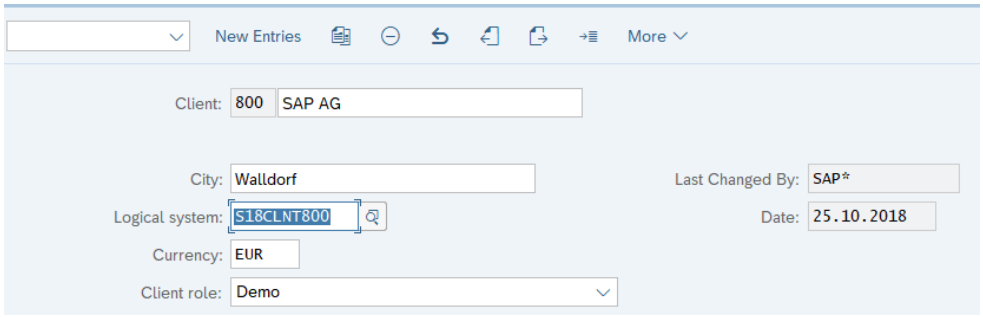
1. Run transaction SCC4.
2. Use the Table View menu to switch to the change mode.
3. From the list of clients displayed, select the client that you want to associate with the sender logical system.



4. From the Goto menu, click Details. The details of the client are displayed.



5. In the Logical System field, select the sender logical system.



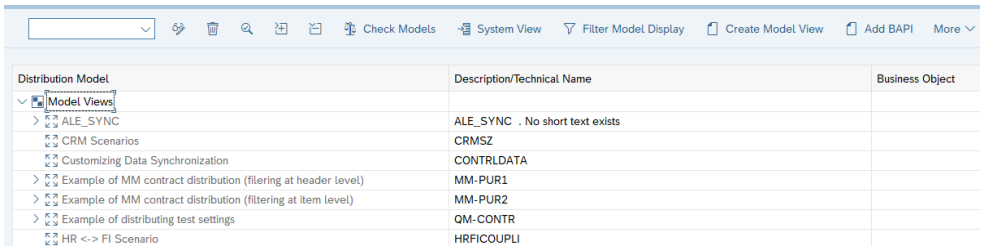
6. Click the Save icon.

2.3.4.4 Defining the Distribution Model

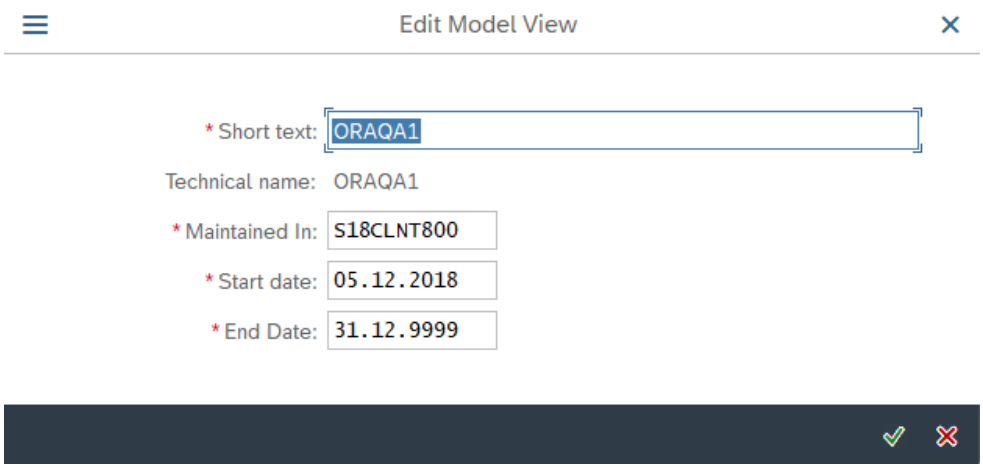
The distribution model holds information about the sending and receiver logical systems that you define and the message type that flows between them.

To define the distribution model:

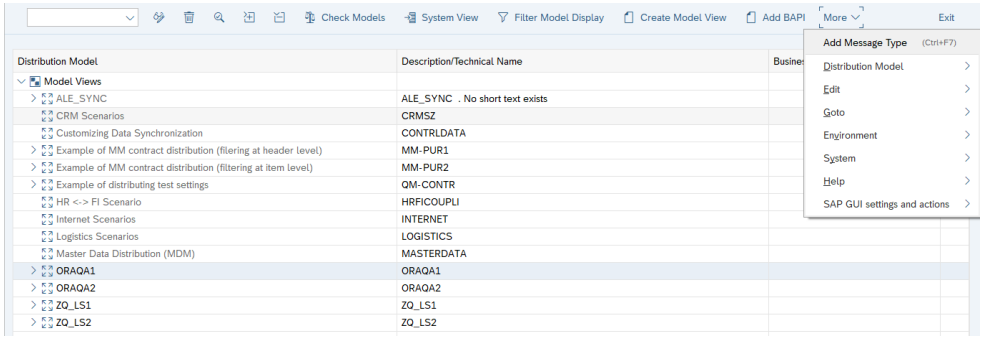
1. Run transaction BD64.
2. Switch to the Edit mode.
3. From the Edit mode, select Model View, and then select Create.



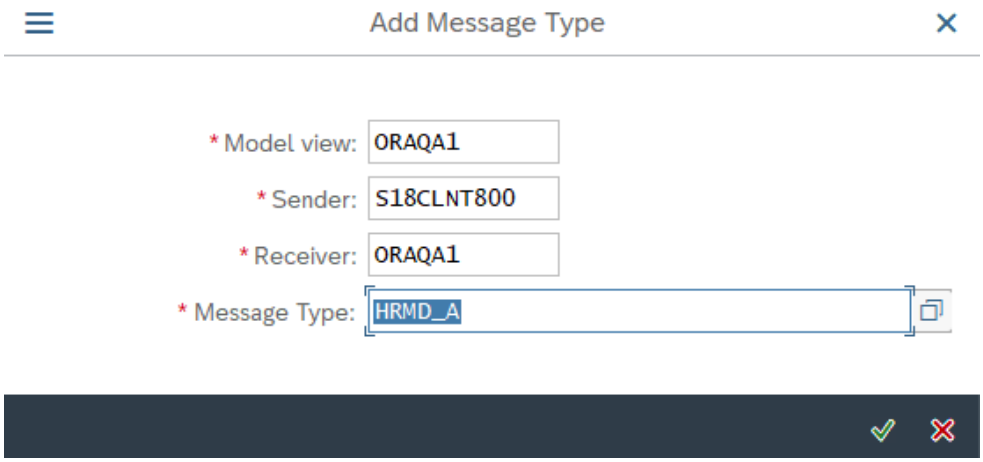
4. In the Create Model View dialog box, enter values for the Short Text and Technical Name fields, and accept the default Start date and End date values.



5. Click the Save icon.
6. From the list of views, select the created view, and then click Add message type.



7. In the Add Message Type dialog box, specify the names of the sending and receiver logical systems and then specify HRMD_A as the message type.



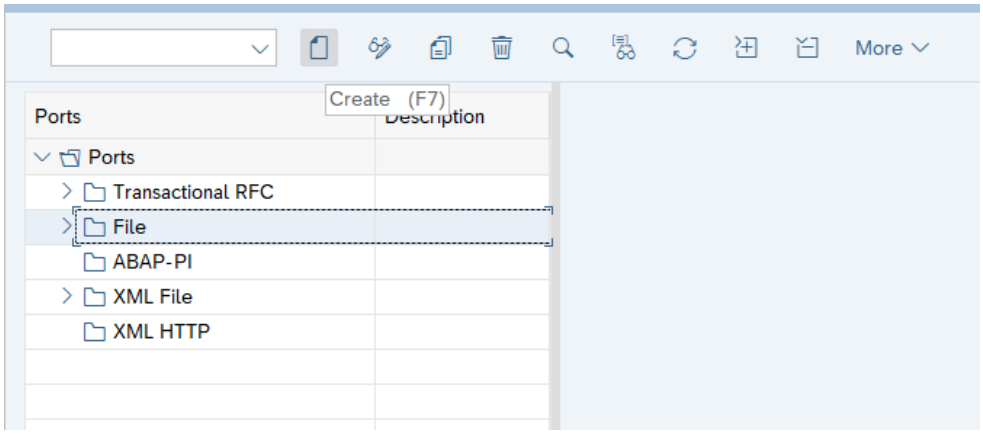
8. Save the entry.

2.3.4.5 Creating the File Port

The file port is a definition of the directory location and name of the file in which IDocs are recorded. In full reconciliation, IDocs for all existing target system users is generated and written to flat files. The file port holds the directory location and name of these flat files.

To create the file port:

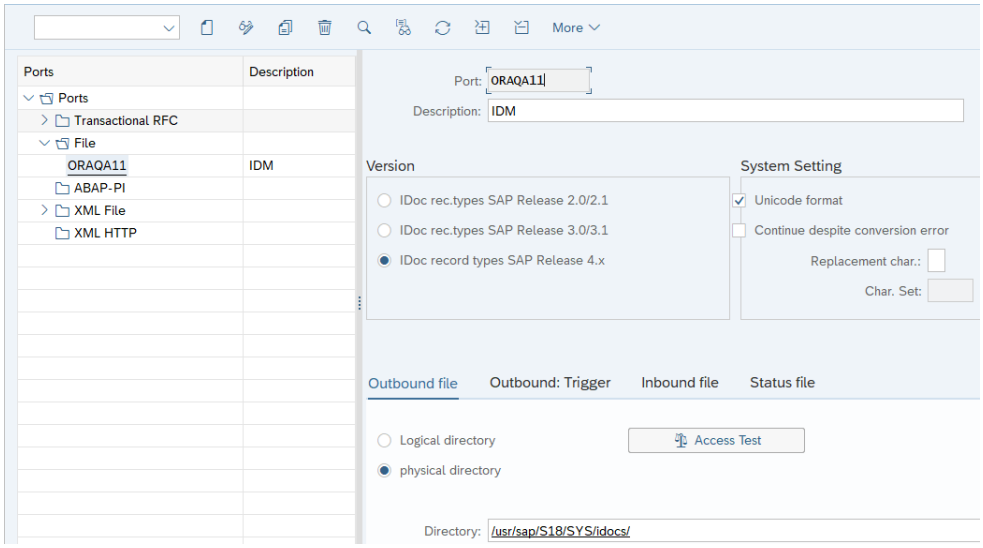
1. Run transaction WE21.
2. Expand **Ports**, select **File**, and then click **Create**.



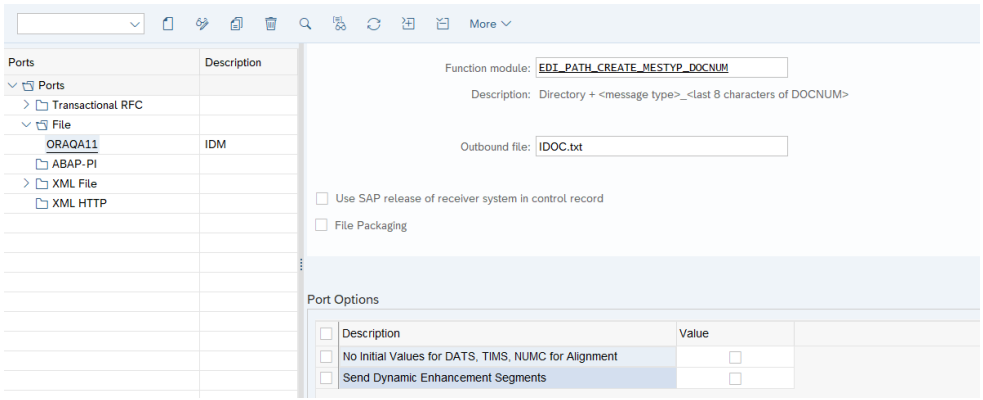
3. Enter the following details:
   - Port: Enter a name for the file port.
   - Description: Enter a description for the port.
   - Version: Select **IDoc record types SAP Release 4.*x***
   - System Setting: Select **Unicode** format
   - On the Outbound file tab:
     - Physical directory: Specify the path of the directory in which you want the file containing IDocs to be placed.

- Function module: Select a naming convention for the flat file, for example, *EDI_PATH_CREATE_MESTYP_DOCNUM*
- Outbound file: This is the alternative to the Function Module (preceding field) approach to naming the flat file. You use the Outbound file field to specify a fixed name for the flat file. It is recommended that you specify a function module instead of entering a fixed name for the flat file in the Outbound file field. The advantage of the Function Module approach is that the name of the generated file will be time stamped.

Screenshot 1:



Screenshot 2:



4. Click the Save icon.

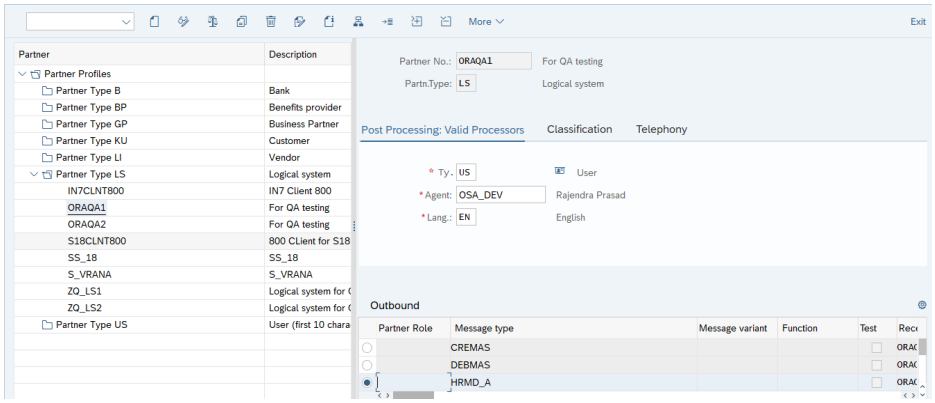
2.3.4.6 Defining the Partner Profile

A partner profile is a mapping of the receiver logical system, ports used by the receiver logical system, and IDoc collection mode.

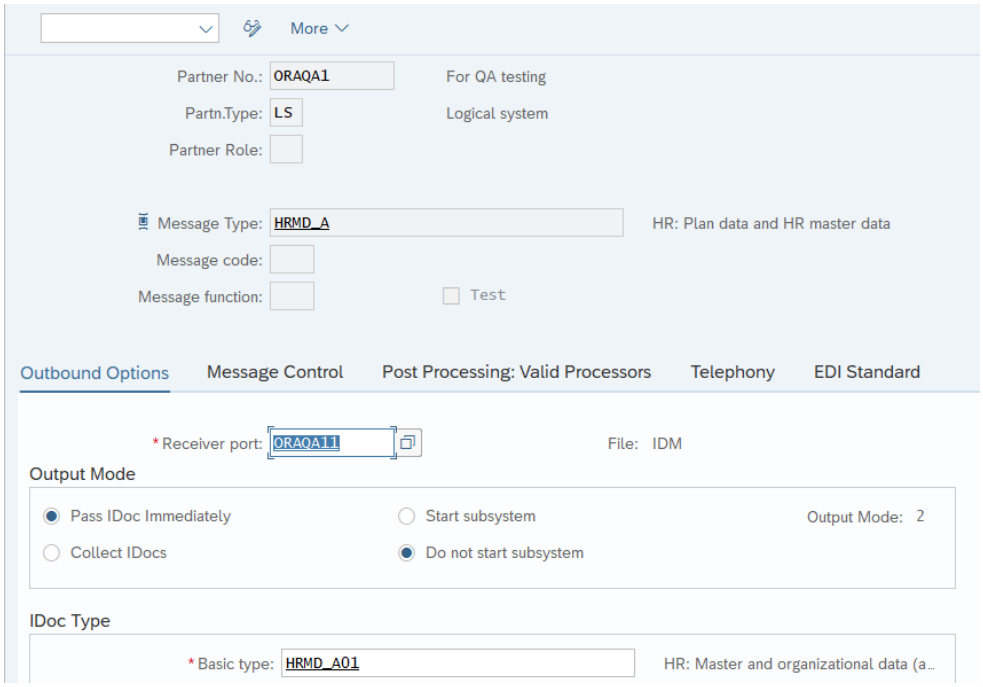
> **Note:**
>
> When you start using the connector to reconcile user data from the target system, you use the partner profile to switch between full and incremental reconciliation. When you switch to full reconciliation, the scheduled task for incremental recon continues to run. However, IDocs are not sent to Oracle Identity Manager.

To define the partner profile:

1. Run transaction WE20.
2. Expand Partner Profiles, select Partner Type LS, click the Create icon, and then enter the following details.
   - In the Partner no. field, enter the name that you specify for the receiver logical system while performing the procedure described in Defining the Sending and Receiver Logical Systems.
   - In the Outbound Parameters table, double-click HRMD_A in the Message Type column.



   - On the Outbound Options tab:
     - In the Receiver port field, select the file port that you define by performing the procedure described in Creating the File Port.
     - In the Output Mode region, select Collect IDocs. By selecting this option, you specify that IDocs must not be transferred to the file port as and when they are created. Instead, the job that you schedule on the target system will be used to transfer IDocs in flat-file format to the file port.
     - In the IDoc Type region, specify an IDoc type in the Basic type field. It is recommended that you select the latest IDoc type available in the system. In addition, if you want to use an existing extension to an IDoc type, then specify the extension in the Extension field.



3. Save the entry.

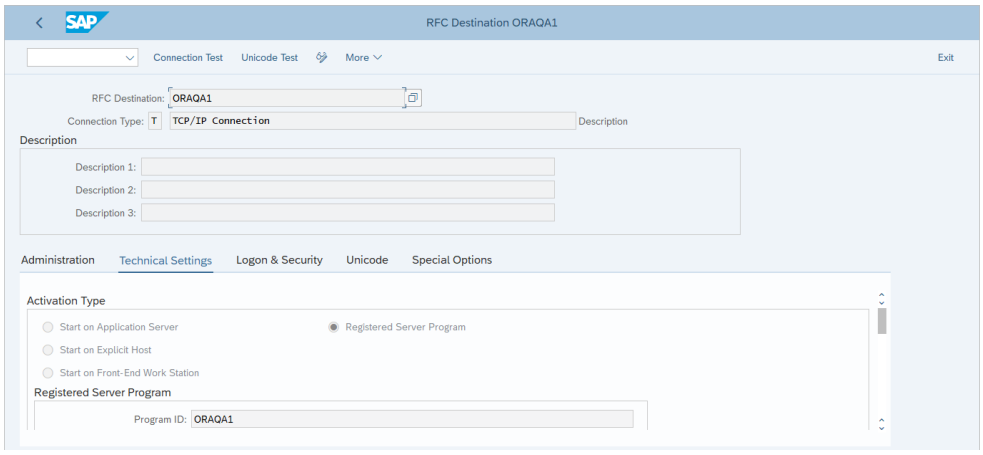
2.3.4.7 Registering the Listener with the SAP Gateway (tRFC)

To register the listener with the SAP gateway, create an RFC destination as follows:

1. Run transaction SM59.
2. Select **TCP/IP** connections, and then click the **Create** icon.
3. In the RFC destination field, enter a name for the listener, for example `ORAQA1`.
4. In the Connection type field, select **T** to specify that this is a TCP/IP connection.
5. In the Description region, enter a description for the listener.
6. On the Technical settings tab, in the Activation Type region, select **Registered Server Program**.
7. In the Program ID field, enter the program ID that you want to set for the listener, for example, `ORAQA1`.

> **Note:**
>
> While performing the procedure described in Configuring the IT Resource, you specify the same program ID as the value of the Program ID parameter of the IT resource.

Figure 2-1 Program ID field of the Listener



8. The target (Oracle Identity Manager) is a Unicode system. On the MDMP & Unicode tab, select the **Unicode** option to configure the port for Unicode.
9. Use the Test connection and Unicode Test features to run the connectivity and Unicode tests as follows:
   a. Run transaction SM59.
   b. In the RFC Destination field, enter the name of the RFC destination that you create.
   c. In the Connection type field, select **TCP/IP connections**.
   d. Click **Test connection**. Connection test data must be displayed.
   e. Click **Unicode Test**.

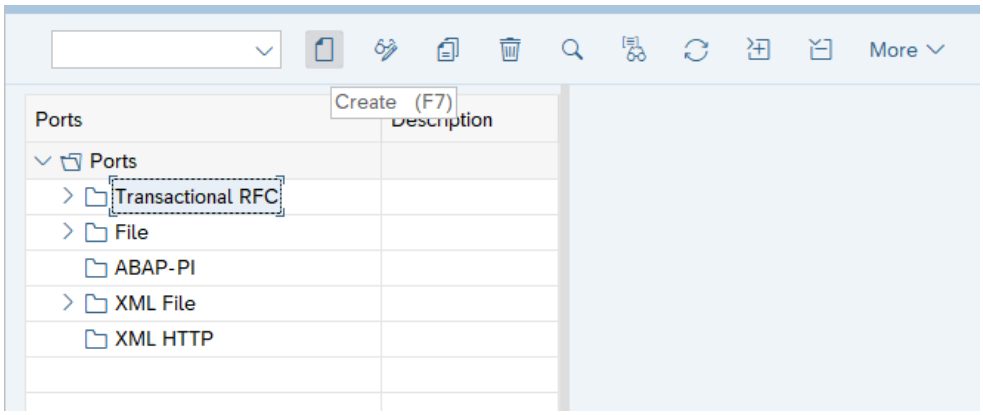
   A message stating that the target is a Unicode system is displayed.

2.3.4.8 Creating the tRFC Port

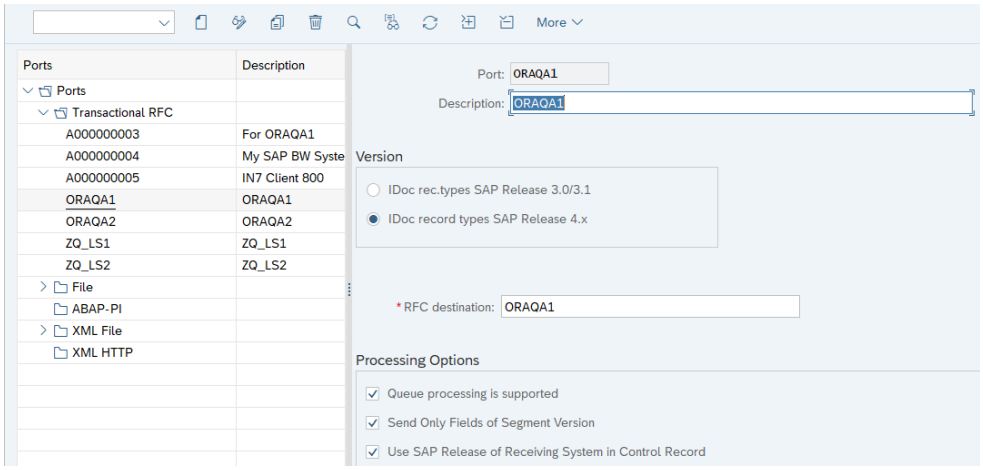
Transactional RFC (tRFC) on SAP is a variant of the Remote Function Call feature. The tRFC port on SAP is used by the listener, which is a scheduled task running on Oracle Identity Manager. The listener picks up IDocs delivered at the tRFC port. These IDocs are in the form of Java objects; there is no exchange of physical files at the tRFC port.

To create the tRFC port:

1. Run transaction WE21.
2. Select **Transactional RFC**, and then click the **Create** icon.



3. In the Ports in IDoc Processing dialog box, either select **Generate port name** or specify a port name.
4. In the RFC destination field, enter the RFC destination that you defined by performing the procedure described in Registering the Listener with the SAP Gateway (tRFC).



5. Click the Save icon.

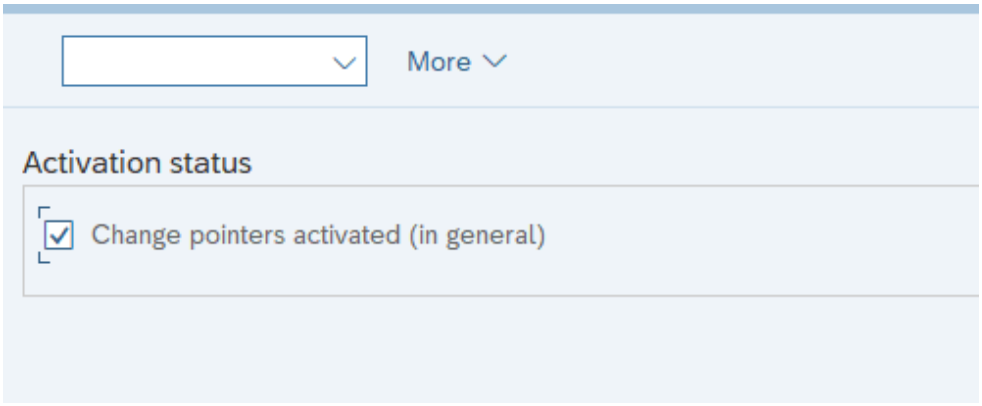
2.3.4.9 Activating Change Pointers

Change pointers are used to record updates to user data on the target system. These records are stored in special tables, and they are called change docs.

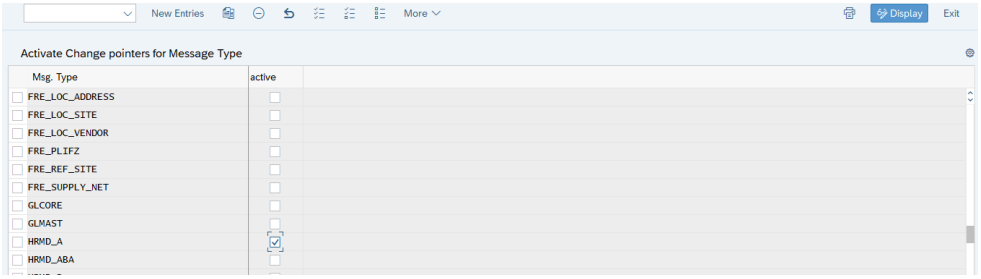
> **Note:**
>
> During incremental reconciliation, a change doc contains only data from attributes of infotypes in which at least one attribute has been modified. For example, consider the 0001 infotype. This infotype holds the MSTBR attribute and some other attributes. If this attribute is modified, then during the next incremental reconciliation run, all the attributes of the 0001 infotype are copied into the change doc that is created to track the change in the MSTBR attribute.

To activate change pointers:

1. Run transaction BD61.
2. Select the **Change pointers activate – generally** check box.



3. Run transaction BD50.
4. In the list that is displayed, select the check box for the HRMD_A message type.



5. Click the Save icon.

2.3.4.10 Configuring Segment Filtering

> **Note:**
>
> The procedure described in this section is optional. Segment filtering is not a requirement for using the ALE feature.

On the target system, multiple attributes of the same type are grouped under an infotype. Multiple infotypes are grouped under a segment. There are more than 100 predefined segments on the target system.

The Lookup.SAP.HRMS.AttributeMapping lookup definition maps attributes of the target system with OIM User fields. Only data from mapped attributes is reconciled into Oracle Identity Manager, regardless of the segments (that is, attributes) in the IDocs received by Oracle Identity Manager. This is illustrated by the following example:

Suppose there are 14 attribute mappings in the Lookup.SAP.HRMS.AttributeMapping lookup definition. If the IDocs contain data for 30 attributes, then only data from the 14 mapped attributes is reconciled into Oracle Identity Manager. Data for the remaining 16 attributes is not used at all.

The segment filtering feature of the target system enables you to specify the segments that must not be included in IDocs. By configuring segment filtering, you ensure that

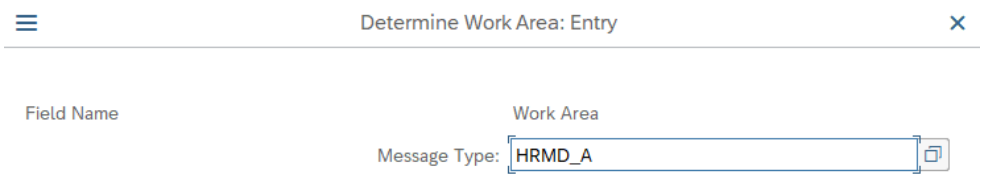
attribute data that is not required in Oracle Identity Manager is not brought to Oracle Identity Manager.

Segment filtering is applied at the IDoc creation stage. Change docs are created for a change in any attribute of infotypes in any segment.

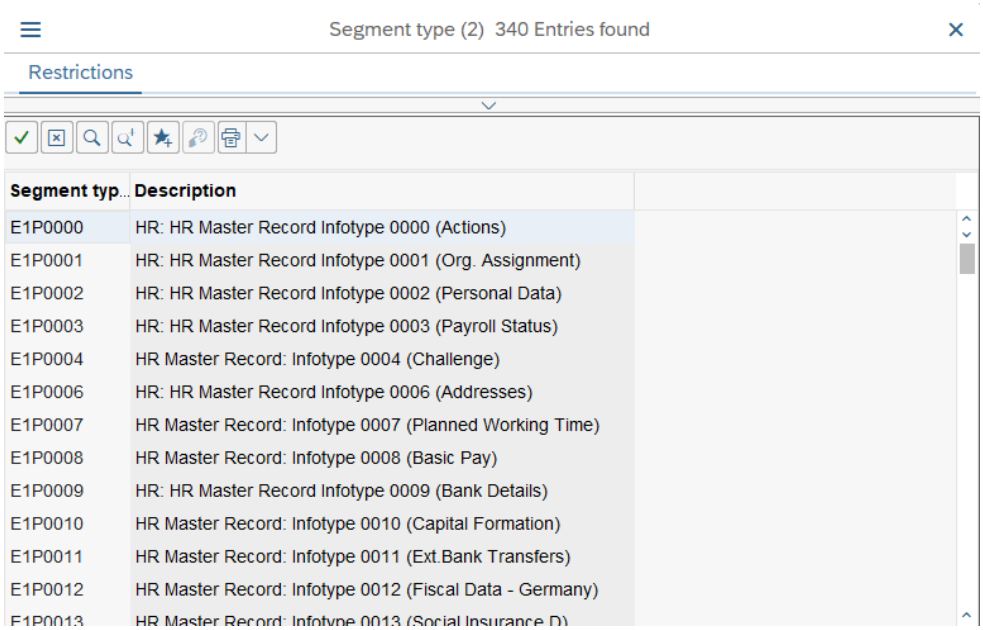
> **Note:**
>
> When you configure segment filtering, you must ensure that the E1P0000, E1P0001, E1P0002, E1P0006 and E1P0105 segments are always included. Some attributes from infotypes in these segments are configured as predefined attributes that are mapped to OIM User attributes. See Structure of a Sample IDoc for information about the structure of a sample IDoc.
>
> You can configure and then reconfigure segment filtering at any time after deployment. While configuring segment filtering, you must ensure that mandatory attributes defined in the target system and Oracle Identity Manager are always included.

To configure segment filtering:

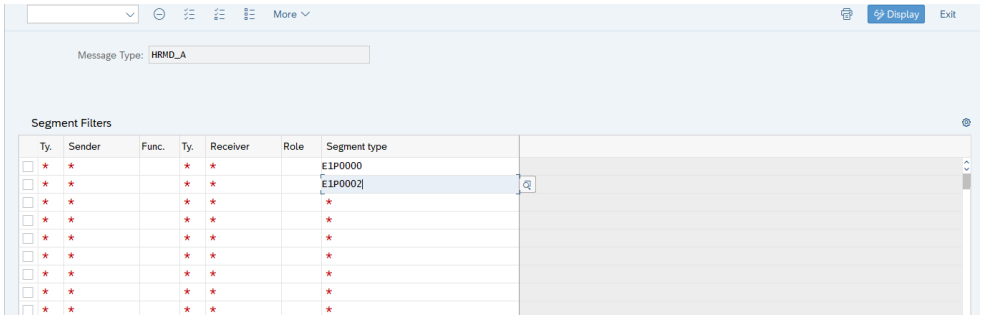
1. Run transaction code BD56.
2. In the Determine Work Area: Entry dialog box, select the HRMD_A message type.



3. Click **New Entries**.
4. Click the first row of the Segment Type column, and then press F4.



5. From the Segment Type list, select the segments that you want to exclude using segment filtering.



6. Click the Save icon.

2.3.4.11 Configuring SAP Ports for Communication with Oracle Identity Manager

To enable communication between the target system and Oracle Identity Manager, you must ensure that the ports listed in Table 2-4 are open.

Table 2-4 Ports for SAP Services

Service Port Number	Format Default Port
Dispatcher 32*SYSTEM_NUMBER*	3200
Gateway (for non-SNC communication) 33*SYSTEM_NUMBER*	3300
Gateway (for SNC communication) 48*SYSTEM_NUMBER*	4800
Message server 36*SYSTEM_NUMBER*	3600

To check if these ports are open, you can, for example, try to establish a Telnetconnection from Oracle Identity Manager to these ports.

2.3.5 Changing to the Required Input Locale on Oracle Identity Manager

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

You may require the assistance of the system administrator to change to the required input locale.

2.3.6 Clearing Content Related to Connector Resource Bundles from the Server Cache

> **Note:**
>
> In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the Oracle Identity Manager database. Whenever you add a new resource bundle to the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, switch to the *OIM_HOME*/server/bin directory.

   > **Note:**
   >
   > You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:
   >
   > *OIM_HOME*/server/bin/*SCRIPT_FILE_NAME*

2. Enter one of the following commands:

> **Note:**
>
> You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat` ***CATEGORY_NAME*** on Microsoft Windows or `PurgeCache.sh` ***CATEGORY_NAME*** on UNIX. The ***CATEGORY_NAME*** argument represents the name of the content category that must be purged.
>
> For example, the following commands purge Metadata entries from the server cache:
>
> `PurgeCache.bat MetaData`
>
> `PurgeCache.sh MetaData`

On Microsoft Windows: `PurgeCache.bat All`

On UNIX: `PurgeCache.sh All`

When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

`t3://`*`OIM_HOST_NAME`*`:`*`OIM_PORT_NUMBER`*

In this format:

- Replace *`OIM_HOST_NAME`* with the host name or IP address of the Oracle Identity Manager host computer.
- Replace *`OIM_PORT_NUMBER`* with the port on which Oracle Identity Manager is listening.

2.3.7 Copying Resource Bundle Entries for UDFs

If you are using a non-English locale, then copy entries for the UDFs from the connector resource bundle to the customResources_LOCALE.properties file.

The following example illustrates this procedure:

Suppose you are using the French locale. When you install Oracle Identity Manager, the customResources_fr.properties file is copied into the Oracle Identity Manager database for Oracle Identity Manager release 11.1.*x*.

1. Open the customResources_fr.properties file in a text editor.
2. Copy the following lines present in the SAP-ER_fr.properties file:

```
global.udf.USR_UDF_DEPARTMENT=Service

global.udf.USR_UDF_CITY=Ville

global.udf.USR_UDF_STREET=Rue

global.udf.USR_UDF_DISTRICT=District

global.udf.USR_UDF_COUNTRY=Pays

global.udf.USR_UDF_POSTALCODE=Code postal
```

```
global.udf.USR_UDF_TELEPHONE=Num\u00E9ro de
t\u00E9l\u00E9phone

global.udf.USR_UDF_LINKED_USER_ID=ID d'utilisateur SAP
li\u00E9

global.udf.USR_UDF_POSITION=Fonction

global.udf.USR_UDF_COST_CENTER=Centre de co\u00FBts

global.udf.USR_UDF_USR_CREATE_FROM_HRMS=Utilisateur
cr\u00E9\u00E9 \u00E0 partir de HRMS

global.udf.USR_UDF_SUB_GROUP=Sous-groupe
```

3. Paste these lines in the following section of the *OIM_HOME*/xellerate/customResources/customResources_fr.properties file:

   # For UDF Label addition:

   # global.udf.*UDF_COLUMN_NAME=UNICODED_LABEL_STRING*

4. Save and close the customResources_fr.properties file.

2.3.8 Managing Logging

If you are using Oracle Identity Manager release 11.1.*x*, perform the instructions in the following sections:

- Understanding Log Levels
- Enabling Logging

2.3.8.1 Understanding Log Levels

When you enable logging, Oracle Identity Governance automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations.

> **Note:**
>
> In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

Oracle Identity Manager release 11.1.x uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

  This level enables logging of information about errors that might allow Oracle Identity Governance to continue running.

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

  This level enables logging of messages that highlight the progress of the application.

- CONFIG

  This level enables logging of information about fine-grained events that are useful for debugging.

- FINE, FINER, FINEST

  These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These message types are mapped to ODL message type and level combinations as shown in Table 2-5.

Table 2-5 Log Levels and ODL Message Type:Level Combinations

Java Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

The configuration file for OJDL is logging.xml, which is located at the following path:

DOMAIN_HOME/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

Here, *DOMAIN_HOME* and *OIM_SEVER* are the domain name and server name specified during the installation of Oracle Identity Governance.

2.3.8.2 Enabling Logging

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:
   a. Add the following blocks in the file:

```
<log_handler name='sap-er-handler' level='[LOG_LEVEL]'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path' value='[FILE_NAME]'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>
```

```
<logger name="OIMCP.SAPH" level="[LOG_LEVEL]" useParentHandlers="false">
     <handler name="sap-er-handler"/>
     <handler name="console-handler"/>
   </logger>
```

b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2-5 lists the supported message type and level combinations.

   Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages to be recorded.

   The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]**:

```
<log_handler name='sap-er-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers
\oim_server1\logs\oim_server1-diagnostic-1.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="OIMCP.SAPH" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="sap-er-handler"/>
     <handler name="console-handler"/>
   </logger>
```

   With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION:1 level are recorded in the specified file.

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:

   For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

   For UNIX:

```
export WLS_REDIRECT_LOG=FILENAME
```

   Replace ***FILENAME*** with the location and name of the file to which you want to redirect the output.

4. Restart the application server.

2.3.9 Configuring Reconciliation of Effective-Dated Target System Events

> **Note:**
>
> If you do not perform the procedure described in this section, then support for effective-dated events is disabled. In other words, an event is brought to Oracle Identity Manager, regardless of the effective date of the infotype. See Reconciliation of Effective-Dated Lifecycle Events for information about how future-dated events are processed.

On the target system, events IDs are assigned to all employee lifecycle events. The connector can distinguish between current-dated and future-dated lifecycle events related to hiring employees and terminating the services of employees.

To enable this feature of the connector, define the event IDs as follows:

1. Enter the following as values for the import parameters of the standard BAPI_HELPVALUES_GET BAPI and run BAPI:

   > **Note:**
   >
   > You need not specify values for the parameters that are not listed in the table.

Import Parameter	Value
OBJTYPE	EMPLOYEET
METHOD	GETPASSWORD
PARAMETER	STATUSINFO
EXPLICIT_SHLP-SHLPNAME	H_T529A
EXPLICIT_SHLP-SHTYPE	SH
MAX_OF_ROWS	0

2. Write down the events IDs for all Hire and Terminate events listed in the HELPVALUES table on the target system that you want to define in Oracle Identity Manager.
3. In the Lookup.SAP.HRMS.HireEvents lookup definition on Oracle Identity Manager, enter the events IDs for all hire events (events that occur when an employee is hired for the first time). In each row that you add, enter the same event ID in the Code Key and Decode columns.
4. In the Lookup.SAP.HRMS.TerminateEvents lookup definition on Oracle Identity Manager, enter events IDs for the events (for example, events created when an employee resigns, is terminated, or is on long leave) that disable employees (records) in Oracle Identity Manager. In each row that you add, enter the same event ID in the Code Key and Decode columns.

5. In the Lookup.SAP.HRMS.RehireEvents lookup definition on Oracle Identity Manager, enter events IDs for the events (for example, events created when an employee re-joins the company or returns from long leave) that enable employees (records) in Oracle Identity Manager that are in the disabled state. In each row that you add, enter the same event ID in the Code Key and Decode columns.

2.3.10 Recovering from Failed Communication Between the Target System and Oracle Identity Manager

What Happens When the Listener Becomes Unavailable

When an IDoc is sent to the listener running on Oracle Identity Manager during incremental reconciliation, the status of the IDoc on the target system is changed to "Transferred to Destination." This status change takes place regardless of whether or not the listener is available.

If you determine that the listener was unavailable for some time, then you can reset the status of the IDocs on the target system and then resend them to Oracle Identity Manager.

What Happens When the Target System Becomes Unavailable

The listener receives an exception, which is recorded in the log file. When the target system becomes available again, the listener starts receiving IDocs again.

2.3.11 Configuring SNC to Secure Communication Between Oracle Identity Manager and the Target System

Oracle Identity Manager uses a Java application server. To connect to the SAP system application server, this Java application server uses the SAP Java connector (JCo). If required, you can use Secure Network Communication (SNC) to secure communication between Oracle Identity Manager and the SAP system.

This section discusses the following topics:

- Prerequisites for Configuring the Connector to Use SNC
- Installing the Security Package
- Configuring SNC

2.3.11.1 Prerequisites for Configuring the Connector to Use SNC

The following are prerequisites for configuring the connector to use SNC:

- SNC must be activated on the SAP application server.
- You must be familiar with the SNC infrastructure. You must know which Personal Security Environment (PSE) the application server uses for SNC.

2.3.11.2 Installing the Security Package

To install the security package on the Java application server used by Oracle Identity Manager:

1. Download SAP Cryptolib for encrypted communication with Oracle Identity Manager.

   The necessary SAP Cryptolib for the encrypted communication of third-party software can be downloaded directly from the SAP Service Marketplace.
2. Extract the contents of the SAP Cryptographic Library installation package. This package contains the following files:
   - SAP Cryptographic Library (sapcrypto.dll for Microsoft Windows or libsapcrypto.ext for UNIX)
   - A corresponding license ticket (`ticket`)
   - The configuration tool, sapgenpse.exe
3. Copy the library and the sapgenpse.exe file into a local directory. For example: C:/usr/sap
4. Check the file permissions. Ensure that the user under which the Java application server runs is able to run the library functions in the directory into which you copy the library and the sapgenpse.exe file.
5. Create the sec directory inside the directory into which you copy the library and the sapgenpse.exe file.

   > **Note:**
   >
   > You can use any names for the directories that you create. However, creating the C:\usr\sap\sec (or /usr/sap/sec) directory is SAP recommendation.
6. Copy the ticket file into the sec directory. This is also the directory in which the Personal Security Environment (PSE) and credentials of the Java application server are generated.
7. Set the SECUDIR environment variable for the Oracle WebLogic Application Server user to the sec directory.

   > **Note:**
   >
   > From this point onward, the term *SECUDIR directory* is used to refer to the directory whose path is defined in SECUDIR environment variable.
8. Set the SNC_LIB and PATH environment variables for the user of the Java application server to the cryptographic library directory, which is the parent directory of the sec directory.

2.3.11.3 Configuring SNC

To configure SNC:

1. Either create a PSE or copy the SNC PSE of the SAP application server to the SECUDIR directory. To create the SNC PSE for the Java application server, use the sapgenpse.exe command-line tool as follows:

a. To determine the location of the SECUDIR directory, run the `sapgenpse` command without specifying any command options. The program displays information such as the library version and the location of the SECUDIR directory.

b. Enter a command similar to the following to create the PSE:

```
sapgenpse get_pse -p PSE_Name -x PIN Distinguished_Name
```

The following is a sample distinguished name:

```
CN=SAPJ2EE, O=MyCompany, C=US
```

The `sapgenpse` command creates a PSE in the SECUDIR directory.

2. Create credentials for the Java application server.

The Java application server must have active credentials at run time to be able to access its PSE. To check whether or not this condition is met, enter the following command in the parent directory of the SECUDIR directory:

```
Sapgenpse seclogin
```

Then, enter the following command to open the PSE of the server and create the credentials.sapgenpse file:

```
seclogin -p PSE_Name -x PIN -O [NT_Domain\]user_ID
```

The *user_ID* that you specify must have administrator rights. *PSE_NAME* is the name of the PSE file.

The credentials file, cred_v2, for the user specified with the `-O` option is created in the SECUDIR directory.

3. Exchange the public key certificates of the two servers as follows:

> **Note:**
>
> If you are using individual PSEs for each certificate of the SAP server, then you must perform this procedure once for each SAP server certificate. This means that the number of times you must perform this procedure is equal to the number of PSEs.

a. Export the Oracle Identity Manager certificate by entering the following command:

```
sapgenpse export_own_cert -o filename.crt -p PSE_Name -x PIN
```

b. Import the Oracle Identity Manager certificate into the SAP application server. You may require the SAP administrator's assistance to perform this step.

c. Export the certificate of the SAP application server. You may require the SAP administrator's assistance to perform this step.

d. Import the SAP application server certificate into Oracle Identity Governance by entering the following command:

```
sapgenpse maintain_pk -a serverCertificatefile.crt -p PSE_Name -x PIN
```

4. Configure the following parameters in the SAP HRMS IT Resource object:

- SAP lib
- SAP mode
- SAP myname
- SAP partnername
- SAP qop

2.3.12 Specifying Values for the Connection Properties (IT Resource Configuration)

The IT resource holds connection properties that are used by SAP JCo.
These connection properties are the ones accepted by the SAP JCo. The Lookup.SAP.HRMS.ITResourceMapping lookup definition holds mappings between the connection properties accepted by the SAP JCo API and the names of IT resource parameters.

> **Note:**
>
> The IT resource is used only during incremental reconciliation. In full reconciliation, you manually copy th e flat file containing user data to the Oracle Identity Manager host computer. See the Javadocs shipped with SAP JCo 3.0.8 for detailed information about connection properties used by the target system.

This section discusses the following topics:

- To meet the requirements of your operating environment, you might need to add connection properties to this default set of properties. For example, if the target system is behind a firewall, then you must also provide a value for the jco.client.saprouter connection property. To add a connection property, see the Mapping New Connection Properties.
- For instructions on specifying values for the IT resource parameters, see the Configuring the IT Resource.
- If your target system is a group of SAP instances that provide a load-balancing connection to applications such as Oracle Identity Manager, then perform the procedure described in the Parameters for Enabling the Use of a Logon Group.

2.3.12.1 Mapping New Connection Properties

To map a new connection property:

1. Add the connection property as a parameter in the SAP HR IT resource type definition as follows:
   a. On the Design Console, expand **Resource Management**, and then click **IT Resources Type Definition**.
   b. Search for and open the **SAP HR** IT resource type.
   c. Click **Add**.
   A new row is displayed in the IT Resource Type Parameter table.

d. In the **Field Name** column, enter a name for the parameter.

e. Do not enter values in any other field.

f. Click the Save icon.

2. Specify a value for the new parameter in the IT resource. See the Configuring the IT Resource for instructions.

3. In the Lookup.SAP.HRMS.ITResourceMapping lookup definition, create a mapping between the connection property and the IT resource parameter as follows:

   For Oracle Identity Manager prior to 11.1.2.1.0:

   a. On the Design Console, expand **Administration**, and then double-click **Lookup Definition**.

   b. Search for and open the **Lookup.SAP.HRMS.ITResourceMapping** lookup definition.

   c. Click **Add**.

   d. In the **Code Key** column, enter the connection property defined in the ServerDataProvider or DestinationDataProvider interface of SAP JCo 3.0.

   e. In the **Decode** column, enter the name of the IT resource parameter.

   f. Click the Save icon.

   For Oracle Identity Manager 11.1.2.1.0 or later:

   a. Log in to Oracle Identity System Administration.

   b. In the left pane, under System Configuration, click **Lookups**.
   Search for and open the Lookup.SAP.HRMS.ITResourceMapping lookup definition.

   c. Click **Edit Lookup Type**.

   d. In the Meaning column for the Code Key, enter a value.

   e. Click the Save icon.

2.3.12.2 Configuring the IT Resource

You must specify values for the parameters of the SAP HRMS IT resource as follows:

1. Depending on the Oracle Identity Manager release you are using, perform the following steps:

   For Oracle Identity Manager release 11.1.2:

   Log in to Oracle Identity System Administration.

2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - If you are using Oracle Identity Manager release 11.1.1, then:

     a. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced**.

     b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the **Configuration** region, click **Manage IT Resource**.

   - If you are using Oracle Identity Manager release 11.1.2, then:
     In the left pane under Configuration, click **IT Resource**.

- If you are using Oracle Identity Manager release 11.1.2.3.*x* or later, then:
  In the left pane under Provisioning Configuration, click **IT Resource**.

3. In the IT Resource Name field on the Manage IT Resource page, enter `SAP HRMS` and then click **Search**.
4. Click the edit icon for the IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the IT resource. Table 2-6 lists the parameters of the IT resource.

   The target system supports the following types of connections:

   - Direct connection to an SAP instance
   - Load-balancing connection to a group of SAP instances

   Some connection properties are mandatory for a specific type of connection. This is highlighted in the table.

> **Note:**
>
> As mentioned earlier, most of the IT resource parameters correspond to connection properties used by the SAP JCo. See SAP JCo Javadocs for detailed descriptions of these parameters.

Table 2-6 IT Resource Parameters

Parameter	Description
App server host	IP address of the R/3 application server host computer This parameter is mandatory for both direct and load-balancing connections.
Client logon	Client logon This parameter is mandatory for both direct and load-balancing connections. Sample value: `800`
Gateway host	Host name of the target system gateway server Typically, the gateway is installed on the same application server (central instance). However, the gateway can be installed on a separate host computer that is connected to the central instance. This parameter is mandatory for a load-balancing connection. Sample value: `examplesap08.corp.example.com`
Gateway service	Gateway service Default value: `3300`

Table 2-6 (Cont.) IT Resource Parameters

Parameter	Description
Language	Logon language This parameter is mandatory for both direct and load-balancing connections. Sample value: `EN`
Password	Logon password This parameter is mandatory for both direct and load-balancing connections.
Peak limit	Maximum number of active connections that can be created for a destination simultaneously Default value: `10`
Pool capacity	Maximum number of idle connections kept open by the destination. A value of 0 has the effect that there is no connection pooling. Default value: 3
Program ID	Program ID used in SAP to register the listener Default value: `IDOCLISTEN` This program ID must be the same as the program ID you specify when you perform the procedure to register the listener with the SAP Gateway (tRFC). **Note**: The program ID is case-sensitive. Use the same case (uppercase and lowercase) when you enter the program ID as the value of this parameter.
Repository destination	Name of the repository destination (jcoDestination) You can enter any string value as the repository destination. Default value: `BCE`
SNC lib	Path to SNC library Sample value: `C://usr/sap`
SNC mode	Specifies whether or not SNC is to be used to secure communication between Oracle Identity Manager and the target system The value is `Yes` if SNC is enabled. Otherwise, it is `No`. Other SNC values are required only if this parameter is set to Yes. This parameter is mandatory for both direct and load-balancing connections. Sample value: `No`
SNC my name	Name of the SNC system
SNC partner name	Name of the partner system, the system on which SAP is installed Default value: `p:CN=I47,OU=SAP,O=ORA, C=IN`

Table 2-6 (Cont.) IT Resource Parameters

Parameter	Description
SNC qop	This parameter controls the protection level (quality of protection, QOP) at which data is transferred. You can specify one of the following numbers as the value of this parameter: • 1: Secure authentication only • 2: Data integrity protection • 3: Data privacy protection • 8: Use value from the parameter • 9: Use maximum value available This is required only if SNC is enabled. Default value: 3
Server name	Unique name that identifies the server You can enter any string value as the server name. Default value: `Server`
System number	R/3 system number This parameter is mandatory for a direct connection. Sample value: `00`
Unicode mode	Specifies whether or not the connection with the target system must be established in Unicode mode. The value can be `Yes` or `No` Default value: `No`
User logon	This parameter is mandatory for both direct and load-balancing connections. Sample value: `remote_user`
Connection Count	Maximum number of connections that can be opened on a server Default value: 2
R3 Name	System ID of the SAP system
Group Name	Group of SAP application servers
Message Server	Host name of the message server

7. To save the values, click **Update**.

2.3.12.3 Parameters for Enabling the Use of a Logon Group

In SAP, a logon group is used as a load-sharing mechanism. When a user logs in to a logon group, the system internally routes the connection request to the logon group member with the least load.

The following parameters of the IT resource are used to enable this feature. These parameters are explained in Table 2-6.

- Group name
- Message server
- R3 name

In addition, perform the following procedure on the Oracle Identity Manager host computer to enable SAP JCo connectivity:

1. Open the following file in a text editor:
   For Microsoft Windows:

   C:\WINDOWS\system32\drivers\etc\services

   For Solaris or Linux, open the following file:

   /etc/services
2. Add an entry in the following format:

   > **Note:**
   >
   > Ensure that you add the entry in the correct ascending order of the port number as shown in the example.

   ```
   sapmsSYSTEM_ID          36SYSTEM_NUMBER/tcp
   ```

   For example:

   ```
   . . .
   ipx               213/udp                          #IPX over IP
   sapmsE60          3600/tcp
   ldap              389/tcp                          #Lightweight Directory
   Access Protocol
   . . .
   ```
3. Save and close the file.
4. Create the sapmsg.ini file and add the following lines in the file:

   ```
   [Message Server]
   o01=oss001.wdf.sap-ag.de
   SYSTEM_ID=HOST_NAME
   ```

   For example:

   ```
   [Message Server]
   o01=oss001.wdf.sap-ag.de
   E60=mysap08.corp.example.com
   ```
5. Save and close the file.
6. On the Oracle Identity Manager host computer, copy the file into the C:\Windows directory or the root directory (depending on the operating system running on the host).

2.3.13 Creating an Authorization Policy

The procedure described in this section is applicable only if you are using Oracle Identity Manager release 11.1.*x*.

On Oracle Identity Manager release 11.1.x, to create an authorization policy, see the instructions given in Managing Authorization Policies of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager*. The following instructions are specific to individual steps of the procedure described in the "Creating an Authorization Policy for User Management" section of that chapter:

- When you reach Step 3, in the Policy Name field, enter a name for the policy. For example: `Personnel Number Authorization Policy`
- When you reach Step 4, in the Description field, enter a description for the policy. For example: `Personnel Number Authorization Policy`
- When you reach Step 7:
  In the Permissions table, select the following check boxes in the Enable column:
  - Modify User Profile
  - Search User
  - View User Details

  Click **Edit Attributes**.

  On the Attribute Settings page, clear all the check boxes, select **Personnel Number**, **User created from HRMS**, and **Manager**. Then, click **Save**.

2.3.14 Displaying UDFs in Oracle Identity Manager 11.1.2 or Later

In Oracle Identity Manager release 11.1.2 or later, some of the user attributes (UDFs) such as City, Cost Center, Department, District, Group, Job Position, Org Unit, Personnel Number, Manager, SAP Linked User ID, Sub Group, User Created from HRMS are not displayed after running the SAP HRMS User Recon.

If you want to display these attributes as form fields in the Oracle Identity Manager user interface, you must customize the associated pages on the interface to add custom form fields. To do so, perform the following procedure:

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox.
3. From the Identity System Administration Console, in the Upgrade region, click **Upgrade User Form**. All the UDFs are listed.
4. Click **Upgrade**.
5. Publish the sandbox.

See Using the Archival and Purge Utilities for Controlling Data Growth in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about the PurgeCache utility.

2.4 Upgrading the Connector

You can upgrade the SAP ER connector while in production, and with no downtime. Your customizations remain intact and the upgrade will be transparent to your users. All form field names are preserved from the legacy connector.

To upgrade the SAP ER connector, perform the procedures described in the following sections:

- Prerequisites for Upgrading the Connector
- Upgrading the Connector
- Performing the Postupgrade Steps

Note:

- Before you perform the upgrade procedure, it is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to *MoS: OIM 11gR2: Schema Backup and Restoration using Data Pump Client Utility (Doc ID 1492129.1)* from OIM perspective.
- As a best practice, first perform the upgrade procedure in a test environment.

See Also:

Upgrading Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information on these steps

2.4.1 Prerequisites for Upgrading the Connector

Before you perform an upgrade operation or any of the upgrade procedures, you must perform the following actions:

- Perform a reconciliation run to fetch all latest updates to Oracle Identity Manager.
- Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector.
- Run the Oracle Identity Manager Delete JARs utility to delete the old connector bundle to the Oracle Identity Manager database.

See Also:

Delete JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for detailed information about the Delete JARs utility

2.4.2 Upgrading the Connector

This is a summary of the procedure to upgrade the connector for both staging and production environments.

Depending on the environment in which you are upgrading the connector, perform one of the following steps:

- Staging Environment

  Perform the upgrade procedure by using the wizard mode.
- Production Environment

  Perform the upgrade procedure by using the silent mode.

> **See Also:**
>
> Managing Connector Lifecycle of *Oracle Fusion Middleware Administering Oracle Identity Governance* for detailed information about the wizard and silent modes

2.4.3 Performing the Postupgrade Steps

Perform the procedure described in this section to complete the steps that are required to post-upgrade.

1. Run the Oracle Identity Manager Upload JARs utility to post the new connector bundle to the Oracle Identity Manager database.
2. From the **Advanced** menu, select **Configuration** and then select **IT Resource** and configure the IT resources created as part of this connector.
3. From the Sysadmin console menu, select **Management** and then select **Scheduled Job** and configure the jobs that are already created for the connector.
4. From the field name reference in the lookup definition (if any duplicates), processed task literals and adapters must be updated according to the old form names.

> **See Also:**
>
> Upload JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for detailed information about the Upload JARs utility

5. Upgrading the connector will generate duplicate entries in Lookups, you must manually delete these duplicate entries. Perform the postupgrade procedure documented in Managing Connector Lifecycle of *Oracle Fusion Middleware Administering Oracle Identity Manager*.

3
Using the Connector

After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

> **Note:**
>
> These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

3.1 Summary of Steps to Use the Connector

> **Note:**
>
> It is assumed that you have performed all the procedures described in the preceding chapter. In Oracle Identity Manager release 11.1.x or later, a scheduled job is an instance of a scheduled task.
> See Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

The following is a summary of the steps to use the connector:

1. Configure and run the scheduled task to synchronize the Lookup.SAP.HRMS.EmployeeType lookup definition. See Configuring the Scheduled Job for Lookup Field Synchronization for information.
2. Test full reconciliation as follows:

   See Performing Full Reconciliation for instructions.

   - Generate flat files for a few users.

- Configure and run the SAP HRMS User Recon scheduled job.
- Check if reconciliation events are created for user records in the flat file.

3. Perform first-time (full) reconciliation. See Performing Full Reconciliation for insructions.
4. Change from full reconciliation to incremental reconciliation. See Performing Incremental Reconciliation for instructions.

> **Note:**
>
> As mentioned earlier in this guide, you can switch from incremental reconciliation to full reconciliation and back to incremental reconciliation at any time. It is recommended that you perform full reconciliation at periodic intervals (for example, a few months) to fully ensure that OIM Users exist for all target system users.

3.2 Configuring the Scheduled Job for Lookup Field Synchronization

The Lookup.SAP.HRMS.EmployeeType lookup definition is used to hold mappings between combinations of Employee Group and Employee Subgroup values from the target system and employee types defined in Oracle Identity Manager.

The SAP HRMS EmployeeType Lookup Recon scheduled Job is used to fetch the Employee Group and Employee Subgroup values from the target system and populate them in the Code Key column of the Lookup.SAP.HRMS.EmployeeType lookup definition.To configure and run the SAP HRMS EmployeeType Lookup Recon scheduled task:

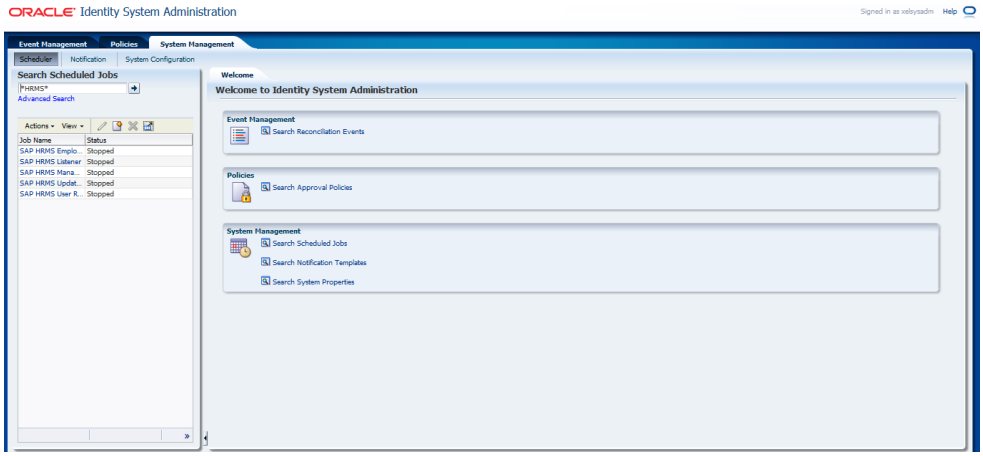
1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   For Oracle Identity Manager release 11.1.1.*x*:

   - Log in to the Administrative and User Console.
   - On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.

   For Oracle Identity Manager release 11.1.2.*x* or later, search for and open the scheduled job as follows:

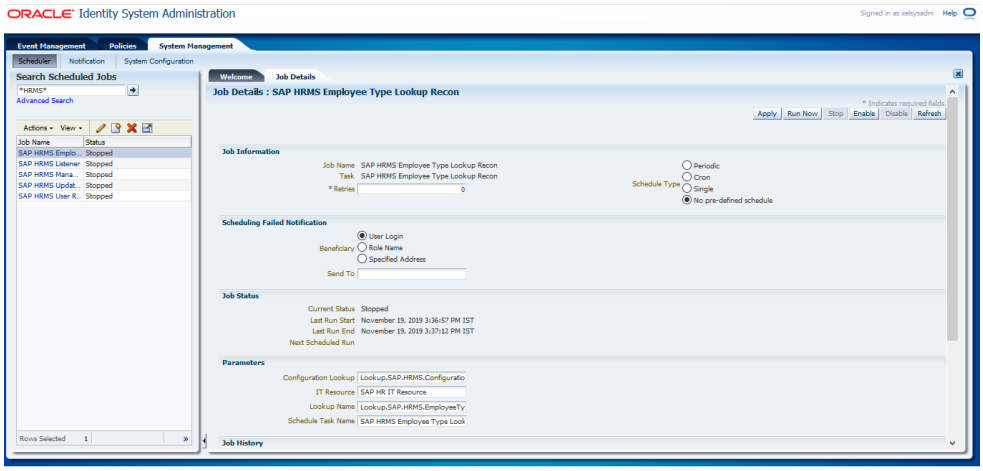
   - On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
   - On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   - In the search results table on the left pane, click the scheduled job in the Job Name column.



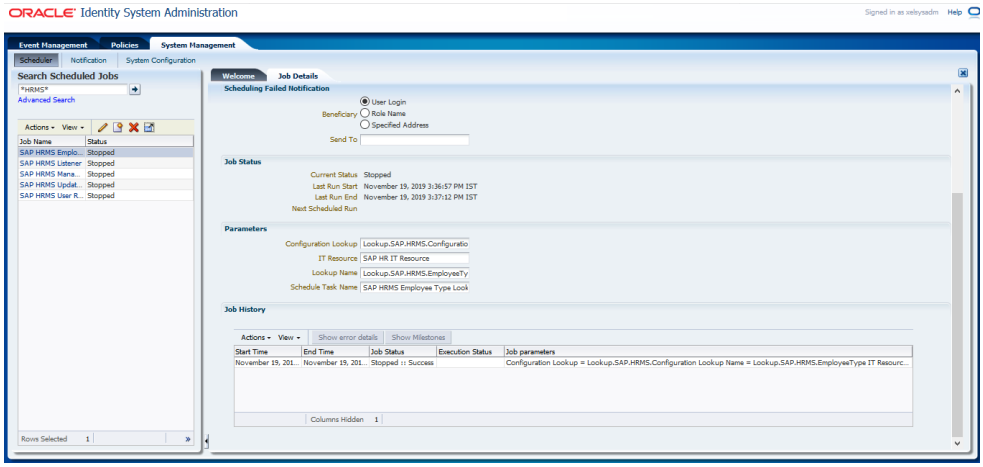
2. On the Job Details tab, you can modify the parameters of the scheduled jobs.
   - Retries: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
   - Schedule Type: Depending on the frequency at which you want the job to run, select the appropriate schedule type.

> **Note:**
>
> See Creating Jobs of *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about schedule types.

   In addition to modifying the job details, you can enable or disable a job.



3. On the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.



4. Click **Apply** to save the changes.

Table 3-1 lists the attributes of this scheduled task.

Table 3-1 Attributes of the SAP HRMS EmployeeType Lookup Recon Scheduled Task

Attribute	Description
Configuration lookup	This attribute holds the name of the lookup definition that contains configuration details. Value: `Lookup.SAP.HRMS.Configuration` **Note**: For this scheduled task, you must not change the value of this attribute. However, if you create a copy of the lookup definition, then you must enter the unique name of that lookup definition as the value of the Configuration lookup attribute. See Setting Up the Lookup.SAP.HRMS.Configuration Lookup Definition in Oracle Identity Manager for information about this lookup definition.
IT Resource	Enter the name of the IT resource that you create by performing the procedure described in the Configuring the IT Resource.
Lookup Name	Value: `Lookup.SAP.HRMS.EmployeeType` **Note**: For this scheduled task, you must not change the value of this attribute. However, if you create a copy of the lookup definition, then you must enter the unique name of that lookup definition as the value of the Lookup Name attribute.

Table 3-1 (Cont.) Attributes of the SAP HRMS EmployeeType Lookup Recon Scheduled Task

Attribute	Description
Schedule Task Name	This attribute holds the name of the scheduled task. Value: `SAP HRMS EmployeeType Lookup Recon` **Note**: For this scheduled task, you must not change the value of this attribute. However, if you create a copy of the scheduled task, then you must enter the unique name of that scheduled task as the value of the Schedule Task Name attribute in that scheduled task.

3.3 Guidelines on Performing Reconciliation

On a Microsoft Windows platform, if you encounter the org.quartz.SchedulerException exception during a reconciliation run, then download and install the Microsoft Visual C++ 2005 SP1 Redistributable Package from the Microsoft Web site.

3.4 Performing Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation.

The following section discusses the procedures involved in full reconciliation:

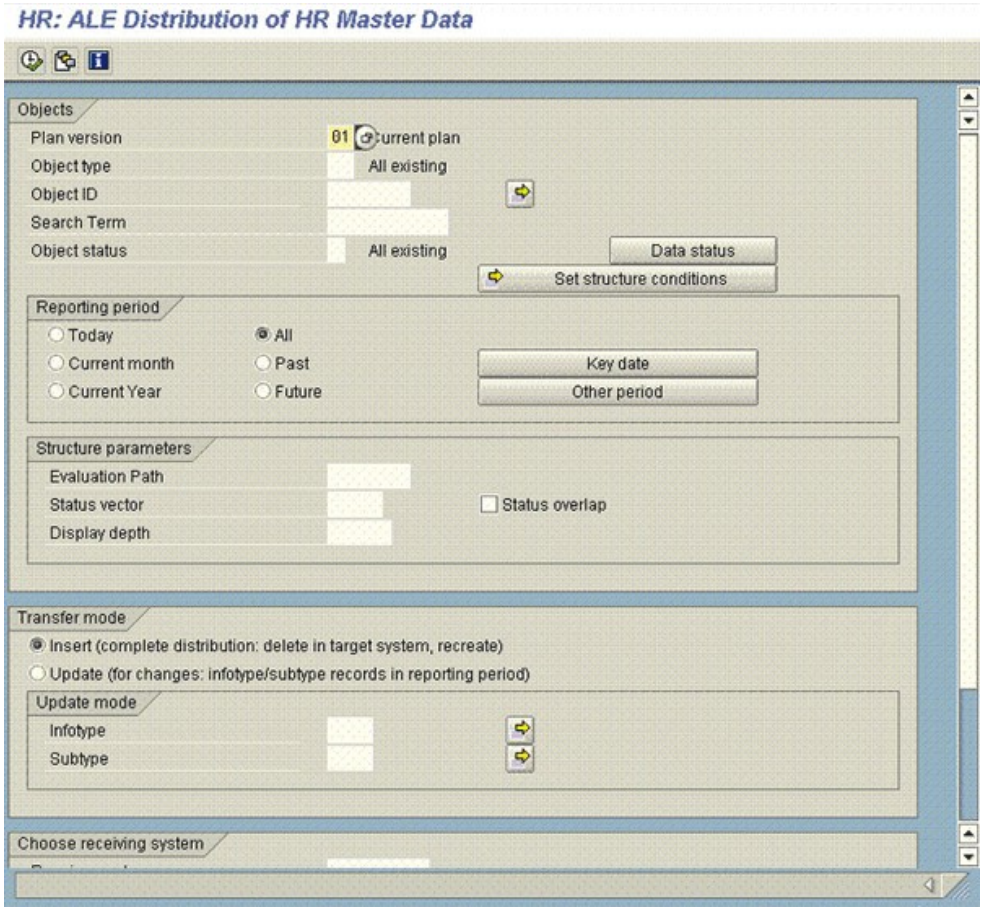
- Generating IDocs
- Importing IDocs Into Oracle Identity Manager

3.4.1 Generating IDocs

You must generate IDocs for all existing employees in the target system.

To generate IDocs for full reconciliation:

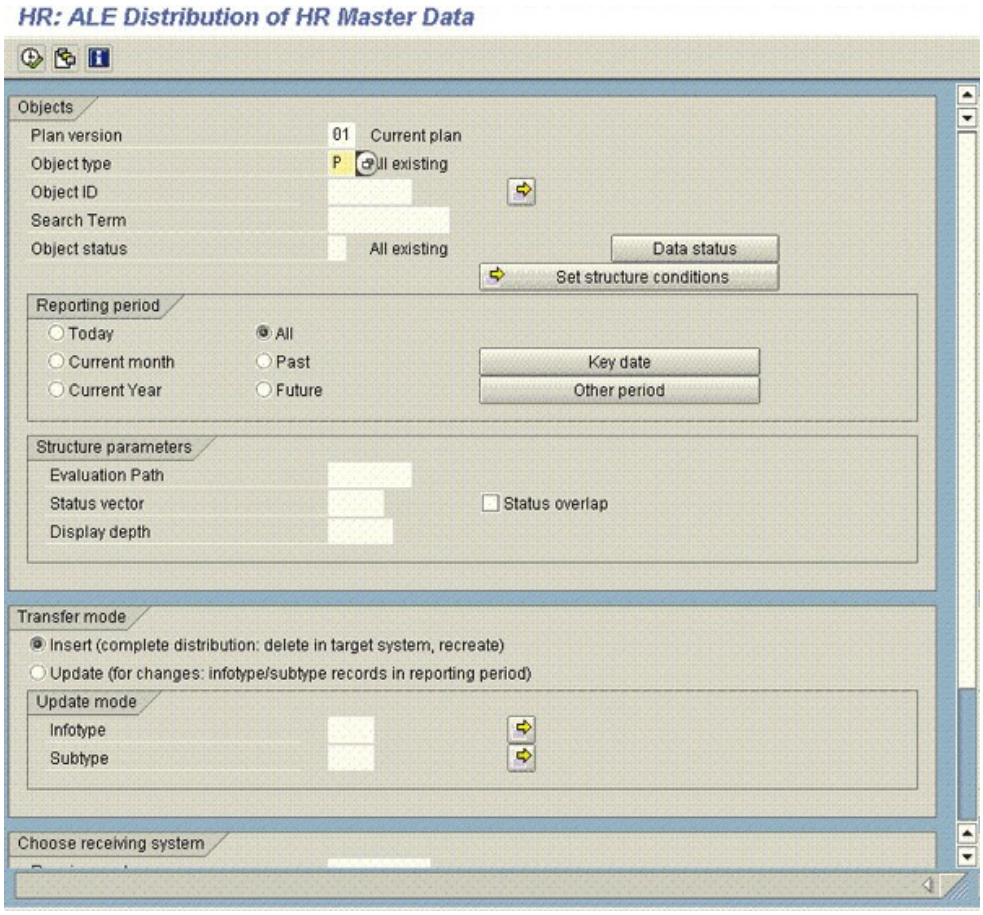
1. Run transaction PFAL.



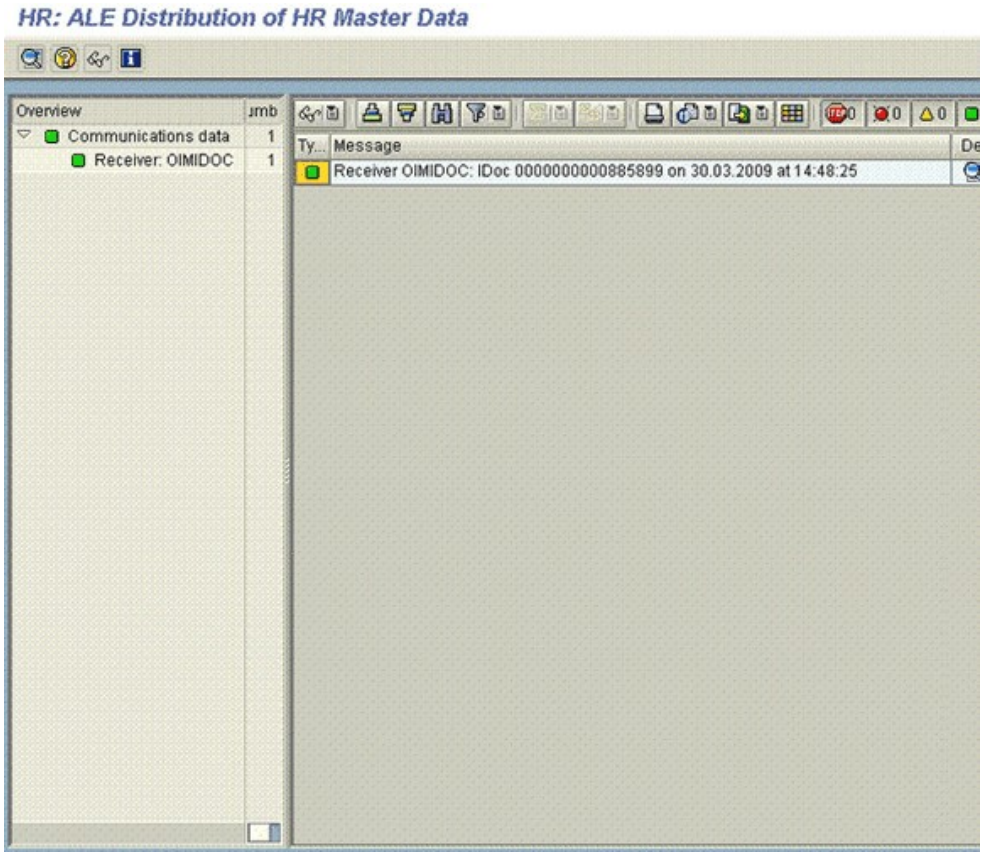
2. In the Objects region, select **P** as the object type. The value P indicates that you want IDocs to be created for person records.
3. Use the Object ID field to specify the persons for whom you want to generate IDocs. The Personnel Number attribute is of the numeric data type. If required, you can use the Object ID field to specify the range of personnel numbers of persons for whom you want to generate IDocs.

> **Note:**
>
> To specify that you want IDocs to be generated for all persons at the same time, do not enter a value in the object ID field.

4. In the Reporting period region, the **All** option is selected by default. With this option, IDocs are created for all infotypes, regardless of the end date of the infotypes. If you want IDocs to be created only for current- or future-dated infotypes, then click **Key date** and enter the date relative to which infotypes must be considered for reconciliation. IDocs are created only for infotypes that are current- or future-dated on the date that you enter. For example, if you enter `02-Dec-2009`, then IDocs are created only for infotypes having an end date that equals or is greater than 02-Dec-2009.
5. In the Number of objects per process field, enter the number of IDocs that must be recorded in one flat file. This field takes a maximum value of 200. If you do not specify a value, then a system default is used, which may be less than or equal to 200.



6. Click **Execute**.
7. Verify that the status is **Passed to Port OK**.



At this stage, flat files containing the IDocs are in the directory location that you specify in the file port definition.

8. Copy the flat files to a directory on the Oracle Identity Manager host computer.

> **Note:**
>
> In an Oracle Identity Manager cluster, copy the flat files to each node of the cluster.

3.4.2 Importing IDocs Into Oracle Identity Manager

- Limited Reconciliation discusses scheduled task attributes that you can use to customize the reconciliation process.
- Configuring the Scheduled Task for User Data Reconciliation describes the procedure to configure the scheduled task.
- Running the SAP HRMS Update Manager Scheduled Task describes the procedure to configure the scheduled task for reconciliation of Manager ID values.

3.4.2.1 Limited Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current incremental reconciliation run. For full reconciliation, all target system records are fetched into Oracle Identity Manager.

You configure segment filtering to specify the attributes whose values you want to fetch into Oracle Identity Manager. Similarly, you can configure limited reconciliation to specify the subset of target system records that must be fetched into Oracle Identity Manager.

You configure limited reconciliation by specifying a query condition as the value of the Custom Query attribute of the SAP HRMS User Recon and SAP HRMS Listener scheduled tasks.

You must use the following format to specify a value for the Custom Query attribute:

```
RESOURCE_OBJECT_ATTRIBUTE_NAME=VALUE
```

For example, suppose you specify the following as the value of the Custom Query attribute:

```
Last Name=Doe
```

With this query condition, only records for users whose last name is Doe are considered for reconciliation.

> **Note:**
>
> IDocs for the records to which the query condition is applied have already been fetched to Oracle Identity Manager. The query condition only limits records that are sent to the Reconciliation Manager.

You can add multiple query conditions by using the ampersand (&) as the AND operator and the vertical bar (|) as the OR operator. For example, the following query condition is used to limit reconciliation to records of those users whose first name is John and last name is Doe:

```
First Name=John & Last Name=Doe
```

To configure limited reconciliation:

1. Ensure that the OIM User attribute that you want to use in the query exists in the Lookup.SAP.HRMS.AttributeMapping lookup definition. This lookup definition maps OIM User form fields with target system attributes.

   See Lookup.SAP.HRMS.AttributeMapping for a listing of the default contents of this lookup definition. If there is no entry in this lookup definition for the attribute that you want to use, then create an entry. See Adding Attribute Mapping for more information.

2. Ensure that the OIM User attribute that you want to use in the query exists in the Lookup.SAP.HRMS.CustomQueryMapping lookup definition. This lookup definition maps resource object fields with OIM User form fields. It is used during application of the query condition that you create.

If there is no entry in this lookup definition for the attribute that you want to use, then create an entry.

3. Create the query condition. Apply the following guidelines when you create the query condition:

   - Use only the equal sign (=), ampersand (&), and vertical bar (|) in the query condition. Do not include any other special characters in the query condition. Any other character that is included is treated as part of the value that you specify.
   - Add a space before and after ampersand and vertical bars used in the query condition. For example:
     ```
     First Name=John & Last Name=Doe
     ```
     This is to ensure to help the system distinguish between ampersands and vertical bars used in the query and the same characters included as part of attribute values specified in the query condition.
   - You must not include unnecessary blank spaces between operators and values in the query condition.
     A query condition with spaces separating values and operators would yield different results as compared to a query condition that does not contain spaces between values and operators. For example, the output of the following query conditions would be different:
     ```
     First Name=John & Last Name=Doe
     ```
     ```
     First Name= John & Last Name= Doe
     ```
     In the second query condition, the reconciliation engine would look for first name and last name values that contain a space at the start.
   - Ensure that attribute names that you use in the query condition are in the same case (uppercase and lowercase) as the case of values in the Lookup.SAP.HRMS.AttributeMapping and Lookup.SAP.HRMS.CustomQueryMapping lookup definitions. For example, the following query condition would fail:
     fiRst Name = John

4. While configuring the SAP HRMS User Recon scheduled task, specify the query condition as the value of the Custom Query attribute. The procedure is described later in this chapter.

3.4.2.2 Configuring the Scheduled Task for User Data Reconciliation

The SAP HRMS User Recon scheduled task is used to transfer IDocs data from the file to the parser. The parser then converts this data into reconciliation events.

Table 3-2 describes the attributes of this scheduled task. See Configuring Scheduled Tasks for instructions on running the scheduled task.

> **Note:**
>
> In an Oracle Identity Manager cluster, the file is automatically deleted only from one node after the reconciliation run. You must manually delete the file from the other nodes.
> The scheduled task connects to the target system during a full reconciliation run. You must ensure that connectivity to the target system is maintained during the reconciliation run.

Table 3-2 Attributes of the SAP HRMS User Recon Scheduled Task

Attribute	Description
Attribute Mapping Lookup	Lookup.SAP.HRMS.AttributeMapping
Configuration lookup	This attribute holds the name of the lookup definition that stores configuration details. Value: `Lookup.SAP.HRMS.Configuration` **Note**: For a particular target system installation, you must not change the value of this attribute. If you create and use a copy of the configuration lookup definition for a different installation of the target system, then you must enter then name of that lookup definition as the value of this attribute.
Custom Query	If you want to implement limited reconciliation, then enter the query condition that you create by following the instructions given in Limited Reconciliation.
Custom Query Lookup	This attribute holds the name of the lookup definition that maps resource object fields with OIM User form fields. This lookup definition is used during application of the custom query. See Limited Reconciliation for more information. Default Value: `Lookup.SAP.HRMS.CustomQueryMapping`

Table 3-2 (Cont.) Attributes of the SAP HRMS User Recon Scheduled Task

Attribute	Description
Employee Type Query	Use this attribute to specify the combination of employee group and subgroup for which you want fetch users for reconciliation. You can use the following target system attributes to specify a value for the Employee Type Query attribute: • PERSG: This is the Employee Group attribute on the target system. In the Lookup.SAP.HRMS.Configuration lookup definition, this attribute is represented as follows: `E2P0001001;PERSG;146;146` • PERSK: This is the Employee Subgroup attribute on the target system. In the Lookup.SAP.HRMS.Configuration lookup definition, this attribute is represented as follows: `E2P0001001;PERSK;147;148` The following is a sample value for the Employee Type Query attribute: `Group=1 & SubGroup=DU` When this employee type query is applied during reconciliation, only user records belonging to employee group 1 and subgroup `DU` are fetched for reconciliation. **Note**: The guidelines for creating the employee type query are the same as those described inLimited Reconciliation
File Archival	Enter `yes` if you want flat files used during full reconciliation to be archived. Enter `no` if you want the flat files to be deleted after data inside the files is reconciled.
File Archival Folder	Enter the full path and name of the directory in which you want flat files used during full reconciliation to be archived. You must enter a value for the File Archival Folder attribute only if you specify `yes` as the value for the File Archival attribute.
IDoc Folder Path	Enter the path of the directory on the Oracle Identity Manager host computer into which you copy the file containing IDocs data. Sample value: `/usr/idocs_data`
IT resource	Enter the name of the IT resource that you create by performing the procedure described in Configuring the IT Resource section. Default value: `SAP HRMS IT Resource`
Resource Object	This attribute holds the name of the resource object. Default value: `SAP HRMS Resource Object`

Table 3-2 (Cont.) Attributes of the SAP HRMS User Recon Scheduled Task

Attribute	Description
Schedule Task Name	This attribute holds the name of the scheduled task. Value: `SAP HRMS User Recon` **Note**: For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that new reconciliation scheduled task as the value of the Schedule Task Name attribute in the copy of this scheduled task.

3.4.2.3 Running the SAP HRMS Update Manager Scheduled Task

Manager ID values might not be reconciled for some users at the end of a full reconciliation run. The following scenario illustrates this condition:

During a reconciliation run, suppose Mark's record was brought to Oracle Identity Manager before the record of Mark's manager. When this happens, the Manager ID attribute in Mark's record will remain empty.

In addition, when the manager of an organization is replaced by another manager, the change in Manager ID values is not automatically propagated to OIM User records of users who belong to that organization.

If you come across either of these issues, then you must configure and run the SAP HRMS Update Manager scheduled task.

Before you run this scheduled task, you must specify a value for the "Update users with empty manager id only" attribute:

- Enter `yes` if you want the scheduled task to populate Manager ID values in OIM User records that do not have this value. Existing Manager ID values in other OIM User records are not modified.
- Enter `no` if you want the scheduled task to fetch and populate Manager ID values for all OIM User records, regardless of whether the Manager ID attribute in these records currently contains a value.

> **Note:**
>
> You must ensure that the Lookup.SAP.HRMS.OrgHierarchy and Lookup.SAP.HRMS.OrgManager lookup definitions are updated before you run this scheduled task.

When it is run, this scheduled task performs the process described in Reconciliation of the Manager ID Attribute.

3.5 Performing Incremental Reconciliation

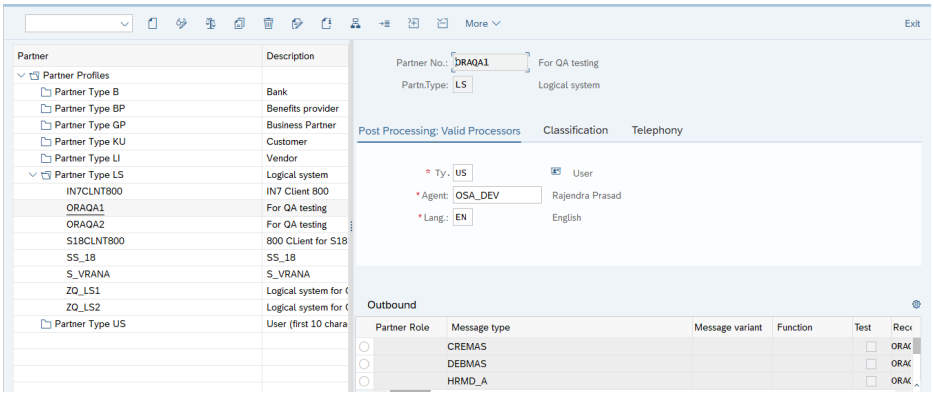
Performing incremental reconciliation involves the following tasks:

- Specifying the Mode of Reconciliation in the Partner Profile
- Scheduling Jobs on the Target System for Incremental Reconciliation
- Configuring the Listener on Oracle Identity Manager
- Configuring Incremental Reconciliation of Manager ID Attribute Values

3.5.1 Specifying the Mode of Reconciliation in the Partner Profile

To change from full reconciliation to incremental reconciliation or from incremental reconciliation to full reconciliation:

1. Run transaction WE20.
2. Expand Partner Profiles, select Partner Type LS, and then double-click the partner profile that you created by performing the procedure described in Defining the Partner Profile.
   - In the Outbound Parameters table, double-click **HRMD_A** in the Message Type column.

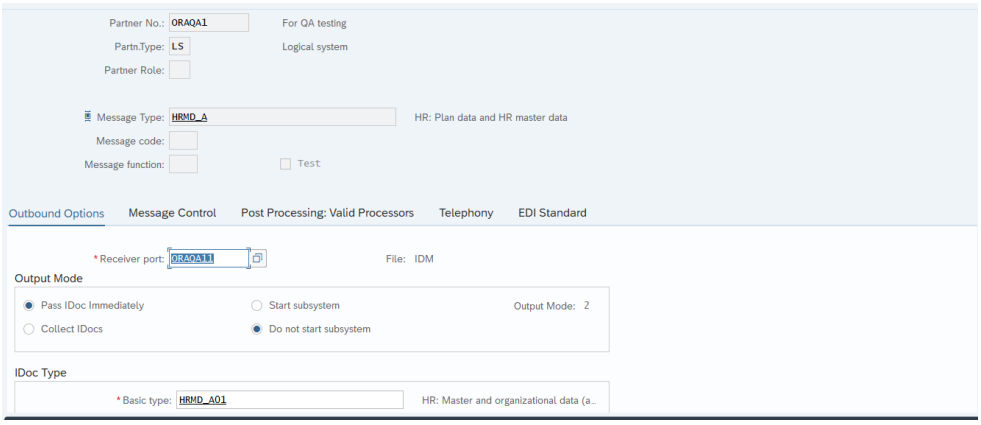


   - On the Outbound Options tab:
     - In the Receiver port:
       * For incremental reconciliation, select the tRFC port that you define by performing the procedure described in Creating the tRFC Port.

       * For full reconciliation, select the file port that you define by performing the procedure described in Creating the File Port

       .
     - In the Output Mode region, select one of the following options:
       * For incremental reconciliation, select either the Transfer IDocs immediately or the Collect IDocs option.

       * For full reconciliation, select the Collect IDocs option.



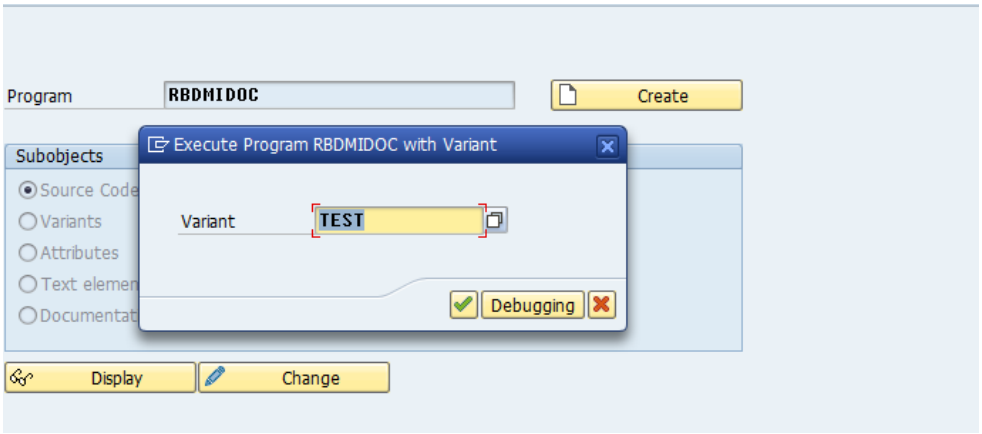
3. Click the Save icon.

3.5.2 Scheduling Jobs on the Target System for Incremental Reconciliation

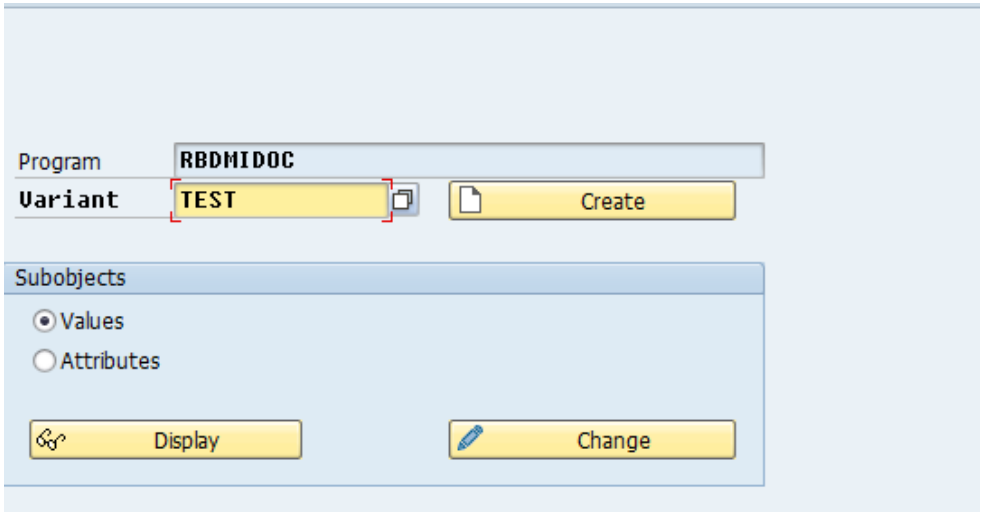
While configuring the partner profile for incremental reconciliation, you can specify that you want IDocs to be created out of change docs at two-hour intervals. Alternatively, you can select the Collect IDocs option that lets you schedule a job to create IDocs out of change docs at specified time intervals.

Regardless of the option you select in the partner profile, you must schedule a job to generate IDocs:

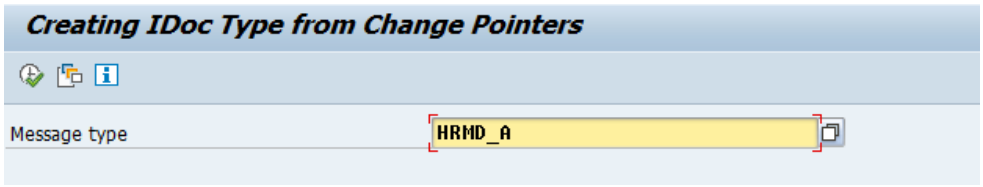
1. Run transaction SE38.
2. Select the RBDMIDOC program, select the **Variants** option, and then click the Variants icon on the toolbar.



3. Select a variant, and then click **Create**.



4. In the Message type field, enter `HRMD_A`, and then click **Attributes**.
5. Select the **Only for background processing** check box.



6. Click the Save icon.
7. Run transaction SM36.
8. Specify values for the following fields:
   - Job name: Enter a name for the job.
   - Job class: Specify a priority for the job.

   Job class is the priority in which jobs are processed. Class A is the highest priority
9. Click the **Start** condition button on the toolbar.
10. In the Start Time dialog box, click **Date/Time**, and enter the required details.
11. Click the **Step** button on the toolbar.
12. In the Create Step 1 dialog box, enter `RBDMIDOC` as the program name and then enter the name of the variant that you specified in Step 3 of this procedure.
13. Click the Save icon.

    Whether or not you must schedule a job to publish IDocs depends on the option that you select for IDocs transfer while creating the partner profile:

    - If you select the Transfer IDocs immediately option, then IDocs are transferred to the tRFC port as soon as they are created by the job built around the RBDMIDOC program.
    - If you select the Collect IDocs option in the partner profile, then schedule a job to publish IDocs by perform the procedure given in this section. While performing Steps 2 and 12 of the procedure, specify `RSEOUT00` as the program name instead of the `RBDMIDOC` program.

3.5.3 Configuring the Listener on Oracle Identity Manager

The SAP HRMS Listener scheduled task is used to transfer IDocs data from the Java object to the parser. Depending on the Oracle Identity Manager version that you are using, the following actions are performed:

Oracle Identity Manager release 11.1.*x* or later:

The parser converts IDocs data into reconciliation events. These reconciliation events have the Events Received status only and are not forwarded to the reconciliation manager for linking until the SAP HRMS Listener scheduled task is completed. Therefore, to link these reconciliation events to an OIM User while the SAP HRMS Listener scheduled task is running, you must run the Non Scheduled Batch Recon scheduled task.

Configuring the Listener on Oracle Identity Manager describes the attributes of this scheduled task.

Table 3-3 Attributes of the SAP HRMS Listener Scheduled Task

Attribute	Description
Attribute Mapping Lookup	Lookup.SAP.HRMS.AttributeMapping
Configuration lookup	This attribute holds the name of the lookup definition that stores configuration details. Value: `Lookup.SAP.HRMS.Configuration` **Note**: For a particular target system installation, you must not change the value of this attribute. If you create and use a copy of the configuration lookup definition for a different installation of the target system, then you must enter then name of that lookup definition as the value of this attribute.
Custom Query	If you want to implement limited reconciliation, then enter the query condition that you create by following the instructions given in Limited Reconciliation.
Custom Query Lookup	This attribute holds the name of the lookup definition that maps resource object fields with OIM User form fields. This lookup definition is used during application of the custom query. See Limited Reconciliation for more information. Default Value: `Lookup.SAP.HRMS.CustomQueryMapping`

Table 3-3 (Cont.) Attributes of the SAP HRMS Listener Scheduled Task

Attribute	Description
Employee Type Query	Use this attribute to specify the combination of employee group and subgroup for which you want fetch users for reconciliation. You can use the following target system attributes to specify a value for the Employee Type Query attribute: • PERSG: This is the Employee Group attribute on the target system. In the Lookup.SAP.HRMS.Configuration lookup definition, this attribute is represented as follows: `E2P0001001;PERSG;146;146` • PERSK: This is the Employee Subgroup attribute on the target system. In the Lookup.SAP.HRMS.Configuration lookup definition, this attribute is represented as follows: `E2P0001001;PERSK;147;148` The following is a sample value for the Employee Type Query attribute: `Group=1 & SubGroup=DU` When this employee type query is applied during reconciliation, only user records belonging to employee group 1 and subgroup `DU` are fetched for reconciliation. **Note**: The guidelines for creating the employee type query are the same as those described inLimited Reconciliation
IT resource	Enter the name of the IT resource that you create by performing the procedure described in Configuring the IT Resource section. Default value: `SAP HRMS IT Resource`
Resource Object	This attribute holds the name of the resource object. Default value: `SAP HRMS Resource Object`
Schedule Task Name	This attribute holds the name of the scheduled task. Value: `SAP HRMS Listener` **Note**: For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that new reconciliation scheduled task as the value of the Schedule Task Name attribute in the copy of this scheduled task.

3.5.4 Configuring Incremental Reconciliation of Manager ID Attribute Values

Manager ID values are reconciled when you run the SAP HRMS Update Manager scheduled task. Configure this scheduled task to run at periodic intervals and fetch manager ID values for OIM Users created through reconciliation.

While configuring this scheduled task, enter `no` as the value of the "Update users with empty manager id only" attribute. With this value, the scheduled task fetches and populates Manager ID values for all OIM User records, regardless of whether the Manager ID attribute in these records already contains a value.

You set the value of this attribute to `yes` while performing the procedure described in Running the SAP HRMS Update Manager Scheduled Task .

3.6 Resending IDocs That Are Not Received by the Listener

As mentioned earlier in this guide, IDocs are generated and sent to Oracle Identity Manager regardless of whether or not the listener is running.

Reconciliation events are not created for the IDocs that are sent to Oracle Identity Manager while the listener is unavailable. To ensure that all IDocs generated on the target system reach Oracle Identity Manager, perform the following procedures:

- Configuring the Target System to Resend IDocs
- Manually Sending IDocs

3.6.1 Configuring the Target System to Resend IDocs

To configure the target system for resending IDocs:

1. Run transaction SM59.
2. Select **RFC Destinations**, and then select **TCP/IP Connections**.
3. Double-click the tRFC port that you defined earlier.
4. Select the **Destination** and **tRFC** options.
5. Specify values for the following variables:
   - Connection attempts up to task: Enter the number of attempts to be made to retry sending the iDoc.
   - Time between 2 tries (mins).

3.6.2 Manually Sending IDocs

After an IDoc is sent to the tRFC port, its status is set to "03 Data transfer to port OK," regardless of whether or not the listener was available when the IDoc was sent.

1. Ensure that the listener is available.

   To check the listener program:

   - Run transaction SMGW.

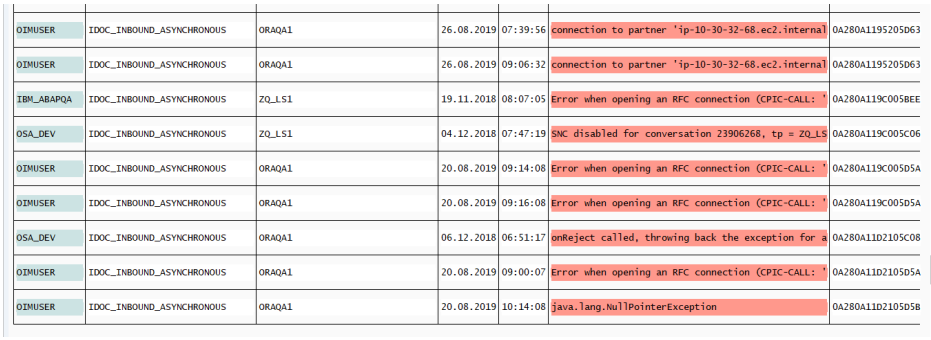
- From the GOTO menu, select **Logged on Clients**.
  Oracle Identity Manager should be displayed in the list of logged on clients.
- To confirm that the listener program is running on the Oracle Identity Manager side, verify that EFP_LIST is displayed in the TP Name column.

2. Run transaction BD75.

   This transaction changes the status of all IDocs received by the listener to "12 Sent OK." After this transaction is run, the IDocs that are still at status "03 Data transfer to port OK" are the ones that were not received by the listener.

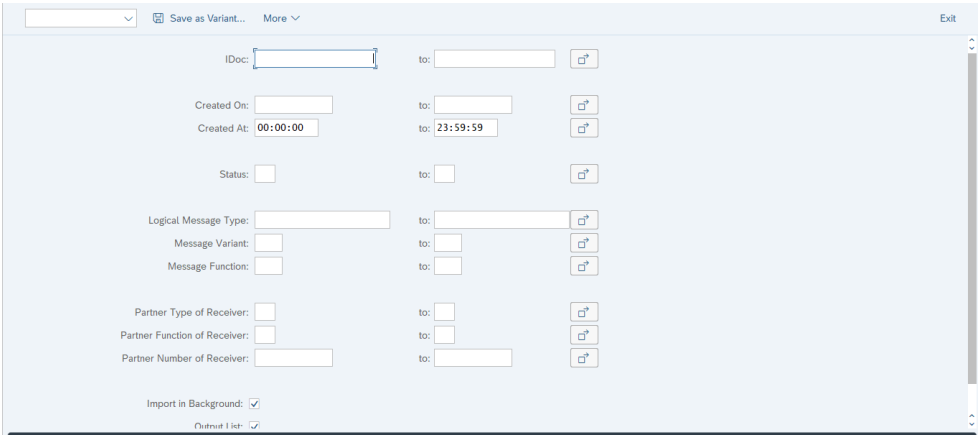
3. To resend IDocs that are at status "03 Data transfer to port OK," use one of the following approaches:

   - Run transaction SM58 for IDocs sent within the given date range. Status text is highlighted in red font for all IDocs that do not reach the listener. To resend each of these IDocs, click the IDoc and press F6.



OIMUSER	IDOC_INBOUND_ASYNCHRONOUS	ORAQA1	26.08.2019	07:39:56	connection to partner 'ip-10-30-32-68.ec2.internal	0A280A1195205D63
OIMUSER	IDOC_INBOUND_ASYNCHRONOUS	ORAQA1	26.08.2019	09:06:32	connection to partner 'ip-10-30-32-68.ec2.internal	0A280A1195205D63
IBM_ABAPQA	IDOC_INBOUND_ASYNCHRONOUS	ZQ_LS1	19.11.2018	08:07:05	Error when opening an RFC connection (CPIC-CALL: '	0A280A119C005BEE
OSA_DEV	IDOC_INBOUND_ASYNCHRONOUS	ZQ_LS1	04.12.2018	07:47:19	SNC disabled for conversation 23906268, tp = ZQ_LS	0A280A119C005C06
OIMUSER	IDOC_INBOUND_ASYNCHRONOUS	ORAQA1	20.08.2019	09:14:08	Error when opening an RFC connection (CPIC-CALL: '	0A280A119C005D5A
OIMUSER	IDOC_INBOUND_ASYNCHRONOUS	ORAQA1	20.08.2019	09:16:08	Error when opening an RFC connection (CPIC-CALL: '	0A280A119C005D5A
OSA_DEV	IDOC_INBOUND_ASYNCHRONOUS	ORAQA1	06.12.2018	06:51:17	onReject called, throwing back the exception for a	0A280A11D2105C08
OIMUSER	IDOC_INBOUND_ASYNCHRONOUS	ORAQA1	20.08.2019	09:00:07	Error when opening an RFC connection (CPIC-CALL: '	0A280A11D2105D5A
OIMUSER	IDOC_INBOUND_ASYNCHRONOUS	ORAQA1	20.08.2019	10:14:08	java.lang.NullPointerException	0A280A11D2105D5B

   - Specify a value for the date range parameter of the RBDAGAIN ABAP program, and then run the program.



3.7 Configuring Scheduled Tasks

This section describes the procedure to configure scheduled tasks. You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

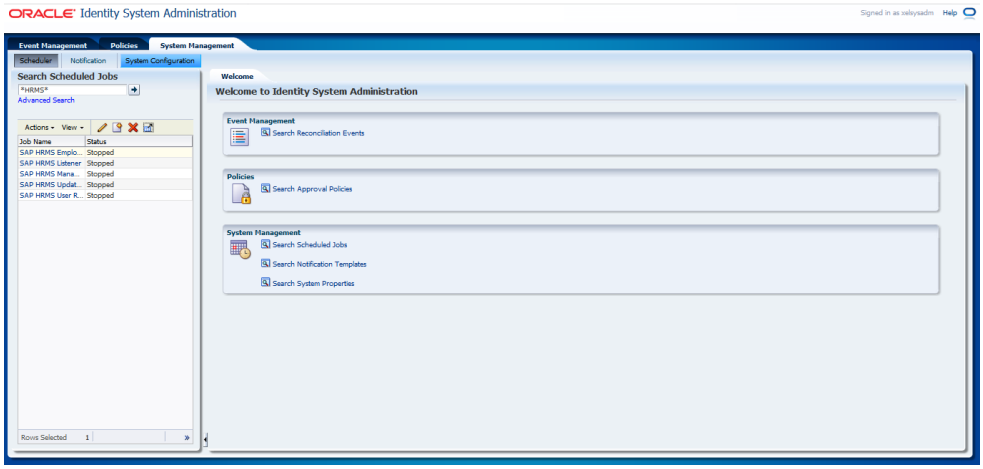
lists the scheduled tasks that you must configure.

Table 3-4 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
SAP HRMS EmployeeType Lookup Recon	This scheduled task is used to fetch values of the Employee Group and Employee Subgroup attributes from the target system and populate them in the Code Key column of the Lookup.SAP.HRMS.EmployeeType lookup definition. See Lookup.SAP.HRMS.EmployeeType for more information.
SAP HRMS User Recon	This scheduled task is used during full reconciliation. It parses the contents of the flat files containing IDocs and then creates reconciliation events for each record.
SAP HRMS Listener	This scheduled task is used during incremental reconciliation. It parses the contents of the IDocs received at the tRFC port and then creates reconciliation events for each record.
SAP HRMS Update Manager	See Running the SAP HRMS Update Manager Scheduled Task for information about this scheduled task.

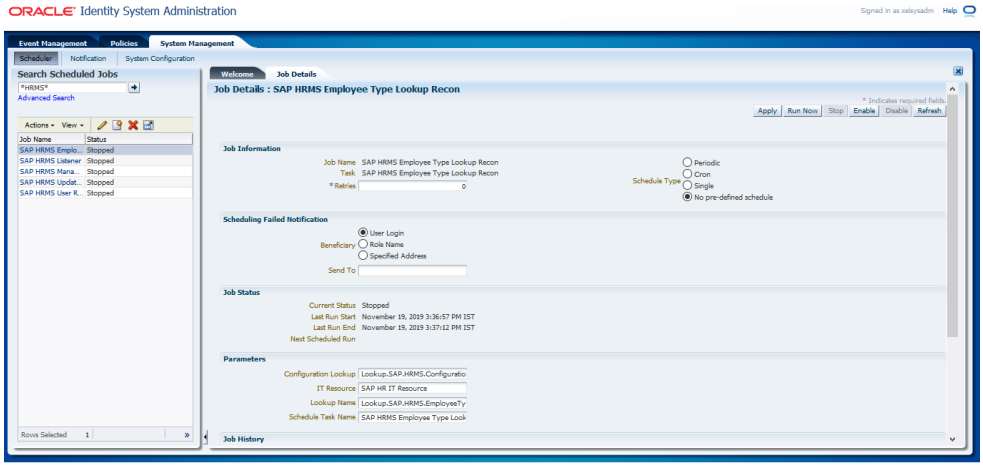
To configure a scheduled task:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1:
     a. Log in to the Administrative and User Console.
     b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
   - For Oracle Identity Manager release 11.1.2 or later:
     a. Log in to Oracle Identity System Administration.
     b. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see Managing Sandboxes in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
     c. In the left pane, under System Management, click **Scheduler**.
2. If you are using Oracle Identity Manager release 11.1.1, then perform the following steps:
   a. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced**.
   b. Click the **System Management** tab, and then click **Scheduler**.
   c. On the left pane, click **Advanced Search**.



3. On the page that is displayed, enter the name of the scheduled task as the search criteria and then click **Search**.

   The list of scheduled tasks that match your search criteria is displayed in the search results table.



4. If you are using Oracle Identity Manager release 11.1.*x*, select the link for the scheduled task from the list of scheduled tasks displayed in the search results table.

5. Modify the details of the scheduled task. To do so:

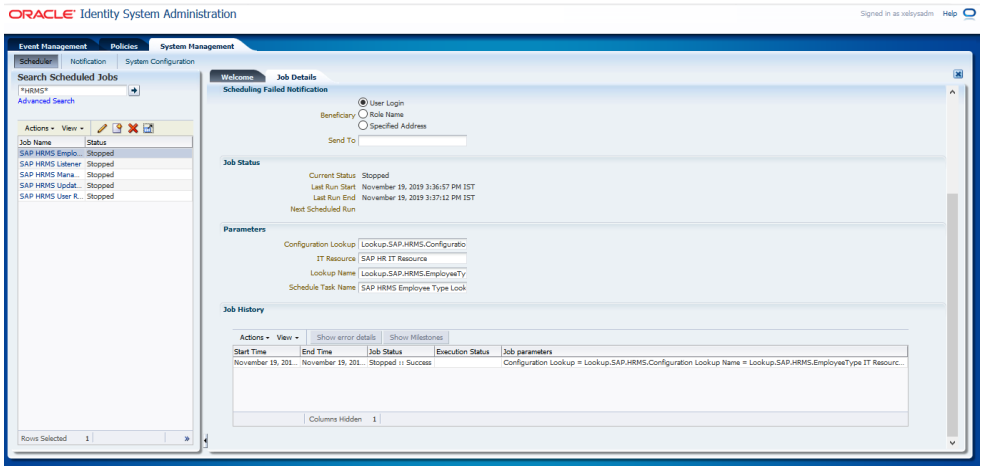
   If you are using Oracle Identity Manager release 11.1.*x*, then on the Job Details tab, you can modify the following parameters:

   - **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
   - **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type.

> **Note:**
>
> See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about schedule types.

6. Specify values for the attributes of the scheduled task. To do so:

   If you are using Oracle Identity Manager release 11.1.*x*, then on the Job Details tab, under the Parameters section, specify values for the attributes of the scheduled task.



> **Note:**
>
> Attribute values are predefined in the connector XML file that is imported during the installation of the connector. Specify values only for the attributes that you want to change.

7. After specifying the attributes, perform one of the following steps:

   If you are using Oracle Identity Manager release 11.1.*x*, then click Apply to save the changes.

> **Note:**
>
> The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

3.8 Uninstalling the Connector

If you want to uninstall the connector for any reason, see Uninstalling Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4

Extending the Functionality of the Connector

You can extend the functionality of the connector to address your specific business requirements.

This chapter discusses the following optional procedures:

- See Removing or Adding Attributes for Reconciliation if you want to modify the default field mappings between Oracle Identity Manager and the target system.
- See Modifying Field Lengths on the OIM User Form if you want to modify lengths of fields on the process form.
- Configuring the Connector for Multiple Installations of the Target System describes the procedure to configure the connector for multiple installations of the target system.
- See Configuring Validation of Data During Reconciliation if you want to configure validation of reconciled data.
- See Configuring Transformation of Data During User Reconciliation if you want configure transformation of reconciled data.

4.1 Removing or Adding Attributes for Reconciliation

The Lookup.SAP.HRMS.AttributeMapping lookup definition holds the default attribute mappings.

Table 1-5 lists the default attribute mappings stored in this lookup definition. If required, you can modify or add to this predefined set of attribute mappings. This section discusses the following procedures:

- Removing Attributes
- Adding Attribute Mapping

4.1.1 Removing Attributes

Before you begin connector operations, you can remove any attribute that is not marked as a mandatory attribute in Table 1-5.

> **Note:**
>
> If required, you can also reconfigure segment filtering to exclude the segment containing the attribute that you remove. See Configuring Segment Filtering for instructions.

To remove an attribute mapping:

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **Lookup Definition**.
3. Search for and open the **Lookup.SAP.HRMS.AttributeMapping** lookup definition.
4. Click the row that you want to delete.
5. Click **Delete**.
6. Click the Save icon.

4.1.2 Adding Attribute Mapping

To add an attribute mapping:

> **Note:**
>
> The names of attributes are case-sensitive. The spelling and case (uppercase and lowercase) of an attribute must be the same in all the connector objects. See existing attribute mappings for examples.

1. Determine the Decode column entry for the attribute that you want to add from the target system.
2. Add the attribute mapping in the Lookup.SAP.HRMS.AttributeMapping lookup definition as follows:

   For Oracle Identity Manager prior to 11.1.2.1.x or later:

   a. Log in to the Design Console.
   b. Expand **Administration**, and double-click **Lookup Definition**.
   c. Search for and open the **Lookup.SAP.HRMS.AttributeMapping** lookup definition.
   d. Click **Add**.
   An empty row is added.
   e. In the Code Key column of the new row, add the name of the OIM User attribute.
   f. In the Decode column of the new row, add the entry that you determine for the target system attribute by performing Step 1.
   The Decode column entry for an attribute is in the following format:

   ```
   SEGMENT_NAME;SUB_TYPE;SAP_ATTRIBUTE_NAME;START_POSITION;END_POSITION;
   [Text|Date]
   ```

   > **Note:**
   >
   > Append `Date` at the end of the Decode value if the attribute holds date values. For all other data types, append `Text` at the end of the Decode value.

g. Click the Save icon.

For Oracle Identity Manager 11.1.2.1.0 or later:

a. Log in to Oracle Identity System Administration.

b. In the left pane, under System Configuration, click **Lookups**.

c. Search for and open the Lookup.SAP.HRMS.AttributeMapping lookup definition.

d. Click **Edit Lookup Type** and then **Action Create Lookup Type**.
A row is added.

e. In the Code Key column of the new row, add the name of the OIM User attribute.

3. Create a UDF for the field.

4. Add the new attribute to the list of reconciliation fields in the resource object as follows:

a. Expand **Resource Management**, and double-click **Resource Objects**.

b. Search for and open the **SAP HRMS** resource object.

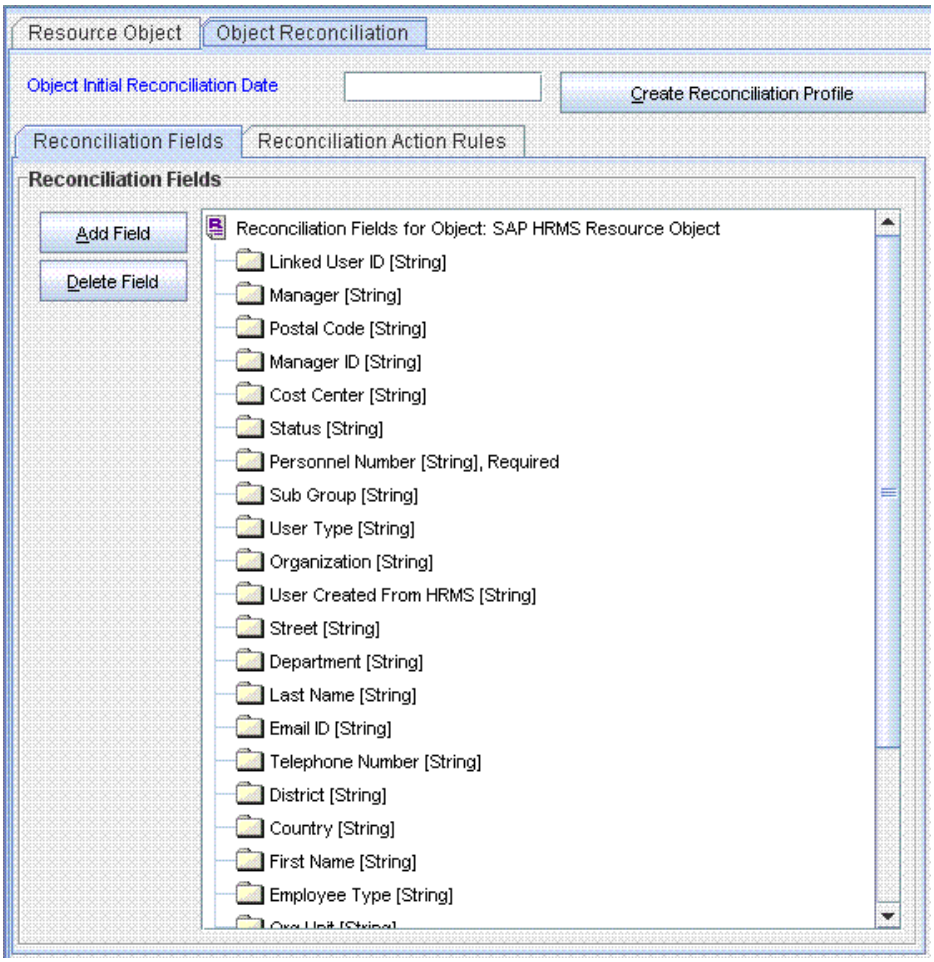
c. On the Object Reconciliation tab, click **Add Field**.

d. Enter the details of the field.
For example, enter the new attribute name in the **Field Name** field and select **String** from the Field Type list.

Later in this procedure, you will enter the field name as the Code value of the entry that you create in the lookup definition for reconciliation.

e. Click the Save icon. The following screenshot shows the new reconciliation field added to the resource object:

Figure 4-1 New reconciliation field added to the resource object



f. If you are using Oracle Identity Manager release 11.1.*x*, then click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.

5. Create a reconciliation field mapping for the new attribute in the process definition as follows:

   a. Expand **Process Management**, and double-click **Process Definition**.

   b. Search for and open the **SAP HRMS Trusted User** process definition.

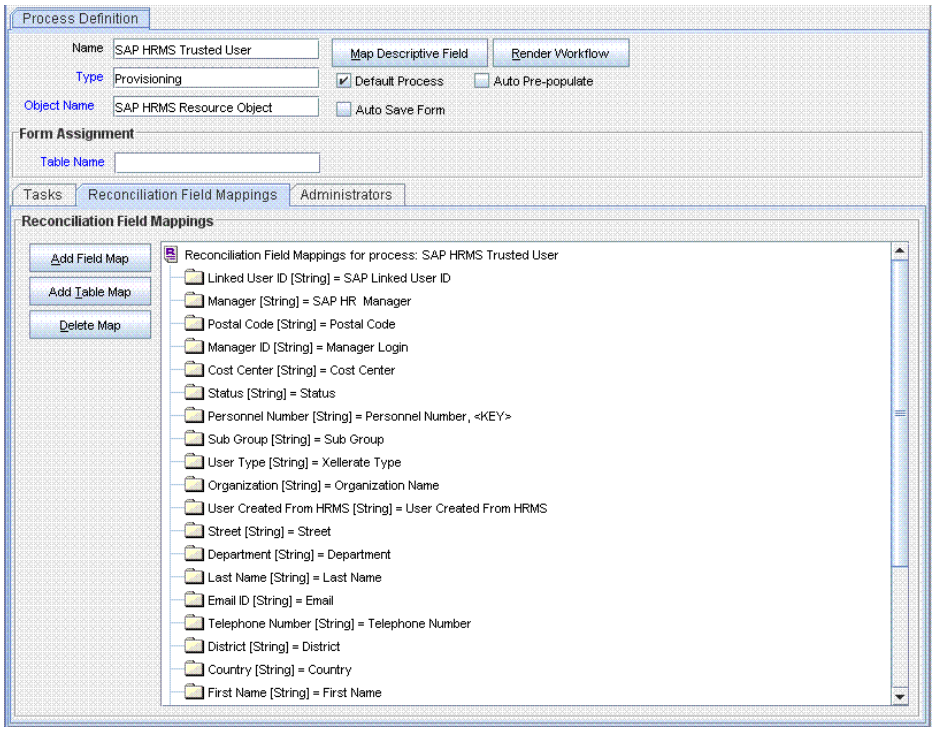
   c. On the **Reconciliation Field Mappings** tab of the **SAP HRMS Trusted User** process definition, click **Add Field Map**.

   d. In the Field Name field, select the value for the field that you want to add.

   e. Double-click the **Process Data Field** field, and then select the UDF added in Step 3.

   f. Click the Save icon. The following screenshot shows the new reconciliation field mapped to a process data field in the process definition:

Figure 4-2 New reconciliation field mapped to a process data field



6. On the target system, add the attribute to the segment filter that you create by performing the procedure described in Configuring Segment Filtering.

4.2 Modifying Field Lengths on the OIM User Form

You might want to modify the lengths of fields (attributes) on the OIM User form. For example, if you use the Japanese locale, then you might want to increase the lengths of OIM User form fields to accommodate multibyte data from the target system.

> **Note:**
>
> On mySAP ERP 2005 (ECC 6.0 running on WAS 7.0), the default length of the password field is 40 characters. The default length of the password field on the process form is 8 characters. If you are using mySAP ERP 2005, then you must increase the length of the password field on the OIM User form.

To modify the length of a field on the OIM User form, do the following:

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **User Defined Field Definition**.
3. Search for and open the **Users** form.
4. Modify the length of the required field.
5. Click the Save icon.

For Oracle Identity Manager 11.1.2.1.0 or later:

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox.
3. In the left pane, under System Entities, click **User.**
4. Modify the length of the required field.
5. Click the Save icon.

4.3 Configuring the Connector for Multiple Installations of the Target System

You might want to configure the connector for multiple installations of the target system. The following example illustrates this requirement:

The London and New York offices of Example Multinational Inc. have their own installations of the target system. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

To meet the requirement posed by such a scenario, you can create copies of connector objects, such as the IT resource and resource object.

The decision to create a copy of a connector object might be based on a requirement. For example, an IT resource can hold connection information for one target system installation. Therefore, it is mandatory to create a copy of the IT resource for each target system installation.

With some other connector objects, you do not need to create copies at all. For example, a single attribute-mapping lookup definition can be used for all installations of the target system.

All connector objects are linked. For example, a scheduled task holds the name of the IT resource. Similarly, the IT resource holds the name of the configuration lookup definition, Lookup.SAP.HRMS.Configuration. If you create a copy of an object, then you must specify the name of the copy in associated connector objects. Table 4-1 lists associations between connector objects whose copies can be created and the other objects that reference these objects. When you create a copy of a connector object, use this information to change the associations of that object with other objects.

> **Note:**
>
> On a particular Oracle Identity Manager installation, if you create a copy of a connector object, then you must set a unique name for it.

Table 4-1 Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
IT Resource	SAP HR IT Resource	SAP HRMS Employee Type Lookup Recon (scheduled task) SAP HRMS Manager Lookup Recon (scheduled task) SAP HRMS User Recon (scheduled task) SAP HRMS Listener (scheduled task)	Create a copy of the IT resource.
Resource object	SAP HRMS Resource Object	SAP HRMS Update Manager (scheduled task) SAP HRMS User Recon (scheduled task) SAP HRMS Listener (scheduled task)	Create copies of the resource object only if there are differences in attributes between the various installations of the target system and if the same user ID exists in different target systems.
Process Definition	SAP HRMS Trusted User	NA	Create copies of this process definition only if there are differences in attributes between the various installations of the target system and if the same user ID exists in different target systems.
Attribute mapping lookup definition	Lookup.SAP.HRMS.AttributeMapping	NA	Create copies of this lookup definition only if you want to use a different set of configuration values for the various installations of the target system.

Table 4-1 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Configuration lookup definition	Lookup.SAP.HRMS.Configuration	SAP HRMS Update Manager (scheduled task) SAP HRMS Employee Type Lookup Recon (scheduled task) SAP HRMS User Recon (scheduled task) SAP HRMS Manager Lookup Recon (scheduled task) SAP HRMS Listener (scheduled task)	Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.

When you configure reconciliation:

To reconcile data from a particular target system installation, specify the name of the IT resource for that target system installation as the value of the scheduled task attribute that holds the IT resource name. For example, you enter the name of the IT resource as the value of the IT resource attribute of the SAP HRMS User Recon scheduled task.

When you perform provisioning operations:

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the target system installation to which you want to provision the user.

4.4 Configuring Validation of Data During Reconciliation

You can configure validation of reconciled single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#).

For data that fails the validation check, the following message is displayed or recorded in the log file:

```
Value returned for field FIELD_NAME is false
```

.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

   This validation class must implement the oracle.iam.connectors.common.validate.Validator interface and the validate method.

> **See Also:**
>
> The Javadocs shipped with the connector for more information about this interface

The following sample validation class checks if the value in the First Name attribute contains the number sign (#):

```
public boolean validate(HashMap hmUserDetails,
             HashMap hmEntitlementDetails, String field) {
            /*
          * You must write code to validate attributes. Parent
          * data values can be fetched by using hmUserDetails.get(field)
          * Depending on the outcome of the validation operation,
          * the code must return true or false.
          */
          /*
          * In this sample code, the value "false" is returned if the field
          * contains the number sign (#). Otherwise, the value "true" is
          * returned.
          */
             boolean valid=true;
             String sFirstName=(String) hmUserDetails.get(field);
             for(int i=0;i<sFirstName.length();i++){
               if (sFirstName.charAt(i) == '#'){
                     valid=false;
                     break;
               }
             }
             return valid;
      }
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file in the following directory:

   For Oracle Identity Manager release 11.1.*x*:

   Oracle Identity Manager database

   Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use this utility, verify that the `WL_HOME` environment variable is set to the directory in which Oracle WebLogic Server is installed.

   For Microsoft Windows:

   OIM_HOME/server/bin/UploadJars.bat

   For UNIX:

   OIM_HOME/server/bin/UploadJars.sh

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

> **Note:**
>
> See Download JAR Utility of *Oracle Fusion Middleware Deveoping and Customizing Applications for Oracle Identity Manager* for detailed information about the Upload JARs utility

4. If you created the Java class for validating a user attribute for reconciliation, then:
   a. Log in to the Design Console.
   b. Search for and open the **Lookup.SAP.HRMS.ReconValidation** lookup definition.
   c. In the Code Key, enter the resource object field name. In the Decode, enter the class name.
   d. Save the changes to the lookup definition.
   e. Search for and open the **Lookup.SAP.HRMS.Configuration** lookup definition.
   f. Set the value of the Use Validation For Recon entry to `yes`.
   g. Save the changes to the lookup definition.

4.5 Configuring Transformation of Data During User Reconciliation

You can configure transformation of reconciled data according to your requirements. For example, you can use First Name and Last Name values to create a value for the Full Name field in Oracle Identity Manager.

To configure transformation of single-valued user data fetched during reconciliation:

1. Write code that implements the required transformation logic in a Java class.

   This transformation class must implement the oracle.iam.connectors.common.transform.Transformation interface and the transform method.

> **See Also:**
>
> The Javadocs shipped with the connector for more information about this interface

The following sample transformation class creates a value for the Full Name attribute by using values fetched from the First Name and Last Name attributes of the target system:

```
package oracle.iam.connectors.common.transform;
```

```
import java.util.HashMap;

public class TransformAttribute implements Transformation {

      /*
      Description:Abstract method for transforming the attributes

      param hmUserDetails<String,Object>

      HashMap containing parent data details

      param hmEntitlementDetails <String,Object>

      HashMap containing child data details

      */
      public Object transform(HashMap hmUserDetails, HashMap
hmEntitlementDetails,String sField) {
      /*
       * You must write code to transform the attributes.
       Parent data attribute values can be fetched by
       using hmUserDetails.get("Field Name").
       * Return the transformed attribute.
       */
      String sFirstName= (String)hmUserDetails.get("First Name");
      String sLastName= (String)hmUserDetails.get("Last Name");
      String sFullName=sFirstName+"."+sLastName;
      return sFullName;
      }
}
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file in the following directory:

   For Oracle Identity Manager release 11.1.*x*:

   Oracle Identity Manager database

   Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use this utility, verify that the `WL_HOME` environment variable is set to the directory in which Oracle WebLogic Server is installed.

   For Microsoft Windows:

   OIM_HOME/server/bin/UploadJars.bat

   For UNIX:

   OIM_HOME/server/bin/UploadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

> **See Also:**
>
> See Download JAR Utility of *Oracle Fusion Middleware Deveoping and Customizing Applications for Oracle Identity Manager* for detailed information about the Upload JARs utility

4. If you created the Java class for transforming a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Search for and open the **Lookup.SAP.HRMS.ReconTransformation** lookup definition.
   c. In the **Code Key** column, enter the resource object field name. In the **Decode** column, enter the class name.
   d. Save the changes to the lookup definition.
   e. Search for and open the **Lookup.SAP.HRMS.Configuration** lookup definition.
   f. Set the value of the Use Transformation For Recon entry to yes.
   g. Save the changes to the lookup definition.

5
Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to connector testing:

- Running Test Cases
- Troubleshooting

5.1 Running Test Cases

When you run the PFAL transaction on the target system, you can specify the number or range of employee records for which you want to generate IDocs. You can use this feature to create the flat file for a minimum number of records and then perform the rest of the full reconciliation procedure.

5.2 Troubleshooting

The following sections provide solutions to some commonly encountered problems associated with the connector:

- Connection Errors
- Common SNC Errors

5.2.1 Connection Errors

The following table provides solutions to common connection errors.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to SAP Employee Reconciliation. **Returned Error Message:** Connection error encountered **Returned Error Code:** `INVALID_CONNECTION_ERROR`	• Ensure that SAP Employee Reconciliation is running. • Ensure that Oracle Identity Manager is running (that is, the database is running). • Ensure that all the adapters have been compiled. • Examine the Oracle Identity Manager record (from the IT Resources form). Ensure that the IP address, admin ID, and admin password are correct.
Authentication error **Returned Error Message:** Invalid or incorrect password **Returned Error Code:** `AUTHRNTICATION_ERROR`	Ensure that the specified SAP connection user ID and password are correct.

5.2.2 Common SNC Errors

The following table provides a solution to an SNC error.

Problem Description	Solution

Trying to connect to SAP through SNC.
Returned Error Message:
SAP Connection JCO Exception
Returned Error Code:
`SNC required for this connection`
	Ensure that values for the following IT resource parameters are correctly specified as shown in the following example:
	• SNC my name:
	`p:CN=TST,OU=SAP, O=ORA,c=IN`
	• SNC partner name:
	`p:CN=I47, OU=SAP, O=ORA, C=IN`
	• SNC lib: The following are examples of SNC lib paths for Windows and Linux:
	– SNC lib for Windows:
	`C://usr//sap//sapcrypto.dll`
	– SNC lib for Linux:
	`//home/oracle/sec/sapcrypto.so`
	• SNC mode: `Yes`

Trying to perform employee reconciliation/ lookup field synchronization in the SNC mode. **Returned Error Message:** No suitable SAP user found for X.509-client certificate. **Returned Error Code:** `JCO_ERROR_LOGON_FAILURE`	Setup a mapping between the Distinguished Name provided by a X.509 Certificate and an ABAP User in view VUSREXTID in transaction SM30. Choose external ID type as DN.
Trying to perform employee reconciliation/ lookup field synchronization in the SNC mode. **Returned Error Message:** Reconciliation via TRFC fails when SNC is enabled. **Returned Error Code:** `JCO_ERROR_LOGON_FAILURE`	Program ID must have SNC enabled in transaction SM59.
Trying to perform employee reconciliation/ lookup field synchronization in the SNC mode. **Returned Error Message:** SNC name of partner system not in the ACL system. **Returned Error Code:** `JCO_ERROR_LOGON_FAILURE`	Maintain SNC names of the system from which RFC and CPIC connections are to be accepted in view VSNCSYSACL for External type ACL entry.

6
Known Issues

The following are known issues associated with this release of the connector:

- **Bug 18668482**

  IDOCs are picked by SAP HRMS listener but stay in data received state for long.

- **Bug 8510259**

  As mentioned earlier in this guide, only infotypes in which at least one attribute has been modified are sent to Oracle Identity Manager during incremental reconciliation. If the organization ID of the user is changed, then mandatory attributes, such as the first and last names, are not sent to Oracle Identity Manager because these attributes are not in the same infotype as the organization ID. When this happens, the reconciliation event created from the IDoc sent to Oracle Identity Manager remains in the Event Received state.

- **Bug 7207232**

  Some Asian languages use multibyte character sets. If the character limit for fields on the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this point:

  Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

  See Modifying Field Lengths on the OIM User Form for information about working around this issue.

- **Bug 9410516**

  If an event is marked as future dated in SAP HRMS, then this change is propagated to Oracle Identity Manager as an IDoc and a deferred reconciliation event is created. However, if you cancel this future-dated event in SAP HRMS, Oracle Identity Manager still processes the deferred reconciliation event at the scheduled time.

- **Bug 9688099**

  On Oracle Identity Manager release 9.1.0.x, suppose a user's manager in SAP HRMS is not an OIM User. When the user's record is reconciled, an OIM User identity is created for the user but the Manager ID field is left empty. On Oracle Identity Manager release 11.1.1, an OIM User identity is not created at all for the user.

- **Bug 13429841**

  Limitation:

Whenever any jar is updated/modified, if application server is not restarted then it will throw the following error:

```
java.lang.UnsatisfiedLinkError: Native Library
      /usr/local/jco/libsapjco3.so


java.lang.UnsatisfiedLinkError: Native Library
      /usr/local/jco/libsapjco3.dll
```

already loaded in another classloader. It is limitation from SAP JCO.

Analysis:

Whenever any jar is updated/modified, the application server tries to register SAP destination data provider (SAP JCO) even though it is already registered. Therefore the application server throws an error.

Workaround:

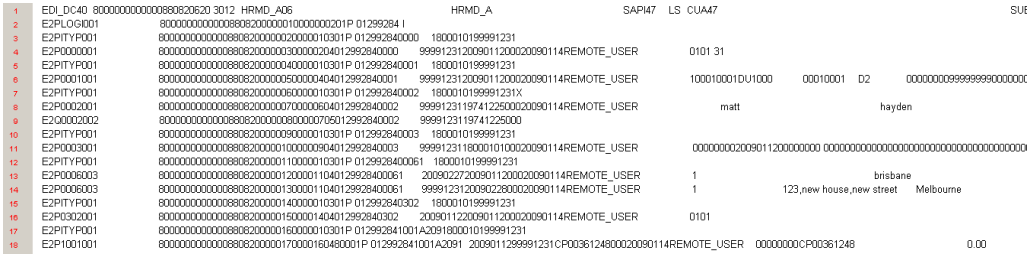
Restart the application server if any jar is updated or modified in Oracle Identity Manager server.

A

Structure of a Sample IDoc

Figure A-1 shows part of a sample IDoc. Display of line numbers was enabled in the text editor in which this IDoc was opened.

Figure A-1 Part of a Sample IDoc



The following are some of the elements seen in this screenshot:

- The first row in the IDoc is called the control record. It starts with the EDI_DC40 segment, and it contains information such as the message type (HRMD_A), idoc type (HRMD_A06), sender ID (CUA47), and receiver ID (OIMIDoc).
- The first column lists the segments.
- All other rows in the IDoc are called data records. Each of these records contains data from one segment.
- In a single IDoc, there is one E2PLOGI segment row for each employee. This record is the header record for the employee, and it contains information such as the object type (for example, P denotes person) and object ID (personnel number).
- The E2PITYP segment row after the E2PLOGI segment is the header record for an infotype. It contains information such as the infotype name, start date, and end date.
- The E2Pxxxx segment row contains the actual data of the infotype specified by the preceding E2PITYP segment row. For example, the E2P0001 segment row contains data, such as the first name and last name, of the 0001 infotype. See Verifying Segment Details in Lookup Definitions for information about the information held in segment names.

During full and incremental reconciliation, the parser used by the connector scheduled tasks reads data in the IDocs. The following sequence of steps describes how the parser reads an IDoc:

1. The parser does not need use the EDI_DC40 segment (control record).
2. The parser considers E2PLOGI as the root segment. This is defined as the value of the Root Segment entry in the Lookup.SAP.HRMS.Configuration lookup definition. The parser also uses some other entries in this lookup definition, such as Event Begin Date, Actions Event, and Event.

> **See Also:**
>
> Table 2-2

3. When the parser reaches an E2LOGI segment, it performs one of the following steps:
   - The connector only processes records whose object type is P (person). If the object type specified in an E2LOGI segment row is not P, then the parser skips rows until it reaches the next E2LOGI segment row.
   - If the value of the delete indicator is D, then the parser considers as the record as a deleted record and it creates a delete reconciliation event. The delete indicator is specified as the value of the Delete Indicator entry in the Lookup.SAP.HRMS.Configuration lookup definition. The parser then skips rows until it reaches the next E2LOGI segment row.
   - For an E2PLOGI row in which the object type is P:
     a. The parser reads the User ID (Personnel number). This is from the E2PLOGI row.
     b. From the E2PITYP segment, the parser reads the event start date. This segment specifies whether the event is current dated or future dated.
     c. E2P0000 is the segment for the Action infotype (0000). This segment specifies whether the event is a hire, terminate, or lifecycle event. also gets employee group and employee sub group to compare with OIM employee type.
     d. When it reads segment records such as E2P0001, E2P0002, and E2P0003, the parser uses the Lookup.SAP.HRMS.AttributeMapping lookup definition to fetch attribute values from the rows.

     > **See Also:**
     >
     > Table 2-2

     e. Using the data that it reads from the E2PLOGI block for a single employee, the parser creates a reconciliation event.