Contents

Preface

<table>
<thead>
<tr>
<th>Audience</th>
<th>ix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation Accessibility</td>
<td>ix</td>
</tr>
<tr>
<td>Conventions</td>
<td>ix</td>
</tr>
<tr>
<td>Related Documents</td>
<td>ix</td>
</tr>
</tbody>
</table>

What's New in Oracle Identity Manager Connector for Fusion Apps?

<table>
<thead>
<tr>
<th>Software Updates</th>
<th>xi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation-Specific Updates</td>
<td>xi</td>
</tr>
</tbody>
</table>

1 About the Fusion Apps Connector

1.1 Introduction to the Fusion Apps Connector                          1-1
1.2 Certified Components for the Fusion Apps Connector                1-2
1.3 Certified Languages for the Fusion Apps Connector                 1-2
1.4 Connector Architecture of the Fusion Apps Connector               1-3
   1.4.1 FA Source of Truth – Cloud or On-Premise Use Case             1-4
   1.4.2 External HRMS or IDM Source of Truth – FA on Cloud or On-Premise Use Case  1-5
   1.4.3 FA and External HRMS Source of Truth – FA on Cloud or On-Premise Use Case  1-6
   1.4.4 FA Source of Truth With LDAPSync – FA on Cloud or On-Premise Use Case  1-7
   1.4.5 External HRMS Source of Truth With LDAPSync – FA on Cloud or On-Premise Use Case  1-8
   1.4.6 FA and External HRMS Source of Truth With LDAPSync – FA on Cloud or On-Premise Use Case  1-9
1.5 Features of the Fusion Apps Connector                               1-9
   1.5.1 Full and Incremental Reconciliation                            1-10
   1.5.2 Limited Reconciliation                                         1-10
   1.5.3 Batched Reconciliation                                         1-10
   1.5.4 Reconciliation of Deleted User Records                          1-10
   1.5.5 Transformation and Validation of Account Data                  1-10
1.5.6 Support for the Connector Server
1.6 Lookup Definitions Used During Connector Operations
  1.6.1 Lookup Definition Synchronized with the Target System
  1.6.2 Preconfigured Lookup Definitions for the Fusion Apps Connector
    1.6.2.1 Lookup.FAIdentityService.Configuration
    1.6.2.2 Lookup.FAIdentityService.UM.Configuration
    1.6.2.3 Lookup.FAIdentityService.UM.ProvAttrMap
    1.6.2.4 Lookup.FAIdentityService.UM.ReconAttrMap
    1.6.2.5 Lookup.FAUserRequestService.Configuration.Trusted
    1.6.2.6 Lookup.FAUserRequestService.UM.Configuration.Trusted
    1.6.2.7 Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted
    1.6.2.8 Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults
1.7 Connector Objects Used During Target Resource Reconciliation
1.8 Connector Objects Used During Trusted Source Reconciliation
1.9 Connector Objects Used During Provisioning
  1.9.1 Provisioning Functions
  1.9.2 User Fields for Provisioning
1.10 Roadmap for Deploying and Using the Connector

2 Deploying the Fusion Apps Connector

2.1 Preinstallation
2.2 Installation
  2.2.1 Understanding Installation of the Fusion Apps Connector
  2.2.2 Running the Connector Installer
  2.2.3 Configuring the IT Resource for the Target System
    2.2.3.1 IT Resource Parameters
    2.2.3.2 Specifying Values for the IT Resource Parameters
2.3 Postinstallation
  2.3.1 Configuring Resource Object Dependency
  2.3.2 Configuring Oracle Identity Manager
    2.3.2.1 Creating and Activating a Sandbox
    2.3.2.2 Creating a New UI Form
    2.3.2.3 Creating an Application Instance
    2.3.2.4 Upgrading User Form in Oracle Identity Manager
    2.3.2.5 Publishing a Sandbox
    2.3.2.6 Harvesting Entitlements and Sync Catalog
    2.3.2.7 Updating an Existing Application Instance with a New Form
    2.3.2.8 Updating an Application Instance
  2.3.3 Updating Access Policies
    2.3.3.1 FA Source of Truth - Cloud or On-Premise Use Case
2.3.3.2 HRMS or IDM Source of Truth - FA on Cloud or On-Premise Use Case 2-11
2.3.3.3 FA and External HRMS Source of Truth - FA on Cloud or On-Premise Use Case 2-12
2.3.3.4 FA Source of Truth With LDAP Sync - FA on Cloud or On-Premise Use Case 2-12
2.3.3.5 External HRMS Source of Truth With LDAP Sync - FA on Cloud or On-Premise Use Case 2-12
2.3.3.6 FA and External HRMS Source of Truth With LDAP Sync - FA on Cloud or On-Premise Use Case 2-13
2.3.4 Process Task Updates 2-13
2.3.5 Clearing Content Related to Connector Resource Bundles from the Server Cache 2-14
2.3.6 Localizing Field Labels in UI Forms 2-15
2.3.7 SSO Email ID propagation for FA Source of Truth with LDAP Sync 2-17
2.3.8 Managing Logging for the Fusion Apps Connector 2-19
  2.3.8.1 Understanding Log Levels 2-19
  2.3.8.2 Enabling Logging 2-20
2.3.9 Configuring SSL for the Fusion Apps Connector 2-21
2.4 Upgrading the Connector 2-22

3 Using the Fusion Apps Connector

3.1 Scheduled Job for Lookup Field Synchronization for Fusion Apps Connector 3-1
3.2 Configuring Reconciliation for Fusion Apps Connector 3-2
  3.2.1 Full Reconciliation for Fusion Apps Connector 3-2
    3.2.1.1 Export Users from the Fusion Apps Target System 3-3
    3.2.1.2 Use Flat File Connector to Load Exported Users 3-5
  3.2.2 Limited Reconciliation for Fusion Apps Connector 3-7
  3.2.3 Batched Reconciliation for Fusion Apps Connector 3-7
  3.2.4 Reconciliation Scheduled Jobs for Fusion Apps Connector 3-8
    3.2.4.1 Scheduled Jobs for Reconciliation of User Records 3-8
    3.2.4.2 Scheduled Job for Reconciliation of Deleted Users Records 3-10
3.3 Configuring Scheduled Jobs 3-11
3.4 Performing Provisioning Operations 3-12
3.5 Uninstalling the Fusion Apps Connector 3-12

4 Extending the Functionality of the Fusion Apps Connector

4.1 Adding New User Attributes for Reconciliation 4-1
  4.1.1 Adding New Attributes on the Process Form 4-2
  4.1.2 Adding Attributes to the Resource Object 4-2
  4.1.3 Creating Reconciliation Field Mapping 4-3
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.4 Creating Entries in Lookup Definitions</td>
<td>4-4</td>
</tr>
<tr>
<td>4.1.5 Performing Changes in a New UI Form</td>
<td>4-5</td>
</tr>
<tr>
<td>4.2 Adding New User Attributes for Provisioning</td>
<td>4-5</td>
</tr>
<tr>
<td>4.2.1 Adding New Attributes for Provisioning</td>
<td>4-6</td>
</tr>
<tr>
<td>4.2.2 Creating Entries in Lookup Definitions for Provisioning</td>
<td>4-7</td>
</tr>
<tr>
<td>4.2.3 Creating a Task to Enable Update Operations</td>
<td>4-8</td>
</tr>
<tr>
<td>4.2.4 Replicating Form Designer Changes to a New UI Form</td>
<td>4-10</td>
</tr>
<tr>
<td>4.3 Configuring Transformation of Data During User Reconciliation</td>
<td>4-11</td>
</tr>
<tr>
<td>4.4 Configuring Validation of Data During Reconciliation and Provisioning</td>
<td>4-13</td>
</tr>
</tbody>
</table>

A Files and Directories on the Fusion Apps Connector Installation

Media
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>Connector Architecture: Topology 1</td>
<td>1-4</td>
</tr>
<tr>
<td>1-2</td>
<td>Connector Architecture: Topology 2</td>
<td>1-5</td>
</tr>
<tr>
<td>1-3</td>
<td>Connector Architecture: Topology 3</td>
<td>1-6</td>
</tr>
<tr>
<td>1-4</td>
<td>Connector Architecture: Topology 4</td>
<td>1-7</td>
</tr>
<tr>
<td>1-5</td>
<td>Connector Architecture: Topology 5</td>
<td>1-8</td>
</tr>
<tr>
<td>1-6</td>
<td>Connector Architecture: Topology 6</td>
<td>1-9</td>
</tr>
<tr>
<td>4-1</td>
<td>Adding a New Field on the Process Form</td>
<td>4-2</td>
</tr>
<tr>
<td>4-2</td>
<td>Newly Added Reconciliation Field</td>
<td>4-3</td>
</tr>
<tr>
<td>4-3</td>
<td>New Reconciliation Field Mapped to a Process Data Field</td>
<td>4-4</td>
</tr>
<tr>
<td>4-4</td>
<td>Newly Added Entry to Lookup Definition</td>
<td>4-5</td>
</tr>
<tr>
<td>4-5</td>
<td>Newly Added Field</td>
<td>4-7</td>
</tr>
<tr>
<td>4-6</td>
<td>Newly Added Entry to the Lookup Definition</td>
<td>4-8</td>
</tr>
<tr>
<td>4-7</td>
<td>Newly Added Task to the Process Definition</td>
<td>4-9</td>
</tr>
<tr>
<td>4-8</td>
<td>List of Adapter Variables</td>
<td>4-9</td>
</tr>
</tbody>
</table>
### List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>Certified Components</td>
<td>1-2</td>
</tr>
<tr>
<td>1-2</td>
<td>Entries in the Lookup.FAIdentityService.Configuration Lookup Definition</td>
<td>1-13</td>
</tr>
<tr>
<td>1-3</td>
<td>Entries in the Lookup.FAIdentityService.UM.Configuration Lookup Definition</td>
<td>1-14</td>
</tr>
<tr>
<td>1-4</td>
<td>Entries in the Lookup.FAUserRequestService.Configuration.Trusted Lookup Definition</td>
<td>1-15</td>
</tr>
<tr>
<td>1-5</td>
<td>Entries in the Lookup.FAUserRequestService.Configuration.Trusted Lookup Definition</td>
<td>1-15</td>
</tr>
<tr>
<td>1-6</td>
<td>Entries in the Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults Lookup Definition</td>
<td>1-16</td>
</tr>
<tr>
<td>1-7</td>
<td>Entries in the Lookup.FAIdentityService.UM.ReconAttrMap lookup definition</td>
<td>1-17</td>
</tr>
<tr>
<td>1-8</td>
<td>Entries in the Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted lookup definition</td>
<td>1-17</td>
</tr>
<tr>
<td>1-9</td>
<td>Provisioning Functions</td>
<td>1-18</td>
</tr>
<tr>
<td>1-10</td>
<td>Entries in the Lookup.FAIdentityService.UM.ProvAttrMap lookup definition</td>
<td>1-19</td>
</tr>
<tr>
<td>2-1</td>
<td>IT Resource Parameters for FA User Request Service</td>
<td>2-4</td>
</tr>
<tr>
<td>2-2</td>
<td>IT Resource Parameters for FA Identity Service</td>
<td>2-5</td>
</tr>
<tr>
<td>2-3</td>
<td>Log Levels and ODL Message Type:Level Combinations</td>
<td>2-20</td>
</tr>
<tr>
<td>3-1</td>
<td>Attributes of the FA Identity Service Application Roles Lookup Reconciliation</td>
<td>3-2</td>
</tr>
<tr>
<td>3-2</td>
<td>Header Names</td>
<td>3-5</td>
</tr>
<tr>
<td>3-3</td>
<td>Attributes of the Scheduled Jobs for Reconciliation of User Records for FA User Request Service</td>
<td>3-8</td>
</tr>
<tr>
<td>3-4</td>
<td>Attributes of the Scheduled Jobs for Reconciliation of User Records for FA Identity Service</td>
<td>3-9</td>
</tr>
<tr>
<td>3-5</td>
<td>Attributes of the Scheduled Job for Delete User Reconciliation</td>
<td>3-11</td>
</tr>
<tr>
<td>A-1</td>
<td>Files and Directories on the Fusion Apps Connector Installation Media</td>
<td>A-1</td>
</tr>
</tbody>
</table>
Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with the Fusion Apps target system.

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.

Conventions

The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td><code>monospace</code></td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>

Related Documents

For information about installing and using Oracle Identity Governance 12.2.1.3.0, visit the following Oracle Help Center page:


For information about installing and using Oracle Identity Manager 11g Release 2, 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
What’s New in Oracle Identity Manager Connector for Fusion Apps?

This chapter provides an overview of the updates made to the software and documentation for the Fusion Apps connector in release 11.1.1.5.0.

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

- **Software Updates**
  This section provides updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- **Documentation-Specific Updates**
  These include major changes made to this guide. For example, the relocation of a section from the second chapter to the third chapter is a documentation-specific update. These changes are not related to software updates.

**Software Updates**

The following section provides information on software updates:

**Software Updates in Release 11.1.1.5.0**

This is the first release of the Oracle Identity Manager connector for Fusion Apps. Therefore, there are no software-specific updates in this release.

**Documentation-Specific Updates**

The following section provides information on documentation-specific updates:

**Documentation-Specific Updates in Release 11.1.1.5.0**

The following documentation-specific update has been made in revision "04" of this guide:

The Table 1-1 table has been modified for the following:

- The “Oracle Identity Manager” row has been renamed to “Oracle Identity Governance or Oracle Identity Manager” and updated to include support for Oracle Identity Governance 12c (12.2.1.3.0) release.
- The “Target System” row has been modified to include support for Fusion Apps Release 13.

The following documentation-specific update has been made in revision "03" of this guide:
In step 3.a of Preinstallation, information on the “ORA_FND_IT_SECURITY_MANAGER_JOB” role has been included.

The following documentation-specific update has been made in revision "02" of this guide:

The “Connector Server” row has been added to Table 1-1.

The following documentation-specific update has been made in revision "01" of this guide:

This is the first release of the Oracle Identity Manager connector for Fusion Apps. Therefore, there are no documentation-specific updates in this release.
1

About the Fusion Apps Connector

The Fusion Apps connector integrates Oracle Identity Manager (OIM) with the Fusion Apps target system.

The following topics provide a high-level overview of the Fusion Apps connector:

• Introduction to the Fusion Apps Connector
• Certified Components for the Fusion Apps Connector
• Certified Languages for the Fusion Apps Connector
• Connector Architecture of the Fusion Apps Connector
• Features of the Fusion Apps Connector
• Lookup Definition Synchronized with the Target System
• Connector Objects Used During Target Resource Reconciliation
• Connector Objects Used During Trusted Source Reconciliation
• Connector Objects Used During Provisioning
• Roadmap for Deploying and Using the Connector

1.1 Introduction to the Fusion Apps Connector

The Fusion Apps connector enables you to use Fusion Apps as a managed (target) source of identity data for Oracle Identity Manager.

Note:

At some places in this guide, Fusion Apps has been referred to as the target system.

The Fusion Apps Connector aims to allow provisioning and reconciliation operations on the target including trusted and target operations. In the account management (target resource) mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Manager.

Note:

The Fusion Apps Connector consists of FA User Request service and FA Identity service for performing various operations. The FA User Request service is used to perform trusted reconciliation operation and is ATOM based. The FA Identity service is used to perform provisioning and target reconciliation operations and is System for Cross-domain Identity Management (SCIM) based.
FA Identity REST service is used to perform provisioning and reconciliation operations for users present on the target system. Reconciliation operation is performed only for those users who have an externalID, which indicates that the users are managed by Oracle Identity Manager. To perform a trusted reconciliation operation, the connector uses the FA User Request service. The Fusion Apps Connector aims to allow provisioning and reconciliation operations on the target including trusted and target operations. To perform a trusted reconciliation operation, the Fusion Apps Connector uses the FA User Request service. To perform a target provisioning and reconciliation operation, the connector uses the FA Identity service.

During a provisioning operation, Single Sign-On (SSO) accounts are first created for all the users and the respective SSO mail IDs are updated back in the target system. If the SSO email is updated later through Oracle Identity Manager, then the updated email is also propagated to the target system.

In the identity reconciliation (trusted source) configuration of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager. However, to perform target based provisioning or reconciliation, the connector uses the FA Identity service.

This connector is an integration between Oracle Identity Manager and Fusion Apps and makes use of the ATOM pub and SCIM RESTful services for managing users and entitlements in the target from Oracle Identity Manager.

### 1.2 Certified Components for the Fusion Apps Connector

These are the software components and their versions required for installing and using the Fusion Apps connector.

Table 1-1 lists the deployment requirements for the connector.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Identity Governance or Oracle Identity Manager</td>
<td>You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager:</td>
</tr>
<tr>
<td></td>
<td>• Oracle Identity Governance 12c (12.2.1.3.0)</td>
</tr>
<tr>
<td></td>
<td>• Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0)</td>
</tr>
<tr>
<td>Target System</td>
<td>Fusion Apps Release 12, Release 13</td>
</tr>
<tr>
<td>Connector Server</td>
<td>11.1.1.5.0</td>
</tr>
<tr>
<td>Connector Server JDK</td>
<td>JDK 1.6 or later</td>
</tr>
</tbody>
</table>

### 1.3 Certified Languages for the Fusion Apps Connector

These are the languages that the connector supports.

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
1.4 Connector Architecture of the Fusion Apps Connector

The Fusion Apps connector is implemented by using the Identity Connector Framework (ICF).

The ICF is a component that provides basic reconciliation and provisioning operations that are common to all Oracle Identity Manager connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering. The ICF is shipped along with Oracle Identity Manager. Therefore, you need not configure or modify the ICF.

Following are the various topologies supported by the connector:

- **FA Source of Truth – Cloud or On-Premise Use Case**
- **External HRMS or IDM Source of Truth – FA on Cloud or On-Premise Use Case**
1.4.1 FA Source of Truth – Cloud or On-Premise Use Case

Topology 1: FA Source of Truth – Cloud or On-Premise Use Case

In this use case, the FA user trusted reconciliation scheduled task will be using the FA User Request service REST API which is responsible for fetching all the users for the first time and later incrementally from the ATOM feed and create them in the Oracle Identity Manager repository. Once the users are successfully created, the FA Role for FA User will be defined in Oracle Identity Manager, which helps define a user membership rule based on the user profile attribute of the FA user created earlier. Once this role is defined, the FA access policy for FA user will be based on the role created earlier. This will be responsible for provisioning an enterprise directory account and also link an FA account for the user created earlier. This process of linking is performed in Oracle Identity Manager in order to ensure that the same can be used to update the SSO attributes back to the target system at a later stage. Additionally, in this use case, a FA Enterprise Directory Resource dependency also exists. To update the SSO, the Fusion Apps connector will ship an adapter which is responsible for copying all the SSO account details like email and username from the enterprise directory process form to the FA process form. Now, the Fusion Apps connector will update the FA account with SSO details using the Identity Service REST API. At this point, the user should be able to login to the target using the SSO details. Finally, the FA User Target Reconciliation scheduled task will use the Identity Service REST API to query all users for the first time and later incrementally followed by updating the FA user accounts in the Oracle Identity Manager. Once the manage FA user account is
linked in an earlier stage, roles are listed in the Oracle Identity Manager catalog after which more entitlements can be requested for this Fusion Apps account. To request entitlements, in Step 1 of Figure 1-1, you must run the FA Identity Service Application Roles Lookup Reconciliation schedule job to reconcile the FA Roles into Oracle Identity Manager and those roles will then list as entitlements. Through this, users can request these entitlement for the FA Account in Oracle Identity Manager itself.

1.4.2 External HRMS or IDM Source of Truth – FA on Cloud or On-Premise Use Case

Topology 2: External HRMS or IDM Source of Truth – FA on Cloud or On-Premise Use Case

Figure 1-2 Connector Architecture: Topology 2

In this use case, users are created in the Oracle Identity Manager repository by running the external HRMS user trusted reconciliation or through other means. After users are successfully created, the FA Role for External User role will be defined in Oracle Identity Manager which helps define a user membership rule based on an attribute of the Oracle Identity Manager user created earlier. Once this role is defined, the FA access policy for an external user will be based on the role created earlier. This policy will be responsible to provision an Enterprise Directory Account and an FA account for the user created earlier. The FA account will create an account in the FA target system as this account is not present in the FA target earlier. This creation will include the creation of SSO attributes and an externalID. The value for externalID will be provided when an Oracle Identity Manager user was created at an earlier instance. Additionally, in this use case, a FA OID resource dependency also exists. This dependency will ensure that an OID account will be provisioned followed by the provisioning of an FA account for users created earlier. Finally, the FA user target
reconciliation scheduled task uses the Identity Service REST API to query all users for the first time and later incrementally followed by updating the FA user accounts in the Oracle Identity Manager. This task will get all the attributes of the Fusion Apps account including any entitlements assigned. However, this task will not get any SSO attributes and will also ensure that it will only get users who have their externalID values set.

1.4.3 FA and External HRMS Source of Truth – FA on Cloud or On-Premise Use Case

Topology 3: FA and External HRMS Source of Truth – FA on Cloud or On-Premise Use Case

This use case is a combination of the above two use cases where the source of truth are both FA target system and External HRMS. In this case, depending on the source, the role FA Role for FA User or FA Role for External User are associated to the user and their corresponding access policies. Additionally, based on the source, the FA User Accounts are either linked or created.
1.4.4 FA Source of Truth With LDAPSync – FA on Cloud or On-Premise Use Case

Topology 4: FA Source of Truth With LDAPSync – FA on Cloud or On-Premise Use Case

Figure 1-4 Connector Architecture: Topology 4

This use case is similar to the use case discussed in FA Source of Truth – Cloud or On-Premise Use Case. In this use case, the LDAP Sync mode is responsible to manage users within LDAP. Here, Oracle Identity Manager with Oracle Internet Directory (OID) or iplanet (ODSEE) or Active Directory (AD) or Oracle Unified Directory (OUD) is selected during installation. It is not required to install any directory connector separately and the dependency of LDAP resource is managed internally in this use case.
1.4.5 External HRMS Source of Truth With LDAPSync – FA on Cloud or On-Premise Use Case

Topology 5: External HRMS Source of Truth With LDAPSync – FA on Cloud or On-Premise Use Case

Figure 1-5  Connector Architecture: Topology 5

This use case is similar to the use case discussed in External HRMS or IDM Source of Truth – FA on Cloud or On-Premise Use Case. In this use case, the LDAP Sync mode is responsible to manage users within LDAP. Here, Oracle Identity Manager with Oracle Internet Directory (OID) or iplanet (ODSEE) or Active Directory (AD) or Oracle Unified Directory (OUD) is selected during installation. It is not required to install any directory connector separately and the dependency of LDAP resource is managed internally in this use case.
1.4.6 FA and External HRMS Source of Truth With LDAPSync – FA on Cloud or On-Premise Use Case

This use case is similar to the use case discussed in FA and External HRMS Source of Truth – FA on Cloud or On-Premise Use Case. In this use case, the LDAP Sync mode is responsible to manage users within LDAP. Here, Oracle Identity Manager with Oracle Internet Directory (OID) or iplanet (ODSEE) or Active Directory (AD) or Oracle Unified Directory (OUD) is selected during installation. It is not required to install any directory connector separately as the dependency of the LDAP resource is managed internally in this use case.

1.5 Features of the Fusion Apps Connector

The features of the connector include support for connector server, full reconciliation, and limited reconciliation.

- Full and Incremental Reconciliation
- Limited Reconciliation
- Batched Reconciliation
- Reconciliation of Deleted User Records
- Transformation and Validation of Account Data
1.5.1 Full and Incremental Reconciliation

In full reconciliation, all records are fetched from the target system to Oracle Identity Manager.

After you deploy the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full reconciliation run, incremental reconciliation is automatically enabled. In incremental reconciliation, user accounts that have been added or modified since the last reconciliation run are fetched into Oracle Identity Manager. You can perform a full reconciliation run at any time.

See Full Reconciliation for Fusion Apps Connector.

1.5.2 Limited Reconciliation

You can reconcile records from the target system based on a specified filter criterion.

To limit or filter the records that are fetched into Oracle Identity Manager during a reconciliation run, you can specify the subset of added or modified target system records that must be reconciled. See Limited Reconciliation for Fusion Apps Connector.

1.5.3 Batched Reconciliation

You can break down a reconciliation run into batches by specifying the number of records that must be included in each batch.

See Batched Reconciliation for Fusion Apps Connector.

1.5.4 Reconciliation of Deleted User Records

You can configure the connector for reconciliation of deleted user records.

In the target resource mode (FA Non-authoritative), if a user record is deleted on the target system, then the corresponding FA user resource is revoked from the OIM User. In trusted source mode (FA Authoritative mode), if a user record is deleted on the target system, then the corresponding OIM User is deleted. To perform FA Identity Service user delete reconciliation, you must specify values for Fusion Apps User Delete Reconciliation scheduled job. This scheduled job is used to reconcile data about deleted users in the target source (identity management) mode of the connector.

See Scheduled Job for Reconciliation of Deleted Users Records.

1.5.5 Transformation and Validation of Account Data

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning.

In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. The following sections provide more information:
1.5.6 Support for the Connector Server

Connector Server is one of the features provided by ICF. By using one or more connector servers, the connector architecture permits your application to communicate with externally deployed bundles.

A Java connector server is useful when you do not want to execute a Java connector bundle in the same VM as your application. It can be beneficial to run a Java connector on a different host for performance improvements if the bundle works faster when deployed on the same host as the native managed resource.

See Also:

Using an Identity Connector Server in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager for information about installing and configuring connector server and running the connector server

1.6 Lookup Definitions Used During Connector Operations

Lookup definitions used during reconciliation and provisioning are either preconfigured or can be synchronized with the target system.

Lookup definitions used during connector operations can be categorized as follows:

- **Lookup Definition Synchronized with the Target System**
- **Preconfigured Lookup Definitions for the Fusion Apps Connector**

1.6.1 Lookup Definition Synchronized with the Target System

Lookup field synchronization involves copying additions or changes made to specific fields in the target system to lookup definitions in Oracle Identity Manager.

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Identity Source lookup field to select an identity source during a provisioning operation performed through the Administrative and User Console. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are automatically created in Oracle Identity Manager.

The Lookup.FAIdentityService.ApplicationRoles lookup definition is populated with values fetched from the target system by the scheduled jobs for lookup field synchronization.

During a provisioning operation, you use the Application Role Name lookup field on the process form to specify a role for the user for whom the provisioning operation is being performed. The Application Role Name lookup field is populated with values from the Lookup.FAIdentityService.ApplicationRoles lookup definition, which is automatically created on Oracle Identity Manager when you deploy the connector.
The Code Key and Decode columns contain values of the __UID__ and __NAME__ of the ApplicationRole object class.

Data in each of the lookup definitions for lookup field synchronization is stored in the following format:

**Code Key:**

<IT_RESOURCE_KEY>~<LOOKUP_FIELD_VALUE>

In this format:

- **IT_RESOURCE_KEY** is the numeric code assigned to each IT resource in Oracle Identity Manager.
- **LOOKUP_FIELD_VALUE** is the connector attribute value defined for code.

Sample value:

14~FARole1

**Decode:**

<IT_RESOURCE_NAME>~<LOOKUP_FIELD_VALUE>

In this format:

- **IT_RESOURCE_NAME** is the name of the IT resource in Oracle Identity Manager.
- **LOOKUP_FIELD_VALUE** is the connector attribute value defined for decode.

Sample value:

FA Identity Service~FARole1

### 1.6.2 Preconfigured Lookup Definitions for the Fusion Apps Connector

Preconfigured lookup definitions are the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

The other lookup definitions are as follows:

- Lookup.FAIdentityService.Configuration
- Lookup.FAIdentityService.UM.Configuration
- Lookup.FAIdentityService.UM.ProvAttrMap
- Lookup.FAIdentityService.UM.ReconAttrMap
- Lookup.FAUserRequestService.Configuration.Trusted
- Lookup.FAUserRequestService.UM.Configuration.Trusted
- Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted
- Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults
1.6.2.1 Lookup.FAIdentityService.Configuration

The Lookup.FAIdentityService.Configuration lookup definition holds connector configuration entries that are used during target resource reconciliation and provisioning operations.

**Note:**

The values for these lookup definitions are preconfigured and cannot be modified.

Table 1-2 lists the default entries in this lookup definition.

**Table 1-2 Entries in the Lookup.FAIdentityService.Configuration Lookup Definition**

<table>
<thead>
<tr>
<th>Code</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any Incremental Recon</td>
<td>true</td>
<td>This entry holds the value which specified that the latest token can be of any type.</td>
</tr>
<tr>
<td>Attribute Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bundle Name</td>
<td>org.identityconnectors.faidentityservice</td>
<td>This entry holds the name of the connector bundle package.</td>
</tr>
<tr>
<td>Bundle Version</td>
<td>1.0.1115</td>
<td>This entry holds the version of the connector bundle class.</td>
</tr>
<tr>
<td>Connector Name</td>
<td>org.identityconnectors.faidentityservice.FAIdentityServiceConnector</td>
<td>This entry holds the name of the connector class.</td>
</tr>
<tr>
<td>defaultBatchSize</td>
<td>500</td>
<td>This entry holds the number of records that must be included in each batch during batched reconciliation. This entry is used only when the Batch Size attribute of the user reconciliation scheduled jobs is either empty or set to 0. See Batched Reconciliation for Fusion Apps Connector for more information about the Batch Size attribute.</td>
</tr>
<tr>
<td>User Configuration Lookup</td>
<td>Lookup.FAIdentityService.UM.Configuration</td>
<td>This entry holds the name of the lookup definition that contains user-specific configuration properties.</td>
</tr>
</tbody>
</table>

1.6.2.2 Lookup.FAIdentityService.UM.Configuration

The Lookup.FAIdentityService.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations when your target system is configured as a target resource.
Table 1-3 lists the default entries in this lookup definition.

**Table 1-3  Entries in the Lookup.FAIdentityService.UM.Configuration Lookup Definition**

<table>
<thead>
<tr>
<th>Code</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Attribute Map</td>
<td>Lookup.FAIdentityService.UM.ProvAttrMap</td>
<td>This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.FAIdentityService.UM.ReconAttrMap for more information about this lookup definition.</td>
</tr>
<tr>
<td>Recon Attribute Map</td>
<td>Lookup.FAIdentityService.UM.ReconAttrMap</td>
<td>This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.FAIdentityService.UM.ReconAttrMap for more information about this lookup definition.</td>
</tr>
</tbody>
</table>

1.6.2.3 Lookup.FAIdentityService.UM.ProvAttrMap

The Lookup.FAIdentityService.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is preconfigured and used during provisioning. Table 1-10 lists the default entries.

You can add entries in this lookup definition if you want to map new target system attributes for provisioning. See Adding New User Attributes for Provisioning.

1.6.2.4 Lookup.FAIdentityService.UM.ReconAttrMap

The Lookup.FAIdentityService.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is preconfigured and used during reconciliation. Table 1-7 lists the default entries.

You can add entries in this lookup definition if you want to map new target system attributes for reconciliation. See Adding New User Attributes for Reconciliation.

1.6.2.5 Lookup.FAUserRequestService.Configuration.Trusted

The Lookup.FAUserRequestService.Configuration.Trusted lookup definition holds connector configuration entries that are used during trusted source reconciliation.

**Note:**

The values for these lookup definitions are preconfigured and cannot be modified.

Table 1-4 lists the default entries in this lookup definition.
Table 1-4  Entries in the Lookup.FAUserRequestService.Configuration.Trusted Lookup Definition

<table>
<thead>
<tr>
<th>Code</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle Name</td>
<td>org.identityconnectors.fauserequestservice</td>
<td>This entry holds the name of the connector bundle package.</td>
</tr>
<tr>
<td>Bundle Version</td>
<td>1.0.1115</td>
<td>This entry holds the version of the connector bundle class.</td>
</tr>
<tr>
<td>Connector Name</td>
<td>org.identityconnectors.fauserequestservice.FAUserRequestServiceConnector</td>
<td>This entry holds the name of the connector class.</td>
</tr>
<tr>
<td>User Configuration Lookup</td>
<td>Lookup.FAUserRequestService.UM.Configuration.Trusted</td>
<td>This entry holds the name of the lookup definition that contains user-specific configuration properties.</td>
</tr>
<tr>
<td>defaultBatchSize</td>
<td>500</td>
<td>This entry holds the number of records that must be included in each batch during batched reconciliation. This entry is used only when the Batch Size attribute of the user reconciliation scheduled jobs is either empty or set to 0. See Batched Reconciliation for Fusion Apps Connector for more information about the Batch Size attribute.</td>
</tr>
</tbody>
</table>

1.6.2.6 Lookup.FAUserRequestService.UM.Configuration.Trusted

The Lookup.FAUserRequestService.UM.Configuration.Trusted lookup definition holds connector configuration entries that are used during trusted source reconciliation.

Table 1-5 lists the default entries in this lookup definition.

Table 1-5  Entries in the Lookup.FAUserRequestService.Configuration.Trusted Lookup Definition

<table>
<thead>
<tr>
<th>Code</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recon Attribute Defaults</td>
<td>Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults</td>
<td>This entry holds the name of the lookup definition that holds default values of the resource object fields and target system attributes. See Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults.</td>
</tr>
</tbody>
</table>
1.6.2.7 Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted

The Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted lookup definition holds the name of the lookup definition that maps resource object fields and target system attributes. This lookup definition is preconfigured. Table 1-8 lists the default entries.

1.6.2.8 Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults

The Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults lookup definition holds default values of the resource object fields and target system attributes. This lookup definition is preconfigured. Table 1-6 lists the default entries in this lookup definition.

Table 1-6 Entries in the Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults Lookup Definition

<table>
<thead>
<tr>
<th>Code</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Type</td>
<td>Full-Time</td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td>Xellerate Users</td>
<td></td>
</tr>
<tr>
<td>User Type</td>
<td>Xellerate Users</td>
<td></td>
</tr>
</tbody>
</table>

1.7 Connector Objects Used During Target Resource Reconciliation

Target resource reconciliation involves fetching data about newly created or modified accounts on the target system and using this data to add or modify resources assigned to OIM Users.

The Lookup.FAIdentityService.UM.ReconAttrMap lookup definition maps user resource object fields and target system attributes. This lookup definition is used for performing target resource user reconciliation runs.

In this lookup definition, entries are in the following format:

- **Code Key**: Reconciliation field of the resource object
- **Decode**: Name of the target system attribute
Table 1-7 lists the entries in this lookup definition.

<table>
<thead>
<tr>
<th>Resource Object Field</th>
<th>Target System Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>External ID</td>
<td>externalId</td>
</tr>
<tr>
<td>Family Name</td>
<td>name.familyName</td>
</tr>
<tr>
<td>Given Name</td>
<td>name.givenName</td>
</tr>
<tr>
<td>Id</td>
<td><em>UID</em></td>
</tr>
<tr>
<td>Preferred Language</td>
<td>preferredLanguage</td>
</tr>
<tr>
<td>Roles~Role Name[LOOKUP]</td>
<td>roles.id</td>
</tr>
<tr>
<td>Status</td>
<td><em>ENABLE</em></td>
</tr>
<tr>
<td>User Name</td>
<td><em>NAME</em></td>
</tr>
</tbody>
</table>

### 1.8 Connector Objects Used During Trusted Source Reconciliation

Trusted source reconciliation involves fetching data about newly created or modified accounts on the target system and using that data to create or update OIM Users.

The Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted lookup definition maps user fields of the OIM User form with corresponding field names in the target system. This lookup definition is used for performing trusted source reconciliation runs.

In this lookup definition, entries are in the following format:

- **Code Key**: OIM User Form Field
- **Decode**: Target System Field

Table 1-8 lists the user identity fields whose values are fetched from the target system during a trusted source reconciliation run.

<table>
<thead>
<tr>
<th>OIM User Form Field</th>
<th>Target System Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Name</td>
<td>addresses.country</td>
</tr>
<tr>
<td>Display Name</td>
<td>user.displayName</td>
</tr>
<tr>
<td>Email</td>
<td>user.emails.value</td>
</tr>
<tr>
<td>Employee Number</td>
<td>employeeNumber</td>
</tr>
<tr>
<td>Employee Type</td>
<td>userType</td>
</tr>
<tr>
<td>FA Account Id</td>
<td><em>UID</em></td>
</tr>
<tr>
<td>FA Account Status[TRUSTED]</td>
<td><em>ENABLE</em></td>
</tr>
<tr>
<td>Generation Qualifier</td>
<td>user.name.honorificSuffix</td>
</tr>
</tbody>
</table>
Table 1-8 (Cont.) Entries in the Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted lookup definition

<table>
<thead>
<tr>
<th>OIM User Form Field</th>
<th>Target System Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given Name</td>
<td>user.name.givenName</td>
</tr>
<tr>
<td>Initials</td>
<td>user.name.initials</td>
</tr>
<tr>
<td>Locality Name</td>
<td>addresses.locality</td>
</tr>
<tr>
<td>Manager</td>
<td>manager.displayName</td>
</tr>
<tr>
<td>Middle Name</td>
<td>user.name.middleName</td>
</tr>
<tr>
<td>Postal Address</td>
<td>addresses.formatted</td>
</tr>
<tr>
<td>Postal Code</td>
<td>addresses.postalCode</td>
</tr>
<tr>
<td>Preferred Language</td>
<td>user.preferredLanguage</td>
</tr>
<tr>
<td>State</td>
<td>addresses.region</td>
</tr>
<tr>
<td>Street</td>
<td>addresses.streetAddress</td>
</tr>
<tr>
<td>Surname</td>
<td>user.name.familyName</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>phoneNumbers.value</td>
</tr>
<tr>
<td>User Login</td>
<td><em>NAME</em></td>
</tr>
</tbody>
</table>

1.9 Connector Objects Used During Provisioning

Provisioning involves creating or modifying user data on the target system through Oracle Identity Manager.

This section contains the following topics:

- Provisioning Functions
- User Fields for Provisioning

1.9.1 Provisioning Functions

These are the supported provisioning functions and the adapters that perform these functions for the connector.

The Adapter column in Table 1-9 gives the name of the adapter that is used when the function is performed.

Table 1-9 Provisioning Functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Adapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a role</td>
<td>adpFAIDENTITYSERVICEADDROLE</td>
</tr>
<tr>
<td>Create a user</td>
<td>adpFAIDENTITYSERVICECREATEUSER</td>
</tr>
<tr>
<td>Delete a user</td>
<td>adpFAIDENTITYSERVICEDELETEUSER</td>
</tr>
<tr>
<td>Disable a user</td>
<td>adpFAIDENTITYSERVICEDISABLEUSER</td>
</tr>
<tr>
<td>Enable a user</td>
<td>adpFAIDENTITYSERVICEENABLEUSER</td>
</tr>
</tbody>
</table>
Table 1-9  (Cont.) Provisioning Functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Adapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Id for a source</td>
<td>adpFAIDENTITYSERVICEEXTERNALIDFORFASOURCE</td>
</tr>
<tr>
<td>Multi update</td>
<td>adpFAIDENTITYSERVICEMULTIUPDATE</td>
</tr>
<tr>
<td>Prepopulate an adapter</td>
<td>adpFAIDENTITYSERVICEPREPOPULATEADAPTER</td>
</tr>
<tr>
<td>Prepopulate external Id for an adapter</td>
<td>adpFAIDENTITYSERVICEPREPOPULATEEXTERNALADAPTER</td>
</tr>
<tr>
<td>Remove a role</td>
<td>adpFAIDENTITYSERVICEREMOVEROLE</td>
</tr>
<tr>
<td>Update a role</td>
<td>adpFAIDENTITYSERVICEUPDATEROLE</td>
</tr>
<tr>
<td>Update a user</td>
<td>adpFAIDENTITYSERVICEUPDATEUSER</td>
</tr>
<tr>
<td>Complete a task</td>
<td>adpFATCOMPLETETASK</td>
</tr>
<tr>
<td>Trigger, create, or link an account</td>
<td>adpTRIGGERCREATEORLINKFAACCOUNT</td>
</tr>
</tbody>
</table>

1.9.2 User Fields for Provisioning

The Lookup.FAIdentityService.UM.ProvAttrMap lookup definition maps process form fields with target system attributes. This lookup definition is used for performing user provisioning operations.

Table 1-10 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-10  Entries in the Lookup.FAIdentityService.UM.ProvAttrMap lookup definition

<table>
<thead>
<tr>
<th>Code</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisplayName</td>
<td>displayName</td>
</tr>
<tr>
<td>Email</td>
<td>emails.value</td>
</tr>
<tr>
<td>External Id</td>
<td>externalId</td>
</tr>
<tr>
<td>Family Name</td>
<td>name.familyName</td>
</tr>
<tr>
<td>Given Name</td>
<td>name.givenName</td>
</tr>
<tr>
<td>Id</td>
<td><em>UID</em></td>
</tr>
<tr>
<td>Preferred Language</td>
<td>preferredLanguage</td>
</tr>
<tr>
<td>User Name</td>
<td><em>NAME</em></td>
</tr>
</tbody>
</table>

1.10 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Deploying the Fusion Apps Connector describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
• **Using the Fusion Apps Connector** describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.

• **Extending the Functionality of the Fusion Apps Connector** describes procedures that you can perform if you want to extend the functionality of the connector.

• **Files and Directories on the Fusion Apps Connector Installation Media** lists the files and directories that comprise the connector installation media.
Deploying the Fusion Apps Connector

The procedure to deploy the connector is divided across three stages namely preinstallation, installation, and postinstallation.

The following topics provide details on these stages:

- Preinstallation
- Installation
- Postinstallation
- Upgrading the Connector

2.1 Preinstallation

Preinstallation for the Fusion Apps connector involves performing a series of tasks on the target system.

Preinstallation involves the following tasks:

1. Copy the external code files by creating a directory named `FAPPS-RELEASE NUMBER` under the `OIM_HOME/server/ConnectorDefaultDirectory/targetsystems-lib/directory`.
   
   For example, if you are using release 11.1.1.5.0 of this connector, then create a directory named `FAAPPS-11.1.1.5.0` in the `OIM_HOME/server/ConnectorDefaultDirectory/targetsystems-lib/directory`.

2. Install the Flat File Connector Release 11.1.1.5.0 from the `FMW_HOME/connectors/flat_file` directory.
   See Installation in Oracle Identity Manager Connector Guide for Flat File.

3. Configure the Flat File Connector IT Resource. To do so:
   a. Ensure that you have been assigned an FA service account with the ORA_FND_IT_SECURITY_MANAGER_JOB role. This role is required for both FA Identity Service and FA User Request Service.
   b. Edit the Flat File Users IT resource.
   c. From the View IT Resource Details and Parameters window, for the schemaFile parameter, enter the absolute path of the Flat File schema file.

   Sample value: `/scratch/shahas/flatfile/schema/FlatFileSchema.txt`

4. Update the Lookup.FlatFile.UM.Configuration lookup definition by setting the decode value as follows:
2.2 Installation

You must install the connector in Oracle Identity Manager. If necessary, you can also deploy the connector in a Connector Server.

The following topics provide details on installing the Fusion Apps connector:

- Understanding Installation of the Fusion Apps Connector
- Running the Connector Installer
- Configuring the IT Resource for the Target System

2.2.1 Understanding Installation of the Fusion Apps Connector

You can run the connector code either locally in Oracle Identity Manager or remotely in a Connector Server.

Depending on where you want to run the connector code (bundle), the connector provides the following installation options:

- Run the connector code locally in Oracle Identity Manager. In this scenario, you deploy the connector in Oracle Identity Manager. Deploying the connector in Oracle Identity Manager involves performing the procedures described in Running the Connector Installer and Configuring the IT Resource for the Target System.

- Run the connector code remotely in a Connector Server. In this scenario, you deploy the connector in Oracle Identity Manager, and then, deploy the connector bundle in a Connector Server. See Using an Identity Connector Server in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager for information about installing, configuring, and running the Connector Server, and then installing the connector in a Connector Server.

2.2.2 Running the Connector Installer

When you run the Connector Installer, it automatically copies the connector files to directories in Oracle Identity Manager, imports connector XML files, and compiles adapters used for provisioning.

To run the Connector Installer, perform the following procedure:

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

   \OIM_HOME\server\ConnectorDefaultDirectory

2. Log in to Oracle Identity System Administration.

3. In the left pane, under Provisioning Configuration, click Manage Connector.

4. In the Manage Connector page, click Install.

5. From the Connector List list, select Fusion Apps Connector RELEASE_NUMBER. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory: \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.
To repopulate the list of connectors in the Connector List list, click **Refresh**.

From the Connector List list, select **Fusion Apps Connector RELEASE_NUMBER**.

6. Click **Load**.

7. To start the installation process, click **Continue**. In a sequence, the following tasks are automatically performed:
   a. Connector library configuration.
   b. Import of the connector XML files (by using the Deployment Manager).
   c. Adapter compilation.

On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark along with a message stating the reason for failure is displayed. If a task fails, then make the required correction and perform one of the following steps:
   a. Retry the installation by clicking **Retry**.
   b. Cancel the installation and begin the procedure from Step 3.

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

9. Click **Exit** to close the installation page.

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 **Files and Directories on the Fusion Apps Connector Installation Media**.

### 2.2.3 Configuring the IT Resource for the Target System

An IT resource for your target system is created after you install the connector. You configure this IT resource to let the connector connect Oracle Identity Manager with your target system.

This section provides information about the following topics:

- **IT Resource Parameters**
- **Specifying Values for the IT Resource Parameters**

#### 2.2.3.1 IT Resource Parameters

An IT resource is composed of parameters that store connection and other generic information about a target system. Oracle Identity Manager uses this information to connect to a specific installation or instance of your target system.

The list of IT resource parameters for this connector can be grouped into the following categories:

- **IT Resource Parameters for FA User Request Service**
- **IT Resource Parameters for FA Identity Service**

**Table 2-1** lists IT resource parameters for FA User Request Service and **Table 2-2** lists IT resource parameters for FA Identity Service.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Sample value</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Host name or IP address of the computer hosting the target system.</td>
<td>myhost.example.com</td>
</tr>
<tr>
<td>port</td>
<td>Port number at which the target system is listening.</td>
<td>10619</td>
</tr>
<tr>
<td>userRequestServiceUri</td>
<td>This parameter holds the uniform resource identifier for user request service API.</td>
<td>/hcmCoreApi/atomervlet/user/</td>
</tr>
<tr>
<td></td>
<td></td>
<td>userRequests</td>
</tr>
<tr>
<td>userName</td>
<td>This parameter is the user ID of the database user account that Oracle Identity Manager uses to connect to the target system.</td>
<td>HCM_INTEGRATION_HCM</td>
</tr>
<tr>
<td>password</td>
<td>This parameter is the password of the database user account that Oracle Identity Manager uses to connect to the target system.</td>
<td></td>
</tr>
<tr>
<td>proxyHost</td>
<td>Name of the proxy host used to connect to an external target system.</td>
<td>proxy.fusionapps.com</td>
</tr>
<tr>
<td>proxyPassword</td>
<td>Password of the proxy user ID of the target system user account that Oracle Identity Manager uses to connect to the target system.</td>
<td></td>
</tr>
<tr>
<td>proxyPort</td>
<td>Proxy port number.</td>
<td>80</td>
</tr>
<tr>
<td>proxyUsername</td>
<td>This parameter is the user ID of the proxy that is used to connect to the target system.</td>
<td></td>
</tr>
<tr>
<td>socketTimeout</td>
<td>This parameter sets the default socket timeout in milliseconds which is the timeout period for data waiting.</td>
<td></td>
</tr>
<tr>
<td>connectionTimeout</td>
<td>This parameter sets the timeout until a connection is established.</td>
<td></td>
</tr>
<tr>
<td>Configuration Lookup</td>
<td>Name of the lookup definition that stores configuration information used during reconciliation and provisioning operations.</td>
<td>Lookup.FAUserRequestService.Configuration.Trusted</td>
</tr>
</tbody>
</table>
### Table 2-1  (Cont.) IT Resource Parameters for FA User Request Service

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| sslEnabled  | Default value: False  
If the target system is SSL based, set the value of this parameter to 'true', else set to 'false'. After the value is set, perform the procedure mentioned in Configuring SSL for the Fusion Apps Connector in order to enable Oracle Identity Manager to setup SSL Handshake with the target system. |

### Table 2-2  IT Resource Parameters for FA Identity Service

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adminUser</td>
<td>Enter the user ID of the target system user account that you create for connector operations.</td>
</tr>
<tr>
<td>adminPassword</td>
<td>Enter the password of the target system user account that you create for connector operations.</td>
</tr>
</tbody>
</table>
| userEndPoint   | This parameter holds the end point URL used to perform operations on users.  
Sample value: /hcmCoreSetupApi/scim/Users                                                                                                       |
| roleEndPoint   | This parameter holds the end point URL used to add or remove users to or from a Role.  
Sample value: /hcmCoreSetupApi/scim.Roles                                                                                                      |
| userSchemaEndPoint | This parameter holds the endpoint URL used to get the user schema.  
Sample value: /hcmCoreSetupApi/scim/Schemas/urn:scim:schemas:core:2.0:User                                                                                                                   |
| Configuration Lookup | Name of the lookup definition that stores configuration information used during reconciliation and provisioning operations.  
Default value: Lookup.FAIdentityService.Configuration                                                                                          |
| Connector Server Name | This parameter holds the hostname of the machine where the connector server resides.                                                                                                                                  |
| proxyHost      | Name of the proxy host used to connect to an external target system.  
Sample value: proxy.fusionapps.com                                                                                                                                                                           |
| proxyPassword  | Password of the proxy user ID of the target system user account that Oracle Identity Manager uses to connect to the target system.  
Sample value: proxy.fusionapps.com                                                                                                                                                                           |
Table 2-2  (Cont.) IT Resource Parameters for FA Identity Service

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxyPort</td>
<td>Proxy port number.</td>
</tr>
<tr>
<td></td>
<td>Sample value: 80</td>
</tr>
<tr>
<td>proxyUsername</td>
<td>This parameter is the user ID of the proxy that is used to connect to the target system.</td>
</tr>
<tr>
<td>host</td>
<td>Host name or IP address of the computer hosting the target system.</td>
</tr>
<tr>
<td></td>
<td>Sample value: myhost.example.com</td>
</tr>
<tr>
<td>port</td>
<td>Port number at which the target system is listening.</td>
</tr>
<tr>
<td></td>
<td>Sample value: 10619</td>
</tr>
<tr>
<td>socketTimeout</td>
<td>This parameter sets the default socket timeout in milliseconds which is the timeout period for data waiting.</td>
</tr>
<tr>
<td>connectionTimeout</td>
<td>This parameter sets the timeout until a connection is established.</td>
</tr>
<tr>
<td>sslEnabled</td>
<td>Default value: False</td>
</tr>
</tbody>
</table>

If the target system is SSL based, set the value of this parameter to 'true', else set to 'false'. After the value is set, perform the procedure mentioned in Configuring SSL for the Fusion Apps Connector in order to enable Oracle Identity Manager to setup SSL Handshake with the target system.

2.2.3.2 Specifying Values for the IT Resource Parameters

The IT resource for the target system contains connection information about the target system. Oracle Identity Manager uses this information during provisioning and reconciliation.

The Fusion Apps IT resource is automatically created when you run the Connector Installer. You must specify values for the parameters of the IT resource. To specify values:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click IT Resource.
3. In the IT Resource Name field on the Manage IT Resource page, enter FA Identity Service or FA User Request Service and then click Search.
4. Click Edit for the IT resource.
5. From the list at the top of the page, select Details and Parameters.
7. To save the values, click Update.
2.3 Postinstallation

Postinstallation for the Fusion Apps connector involves configuring Oracle Identity Manager, enabling logging to track information about all connector events, and configuring SSL. It also involves performing some optional configurations such as localizing the user interface.

The postinstallation steps are divided across the following sections:

• Configuring Resource Object Dependency
• Configuring Oracle Identity Manager
• Updating Access Policies
• Process Task Updates
• Clearing Content Related to Connector Resource Bundles from the Server Cache
• Localizing Field Labels in UI Forms
• SSO Email ID propagation for FA Source of Truth with LDAP Sync
• Managing Logging for the Fusion Apps Connector
• Configuring SSL for the Fusion Apps Connector

2.3.1 Configuring Resource Object Dependency

To configure resource object dependency, perform the following procedure:

See Also:

If you are using the non LDAP Sync topology, install the required enterprise directory and configure the resource object dependency. If you are using any other topologies, do not perform the procedure mentioned here.

1. Log in to the Design Console.
2. Expand Resource Management, and then double-click Resource Objects.
3. In the Object Definition region, search for and specify FA User in the Name field.
4. Select the Depends On tab, and click Assign. A list of resource objects of the already installed connectors are displayed.
5. To configure and add the resource object, specify and double-click the resource object of the installed enterprise directory.
6. Click Save.

2.3.2 Configuring Oracle Identity Manager

You must create an UI form and an application instance for the resource against which you want to perform reconciliation and provisioning operations. In addition, you must run entitlement and catalog synchronization jobs.

These procedures are described in the following sections:
• Creating and Activating a Sandbox
• Creating a New UI Form
• Creating an Application Instance
• Upgrading User Form in Oracle Identity Manager
• Publishing a Sandbox
• Harvesting Entitlements and Sync Catalog
• Updating an Existing Application Instance with a New Form
• Updating an Application Instance

2.3.2.1 Creating and Activating a Sandbox

You must create and activate a sandbox to begin using the customization and form management features. You can then publish the sandbox to make the customizations available to other users.

See Creating a Sandbox and Activating and Deactivating a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.

2.3.2.2 Creating a New UI Form

See Creating Forms By Using the Form in Oracle Fusion Middleware Administering Oracle Identity Manager for instructions on creating a new UI form. While creating the UI form, ensure that you select the resource object corresponding to the Fusion Apps connector that you want to associate the form with. In addition, select the Generate Entitlement Forms check box.

2.3.2.3 Creating an Application Instance

Perform the following steps to create and application instance:

1. In the left pane of the System Administration console, under Configuration, click Application Instances. The Application Instances page is displayed.

2. From the Actions menu, select Create. Alternatively, click Create on the toolbar. The Create Application Instance page is displayed.

3. Specify values for the following fields:
   • Name: The name of the application instance.
   • Display Name: The display name of the application instance.
   • Description: A description of the application instance.
   • Resource Object: The resource object name. Click the search icon next to this field to search for and select the FA User.
   • IT Resource Instance: The IT resource instance name. Click the search icon next to this field to search for and select the name.
   • Form: Select the form name (created in Creating a New UI Form).

4. Click Save. The application instance is created.

5. Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See
2.3.2.4 Upgrading User Form in Oracle Identity Manager

This connector creates a new OIM user attribute (UDF) FA User GUID. Although this user attribute (UDF) is added to a new User Form version, the User Form from the old version is only used for all operations. To use the latest form version which contains the GUID field, you must customize the associated pages on the interface to upgrade to the latest User Form and add the custom form fields. To do so, perform the following procedure:

1. Log in to Oracle Identity System Administration.
2. From the Upgrade region, click Upgrade User Form. The FA User GUID UDF is listed.
3. Click Upgrade.

2.3.2.5 Publishing a Sandbox

Before publishing a sandbox, perform the following procedure as a best practice to validate all sandbox changes made till this stage as it is difficult to revert the changes after a sandbox is published:

1. In Identity System Administration, deactivate the sandbox.
2. Log out of Identity System Administration.
3. Log in to Identity Self Service using the xelsysadm user credentials and then activate the sandbox that you deactivated in Step 1.
4. In the Catalog, ensure that the Fusion Apps application instance form appears with correct fields.
5. Publish the sandbox. See Publishing a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.

2.3.2.6 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Scheduled Job for Lookup Field Synchronization for Fusion Apps Connector.
2. Run the Entitlement List scheduled job to populate the Entitlement Assignment schema from the child process form table.
3. Run the Catalog Synchronization Job scheduled job.

See Also:

Predefined Scheduled Tasks in Oracle Fusion Middleware Administering Oracle Identity Manager for a description of the Entitlement List and Catalog Synchronization Job scheduled jobs.
2.3.2.7 Updating an Existing Application Instance with a New Form

For any changes you do in the Form Designer, you must create a new UI form and update the changes in an application instance. To update an existing application instance with a new form:

1. Create a sandbox and activate it. See Creating a Sandbox and Activating and Deactivating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
2. Create a new UI form for the resource. See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
3. Open the existing application instance.
4. In the Form field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

2.3.2.8 Updating an Application Instance

You can update the application instance created for Fusion Apps by performing the procedure mentioned in Creating an Application Instance with the differences described in this section.

In Step 3 of the procedure, you must specify the following values:

- **Name**: FusionApps User
- **Display Name**: Fusion Apps User
- **Description**: Application instance for FusionApps
- **Resource Object**: FA User
- **IT Resource Instance**: FA Identity Service
- **Form**: Click on the drop-down list and select the form that you created for FA

In addition to the above parameters, you must provide a value for the **Parent AppInstance** parameter. To do so, you must click the search icon in the field and select the app instance created for the enterprise directory.

2.3.3 Updating Access Policies

Depending on the use case, update corresponding access policies.

Based on the use case that you are using, perform one of the procedures discussed in this section:

- **FA Source of Truth - Cloud or On-Premise Use Case**
- **HRMS or IDM Source of Truth - FA on Cloud or On-Premise Use Case**
- **FA and External HRMS Source of Truth - FA on Cloud or On-Premise Use Case**
- **FA Source of Truth With LDAP Sync - FA on Cloud or On-Premise Use Case**
2.3.3.1 FA Source of Truth - Cloud or On-Premise Use Case

If you are using the FA Source of Truth - Cloud or On-Premise use case, perform the following procedure:

1. Log in to Oracle Identity System Administration.
2. In the System Administration Console, click **Access Policies** under the Policies menu. The Manage Access Policies page is displayed.
3. Click **Search Access Policies**.
4. Enter FA Access Policy For FA User in the search field.
5. To view the details of this Access Policy, click on the search result. The Access Policy Details page is displayed.
6. To edit the Fusion Apps resource **FA User**, click the Edit link corresponding to the resource. A set of fields are displayed.
7. For all mandatory fields, you must provide values. Each mandatory field is marked by a asterisk (*) wildcard character. For example, you must enter FA identity service as the value for the mandatory field, **Service Instance**.
8. Add resources to be provisioned by this access policy corresponding to installed enterprise directory. To do so, click **Change**.
9. Click the Edit link to edit the newly added resource and provide values for all mandatory fields.
10. Click **Save**.
11. Click **Exit**.

2.3.3.2 HRMS or IDM Source of Truth - FA on Cloud or On-Premise Use Case

If you are using the HRMS or IDM Source of Truth - FA on Cloud or On-Premise use case, perform the following procedure:

1. Repeat steps 1 through 10 of **FA Source of Truth - Cloud or On-Premise Use Case** with the following difference:
   - While performing Step 4, instead of entering FA Access Policy For FA User, enter FA Access Policy For External User.
2. To update the user membership rule of the role **FA Role for External User**, navigate to the **Manage** region and select **Roles**.
3. Click **FA Role for External User**, and select **Members**.
4. Select the Edit link to edit the rule.
5. Click **Save** and then **Exit**.
2.3.3.3 FA and External HRMS Source of Truth - FA on Cloud or On-Premise Use Case

If you are using the FA and External HRMS Source of Truth - FA on Cloud or On-Premise use case, perform the following procedure:

1. Repeat steps 1 through 11 of FA Source of Truth - Cloud or On-Premise Use Case.
4. Repeat steps 5 through 11 of FA Source of Truth - Cloud or On-Premise Use Case.
5. To update the user membership rule of the role "FA Role for External User", navigate to the Manage region and select Roles.
6. Click FA Role for External User, and select Members.
7. Select the Edit link to edit the rule.
8. Click Save and then Exit.

2.3.3.4 FA Source of Truth With LDAP Sync - FA on Cloud or On-Premise Use Case

If you are using the FA Source of Truth With LDAP Sync - FA on Cloud or On-Premise use case, perform the following procedure:

1. Repeat steps 1 through 7 of FA Source of Truth - Cloud or On-Premise Use Case.
2. Click Save and then Exit.

2.3.3.5 External HRMS Source of Truth With LDAP Sync - FA on Cloud or On-Premise Use Case

If you are using the External HRMS Source of Truth With LDAP Sync - FA on Cloud or On-Premise use case, perform the following procedure:

1. Repeat steps 1 through 7 of FA Source of Truth - Cloud or On-Premise Use Case with the following difference:
   While performing Step 4, instead of entering FA Access Policy For FA User, enter FA Access Policy For External User.
2. To update the user membership rule of the role FA Role for External User, navigate to the Manage region and select Roles.
3. Click FA Role for External User, and select Members.
4. Select the Edit link to edit the rule.
5. Click Save and then Exit.
2.3.3.6 FA and External HRMS Source of Truth With LDAP Sync - FA on Cloud or On-Premise Use Case

If you are using the FA and External HRMS Source of Truth With LDAP Sync - FA on Cloud or On-Premise use case, perform the following procedure:

1. Repeat steps 1 through 7 of FA Source of Truth - Cloud or On-Premise Use Case.
2. Click **Save** and then **Exit**.
3. Reopen the Manage Access Policies page and click **Search Access Policies**.
4. Enter **FA Access Policy For External User** in the search field.
5. Repeat steps 5 through 11 of FA Source of Truth - Cloud or On-Premise Use Case.
6. To update the user membership rule of the role **FA Role for External User**, navigate to the **Manage** region and select **Roles**.
7. Click **FA Role for External User**, and select **Members**.
8. Select the Edit link to edit the rule.
9. Click **Save** and then **Exit**.

2.3.4 Process Task Updates

To update process tasks, you must first create a new task for the process definition form of the enterprise directory being used.

To do so, perform the following procedure:

---

**Note:**

Perform the steps mentioned in this section only if Oracle Identity Manager is in non LDAP Sync mode.

1. Log in to the Design Console.
2. Expand **Process Management**, and then double-click **Process Definition**.
3. Open the process definition for FA User.
4. Select the **Tasks** tab.
5. Click **Add**. The Creating New Task dialog box is displayed.
6. In the Task Name field, enter the name of the process task.
7. From the Integration tab select **CopyProcessFormData** system adapter.
8. From the Toolbar of the Creating New Task window, click **Save**.
9. Select the following check boxes:
   - Conditional
   - Allow Multiple Instances
   - Allow Cancellation While Pending
10. Click Save and then Exit.

11. Add this newly created task to the SUCCESS response of tasks Create FA Account and Link FA Account.

12. Click Save and then Exit.

You must update the process definition for the installed enterprise directory. To do so, perform the following procedure:

1. Log in to the Design Console.
2. Expand Process Management, and then double-click Process Definition.
3. Open the process definition for the installed enterprise directory.
4. Select the Tasks tab.
5. In the Task Name field, enter the name of the process task.
6. From the Integration tab select UpdateDepProcessFormData system adapter.
7. From the Toolbar of the Creating New Task window, click Save.
8. Select the following check boxes:
   - Conditional
   - Allow Multiple Instances
   - Allow Cancellation While Pending
9. Click Save and then Exit.
10. Add this newly created task to the SUCCESS response of tasks responsible for email id update.
11. Click Save and then Exit.

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

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.
2. Enter one of the following commands:
   - On Microsoft Windows: PurgeCache.bat All
   - On UNIX: PurgeCache.sh All
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.

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.

2.3.6 Localizing Field Labels in UI Forms

You can localize UI form field labels by using the resource bundle corresponding to the language you want to use. Resource bundles are available in the connector installation media.

To localize a field label that is added to the UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand Application Deployments and then select `oracle.iam.console.identity.sysadmin.ear`.
3. In the right pane, from the Application Deployment list, select `MDS Configuration`.
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:
   
   `SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en_US.xlf`

6. Edit the BizEditorBundle_en_US.xlf file in the following manner:

   a. Search for the following text:

   ```xml
   <file source-language="en" original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle_en_US" datatype="x-oracle-adf">
   ```

   b. Replace with the following text:

   ```xml
   <file source-language="en" target-language="LANG_CODE" original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle_en_US" datatype="x-oracle-adf">
   ```
In this text, replace `LANG_CODE` with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

```xml
<file source-language="en" target-language="ja" original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle_en_US" datatype="x-oracle-adf">

c. Search for the application instance code. This procedure shows a sample edit for Fusion Apps application instance. The original code is:

```xml
<trans-unit id="${adfBundle["oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle"]['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_Fusion Apps_LOGIN__c_description']]">  
<source>Login</source>  
<target/>
</trans-unit>
<trans-unit id="sessiondef.oracle.iam.ui.runtime.form.model.FusionAppsForm.entity.FusionAppsFormEO.UD_Fusion Apps_LOGIN__c_LABEL">  
<source>Login</source>  
<target/>
</trans-unit>
```

```xml
d. Open the resource file from the connector package, for example FusionApps_ja.properties, and get the value of the attribute from the file, for example, global.udf.UD_Fusion Apps_LOGIN=\u30ED\u30B0\u30A4\u30F3

e. Replace the original code shown in Step 6.c with the following:

```xml
<trans-unit id="${adfBundle["oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle"]['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_Fusion Apps_LOGIN__c_description']]">  
<source>Login</source>  
<target>\u30ED\u30B0\u30A4\u30F3</target>
</trans-unit>
<trans-unit id="sessiondef.oracle.iam.ui.runtime.form.model.FusionAppsForm.entity.FusionAppsFormEO.UD_Fusion Apps_LOGIN__c_LABEL">  
<source>Login</source>  
<target>\u30ED\u30B0\u30A4\u30F3</target>
</trans-unit>
```

```
f. Repeat Steps 6.a through 6.d for all attributes of the process form.

g. Save the file as BizEditorBundle_LANG_CODE.xlf. In this file name, replace `LANG_CODE` with the code of the language to which you are localizing. Sample file name: BizEditorBundle_ja.xlf.

7. Repackage the ZIP file and import it into MDS.
8. Log out of and log in to Oracle Identity Manager.

2.3.7 SSO Email ID propagation for FA Source of Truth with LDAP Sync

To propagate SSO email ID, perform the following procedure:

1. Create a new adapter by performing the following steps:
   a. Log in to the Design Console.
   b. Expand Development Tools, and then double-click Adapter Factory.
   c. Create a new adapter by entering the following values:
      • In the Adapter Name field, enter CopySSOEmailToProcessForm.
      • Double-click the Adapter Type lookup field. The Lookup window is displayed, displaying the five types of Oracle Identity Manager adapters.
      • Select Process Task. Click OK.
      • In the Description field, enter Copy FA User Email to Process Task.
   d. Click the Save icon and close the dialog box.
   e. On the Variables List tab, add the inputVariable variable as follows:
      i. Click Add.
      ii. In the Add a Variable dialog box, enter the following values:
         • Variable Name: inputVariable
         • Type: String
         • Map To: Resolve at runtime
      iii. Within the Description text area, you can enter explanatory information about the adapter variable.
   f. Click Save and close the dialog box.
   g. On the Adapter Task tab, perform the following steps:
      i. Click Add. The Adapter Task Selection window is displayed.
      ii. Select the Logic Task option.
      iii. From the display area, select SET VARIABLE, and click Continue. The Add Set Variable Task Parameters window is displayed.
      iv. From the Variable Name list, select the adapter variable that has a value you want to reassign—for example, Adapter return value.
      v. From the Operand Type list, select the type and qualifier of operand as follows:
2. Create a new process task for the process definition FA User be performing the following steps:

   a. Log in to the Design Console.
   b. Expand **Process Management**, and then double-click **Process Definition**.
   c. Open the process definition for FA User and select the **Tasks** tab.
   d. Click **Add**. The Creating New Task dialog box is displayed.
   e. Enter the following values for the below variables:
      - In the Task Name field, enter **CopyEmailToProcessForm**.
      - Select the following check boxes:
         - Conditional
         - Allow Cancellation while Pending
         - Allow Multiple Instances
      - Click **Save**.
      - In the Integration tab, enter values by performing the following procedure:
         - Click **Add**.
         - In the field named Handler Type, select **Adapter**.
         - From the drop-down list item, select **adpCopySSOEmailToProcessForm** and click **Save**.
         - Double click on the mapping for **Adapter return value** option.
         - To perform the mapping process, map Map To with Process Data and Qualifier with Email.
         - Click **Save** and **Exit**.
         - Double click on the mapping for **inputValue** option.
         - To perform the mapping process, map Map To with User Definition and Qualifier with Email.
         - Click **Save** and **Exit**.
   f. Click **Save** and then **Exit**.

3. Add this newly created task to the SUCCESS response of tasks Create FA Account and Link FA Account by performing the following steps:

   a. Open the window for the Create FA Account task. Click the **Responses** tab and select the **SUCCESS** response.
   b. Click **Assign** and assign the task name **CopyEmailToProcessForm**.
   c. Click **Save**.
   d. Perform Steps 3.a through 3.c with the following changes:
      - Open the window for the Link FA Account task instead of Create FA Account task.
• In step 3.b, assign the task name as CopyEmailToProcessForm for the Link FA Account task instead of Create FA Account task.

4. Remove the Email field from the Pre-Populate form in the UD_FAUSER table by performing the following steps:
   a. Expand Development Tools, and then click Form Designer.
   b. Click the search icon next to this field to search for and select the table name UD_FAUSER.
   c. Select the Pre-populate tab and click Create new version.
   d. Remove the email field and click Make version active.
   e. Click Save and Exit.

2.3.8 Managing Logging for the Fusion Apps Connector

Oracle Identity Manager uses Oracle Diagnostic Logging (ODL) logging service for recording all types of events pertaining to the connector.

The following topics provide detailed information about logging:

• Understanding Log Levels
• Enabling Logging

2.3.8.1 Understanding Log Levels

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

ODL is the principle logging service used by Oracle Identity Manager and 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 Manager 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 2-3.

**Table 2-3 Log Levels and ODL Message Type:Level Combinations**

<table>
<thead>
<tr>
<th>Java Level</th>
<th>ODL Message Type:Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEVERE.intValue()+100</td>
<td>INCIDENT_ERROR:1</td>
</tr>
<tr>
<td>SEVERE</td>
<td>ERROR:1</td>
</tr>
<tr>
<td>WARNING</td>
<td>WARNING:1</td>
</tr>
<tr>
<td>INFO</td>
<td>NOTIFICATION:1</td>
</tr>
<tr>
<td>CONFIG</td>
<td>NOTIFICATION:16</td>
</tr>
<tr>
<td>FINE</td>
<td>TRACE:1</td>
</tr>
<tr>
<td>FINER</td>
<td>TRACE16</td>
</tr>
<tr>
<td>FINEST</td>
<td>TRACE32</td>
</tr>
</tbody>
</table>

The configuration file for OJDL is logging.xml is located at the following path: 
`DOMAIN_HOME/config/fmwconfig/servers/OIM_SERVER/logging.xml`

Here, `DOMAIN_HOME` and `OIM_SERVER` are the domain and server names specified during the installation of Oracle Identity Manager.

### 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:

   ```xml
   <log_handler name='fusionapps-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='ORG.IDENTITYCONNECTORS.FAUSERREQUESTSERVICE' level='[LOG_LEVEL]' useParentHandlers="false">
     <handler name='fusionapps-handler'/>
     <handler name='console-handler'/>
   </logger><logger name='ORG.IDENTITYCONNECTORS.FAIDENTITYSERVICE' level='[LOG_LEVEL]' useParentHandlers="false">
     <handler name='fusionapps-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 2-3 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="fusionapps-handler" level="TRACE:32"
            class="oracle.core.ojdl.logging.ODLHandlerFactory">
  <property name="logreader" value="off"/>
  <property name="path" value="/scratch/RSA/Logs/arimitra/fa.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="ORG.IDENTITYCONNECTORS.FAUSERREQUESTSERVICE"
        level="TRACE:32" useParentHandlers="false">
  <handler name="fusionapps-handler"/>
  <handler name="console-handler"/>
</logger>

<logger name="ORG.IDENTITYCONNECTORS.FAIDENTITYSERVICE"
        level="TRACE:32" useParentHandlers="false">
  <handler name="fusionapps-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 TRACE:32 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 SSL for the Fusion Apps Connector

Configure SSL to secure data communication between Oracle Identity Manager and the target system.
1. Obtain the SSL certificate by obtaining the public key certificate of the target system.
2. Copy the public key certificate of the target system to the computer hosting Oracle Identity Manager.
3. Run the following keytool command to import the public key certificate into the identity key store in Oracle Identity Manager:

```
keytool -import -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks -file CERT_FILE_NAME -storepass PASSWORD
```

In this command:

- `CERT_FILE_NAME` is the full path and name of the certificate file
- `PASSWORD` is the password of the keystore.

The following is a sample value for this command:

```
keytool -import -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks -file /home/target.cert -storepass DemoTrustKeyStorePassPhrase
```

**Note:**

Change the parameter values passed to the keytool command according to your requirements. Ensure that there is no line break in the keytool arguments.

### 2.4 Upgrading the Connector

This is the first release of the Oracle Identity Manager connector for Fusion Apps. Therefore, the connector cannot be upgraded.
3

Using the Fusion Apps Connector

You can use the connector for performing reconciliation and provisioning operations after configuring it to meet your requirements.

This chapter contains the following topics:

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.

- Scheduled Job for Lookup Field Synchronization for Fusion Apps Connector
- Configuring Reconciliation for Fusion Apps Connector
- Configuring Scheduled Jobs
- Performing Provisioning Operations
- Uninstalling the Fusion Apps Connector

3.1 Scheduled Job for Lookup Field Synchronization for Fusion Apps Connector

Scheduled jobs for lookup field synchronization fetch the most recent values from specific fields in the target system to lookup definitions in Oracle Identity Manager. These lookup definitions are used as an input source for lookup fields in Oracle Identity Manager.

The FA Identity Service Application Roles Lookup Reconciliation scheduled job is used for lookup fields synchronization. The values that are fetched by this scheduled job are populated in the Lookup.FAIdentityService.ApplicationRoles lookup definition.

Table 3-1 describes attributes of the FA Identity Service Application Roles Lookup Reconciliation scheduled job. The procedure to configure scheduled jobs is described later in this guide.
Table 3-1 Attributes of the FA Identity Service Application Roles Lookup Reconciliation Scheduled Job

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Key Attribute</td>
<td>Name of the connector attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: <strong>UID</strong></td>
</tr>
<tr>
<td>Decode Attribute</td>
<td>Name of the connector attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: <em>NAME</em></td>
</tr>
<tr>
<td>IT Resource Name</td>
<td>Name of the IT resource for the target system installation from which you want reconcile user records. Default value: FA Identity Service</td>
</tr>
<tr>
<td>Lookup Name</td>
<td>Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. Default value: Lookup.FAIdentityService.Application Roles</td>
</tr>
<tr>
<td>Object Type</td>
<td>This attribute is used to perform reconciliation of specified object type. As per the scheduled job, select the applicable object type. Default value: ApplicationRole</td>
</tr>
</tbody>
</table>

3.2 Configuring Reconciliation for Fusion Apps Connector

You can configure the connector to specify the type of reconciliation and its schedule.

This section provides details on the following topics related to configuring reconciliation:

- Full Reconciliation for Fusion Apps Connector
- Limited Reconciliation for Fusion Apps Connector
- Batched Reconciliation for Fusion Apps Connector
- Reconciliation Scheduled Jobs for Fusion Apps Connector

3.2.1 Full Reconciliation for Fusion Apps Connector

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. Since, initial bootstrap loading of all existing Fusion Apps users might be a time and resource intensive process, we recommend exporting all the users from Fusion Apps system...
into a Flat File in the .csv format, and then using the Flat File connector to load these users into Oracle Identity Manager offline. To do so, perform the procedures mentioned below:

- Export Users from the Fusion Apps Target System
- Use Flat File Connector to Load Exported Users

### 3.2.1.1 Export Users from the Fusion Apps Target System

To export users from the Fusion Apps target system:

1. Login to Oracle BI Publisher.
2. Click on Catalog and navigate to the following path:
   
   /Shared Folders/Human Capital Management/Workforce Management/Human Resources Dashboard/Data Models/User Information

3. From the left pane, select FusionUserInformation and click the Edit icon.
4. Take a backup of the original query.
5. Use the following 2 queries consecutively to export Person & Party Users and Standalone Users respectively:
   - For Person and Party Users:
     ```sql
     SELECT u.user_guid as id, u.username as username, n.last_name as first_name, n.first_name as last_name, e.email_address as email
     FROM fusion.per_person_names_f n, fusion.per_email_addresses e, fusion.per_all_people_f f, fusion.per_users u
     WHERE TRUNC(sysdate) BETWEEN n.effective_start_date AND n.effective_end_date
     AND n.name_type = 'GLOBAL'
     AND TRUNC(sysdate) BETWEEN f.effective_start_date AND f.effective_end_date
     AND f.person_id = n.person_id
     AND e.person_id (+) = f.person_id
     AND e.email_type (+) = 'W1'
     AND e.email_address_id (+) = f.primary_email_id
     ```
AND u.person_id = f.person_id
AND u.active_flag = 'Y'

– TCA
 UNION
 SELECT
 u.user_guid as id,
 u.username as username,
 p.PERSON_LAST_NAME as first_name,
 p.PERSON_FIRST_NAME as last_name,
 c.email_address as email
 FROM
 fusion.hz_person_profiles p,
 fusion.hz_contact_points c,
 fusion.per_users u
 WHERE
 u.party_id = p.party_id
 AND p.party_id = c.OWNER_TABLE_ID(+)
 AND TRUNC(sysdate) between p.EFFECTIVE_START_DATE and
 p.EFFECTIVE_END_DATE
 AND p.status = 'A'
 AND c.OWNER_TABLE_NAME(+) = 'HZ_PARTIES'
 AND TRUNC(sysdate) between c.START_DATE(+) AND c.END_DATE(+)
 AND c.OVERALL_PRIMARY_FLAG(+) = 'Y'
 AND c.CONTACT_POINT_TYPE(+) = 'EMAIL'
 AND c.status(+) = 'A'
 AND u.active_flag = 'Y'
 ORDER BY "USERNAME"

• For Standalone Users:
 StandAlone
 SELECT
 u.user_guid as id,
 username as username
 from
 per_users u
 where
 person_id is null
 and party_id is null
AND u.active_flag = 'Y'
ORDER BY "USERNAME"

6. Click Save and run the report.

7. Export each of these to 2 different csv Flat Files. To do so, click Settings, Export and select Use flat file connector to load the exported users to csv.

3.2.1.2 Use Flat File Connector to Load Exported Users

To use the Flat File connector to load exported users, perform the procedures mentioned below:

- Modifying Exported CSV Files
- Configuring and Using the Flat File Connector
- Updating the SyncToken for Incremental Recon

3.2.1.2.1 Modifying Exported CSV Files

You must modify the exported CSV files as required by the Flat File connector. The Flat file connector expects the CSV file headers to have the same column names as the target field names i.e. names as they appear in the Fusion Apps ATOM feed. Since all flat files exported in previous step have different column names, you must change the header of both the files, by replacing the existing names with the correct names as mentioned in Table 3-2.

<table>
<thead>
<tr>
<th>Existing Name in Exported File</th>
<th>Correct Name/ Target Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>user.id</td>
</tr>
<tr>
<td>username</td>
<td>user.userName</td>
</tr>
<tr>
<td>first_name</td>
<td>user.name.givenName</td>
</tr>
<tr>
<td>last_name</td>
<td>user.name.familyName</td>
</tr>
<tr>
<td>email</td>
<td>user.emails.value</td>
</tr>
</tbody>
</table>

For example, if the header name is username, id, first_name, last_name, email, it should be changed to user.userName, user.id, user.name.givenName, user.name.familyName, user.emails.value.

3.2.1.2.2 Configuring and Using the Flat File Connector

To configure and use the Flat File connector:

Note:

You must perform the following configurations at the minimum to use the connector.
1. Modify the Flat File Users IT Resource to point to the correct trusted main configuration lookup (Lookup.FlatFile.Configuration.Trusted) and schema file location. See Creating a Schema File in Oracle Identity Manager Connector Guide for Flat File.

2. Modify the Flat File User configuration lookup Lookup.FlatFile.UM.Configuration.Trusted to point to the reconciliation attribute map of UserRequestService which is Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted and reconciliation attribute defaults which is Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults. Additionally, edit the reconciliation attribute defaults lookup to add a default value for Surname since Standalone Users in Flat File does not contain a surname field.

3. Run the Flat File Users Loader scheduled job. To run the Flat File Users Loader scheduled job, perform the procedure mentioned below:

   a. Open the Job Details page of the Flat File Users Loader scheduled job.
   b. Update values for the following fields present in the Parameters region:
      - Flat File directory - Location of the csv files exported in Export Users from the Fusion Apps Target System. For example: /scratch/fa/flatfile/data
      - Target IT Resource Name: FA User Request Service
      - Target Resource Object Name: FA User Trusted
   c. Click Apply and run the scheduled job to load all the users into Oracle Identity Manager.

3.2.1.2.3 Updating the SyncToken for Incremental Recon

After all the users are created in Oracle Identity Manager and their successful FA Identity Service accounts are provisioned, hit the ATOM end point of Fusion Apps target system using any REST client. Look at the first ATOM pub entry and fetch the updated datetime value.

For example, `<updated>2016-05-10T08:36:30.000Z</updated>` for the first record means that the record was updated last at **2016-05-10T08:36:30.000Z**. This also means that this is the time when the latest update was done on the Fusion Apps target system.

Copy this value to the FA User Request Service Trusted User Reconciliation scheduled job in the Sync Token parameter along with pre-fixing and post-fixing `<String>` and `</String>` respectively.

For example, `<updated>2016-05-10T08:36:30.000Z</updated>` should be changed to `<String>2016-05-10T08:36:30.000Z</String>` while copying to the Sync Token parameter.
This will ensure that when you run the FA User Request Service Trusted User Reconciliation scheduled job, only records created or modified after this time stamp are considered for reconciliation. This is incremental reconciliation.

3.2.2 Limited Reconciliation for Fusion Apps Connector

Limited or filtered reconciliation is the process of limiting the number of records being reconciled based on a set filter criteria.

By default, all target system records are reconciled during the current reconciliation run. You can customize this process by specifying the subset of target system records that must be reconciled. You do this by creating filters for the reconciliation module.

You can perform limited reconciliation by creating filters for the reconciliation module. This connector provides a filter attribute that supports ICF filters (a scheduled task attribute) allowing you to use any of the Fusion Apps resource attributes to filter the target system records.

See ICF Filter Syntax in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.

Note:
The __UID__ attribute name can only be used with the equalTo filter.

FA User Request service does not support limited reconciliation as the searchOp feature is not supported. However, this operation is performed by FA Identity service using filters.

3.2.3 Batched Reconciliation for Fusion Apps Connector

FA User Request service and FA Identity service supports batching. By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run.

Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete. You can configure batched reconciliation to avoid such problems.

FA Identity service exposes only the Batch Size attribute to the users in the scheduled job. To configure batched reconciliation, specify values for the Batch Size attribute while performing the procedure described in the Scheduled Jobs for Reconciliation of User Records.

Batch Size is an attribute used to specify the number of records that must be included in each batch. If you set the value of this attribute to 0, then the defaultbatchsize entry of the main configuration lookup is considered as the batch size for batched reconciliation. Any numeric value other than 0 takes precedence over the defaultbatchsize entry.
3.2.4 Reconciliation Scheduled Jobs for Fusion Apps Connector

When you run the Connector Installer, reconciliation scheduled jobs are automatically created in Oracle Identity Manager. You must configure these scheduled jobs to suit your requirements by specifying values for its attributes.

This section discusses the following scheduled jobs that you can configure for reconciliation:

- Scheduled Jobs for Reconciliation of User Records
- Scheduled Job for Reconciliation of Deleted Users Records

3.2.4.1 Scheduled Jobs for Reconciliation of User Records

Depending on whether you want to implement trusted source or target resource reconciliation, you must specify values for the attributes of one of the following user reconciliation scheduled jobs:

- Fusion Apps User Target Reconciliation (FA Identity Service User Reconciliation)
  This scheduled job is used to reconcile user data in the target resource (account management) mode of the connector.

- Fusion Apps User Trusted Reconciliation (FA User Request Service Trusted User Reconciliation)
  This scheduled job is used to reconcile user data in the trusted source (identity management) mode of the connector.

Table 3-3 and Table 3-4 describes the attributes of both the scheduled jobs.

**Table 3-3 Attributes of the Scheduled Jobs for Reconciliation of User Records for FA User Request Service**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch Size</td>
<td>Enter the number of records that must be included in each batch fetched from the target system.</td>
</tr>
<tr>
<td></td>
<td>Default value: 0</td>
</tr>
<tr>
<td>IT Resource Name</td>
<td>Enter the name of the IT resource for the target system installation from where the connector must reconcile data.</td>
</tr>
<tr>
<td></td>
<td>If you are running the FA User Request Service Trusted User Reconciliation scheduled job, then enter the name of the IT resource instance that you create for trusted source reconciliation in Configuring the IT Resource for the Target System.</td>
</tr>
<tr>
<td></td>
<td>Default value: FA User Request Service</td>
</tr>
<tr>
<td>Object Type</td>
<td>This attribute holds the name of the object type for the reconciliation run.</td>
</tr>
<tr>
<td></td>
<td>Default value: User</td>
</tr>
<tr>
<td></td>
<td>Do not change the default value.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Resource Object Name</td>
<td>This attribute holds the name of the resource object used for reconciliation.</td>
</tr>
<tr>
<td></td>
<td>Default value: FA User Trusted</td>
</tr>
<tr>
<td></td>
<td>Do not change the default value.</td>
</tr>
<tr>
<td>Scheduled Task Name</td>
<td>Name of the scheduled task used for reconciliation.</td>
</tr>
<tr>
<td></td>
<td>Default value: FA User Request Service</td>
</tr>
<tr>
<td></td>
<td>Trusted User Reconciliation</td>
</tr>
<tr>
<td>Sync Token</td>
<td>This attribute holds the value of the updated timestamp of the ATOM entry.</td>
</tr>
<tr>
<td></td>
<td>Sample value: &lt;String&gt;2015-02-10T10:39:22.000Z&lt;/String&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch Size</td>
<td>Enter the number of records that must be included in each batch fetched from the target system.</td>
</tr>
<tr>
<td></td>
<td>Default value: 0</td>
</tr>
<tr>
<td>Filter</td>
<td>Enter the expression for filtering records. Use the following syntax:</td>
</tr>
<tr>
<td></td>
<td>syntax = expression ( operator expression )*</td>
</tr>
<tr>
<td></td>
<td>perator = 'and'</td>
</tr>
<tr>
<td></td>
<td>expression = ( 'not' )? filter</td>
</tr>
<tr>
<td></td>
<td>filter = ('equalTo'</td>
</tr>
<tr>
<td></td>
<td>'startsWith'</td>
</tr>
<tr>
<td></td>
<td>'lessThan'</td>
</tr>
<tr>
<td></td>
<td>'attributeName'</td>
</tr>
<tr>
<td></td>
<td>attributeValue = singleValue</td>
</tr>
<tr>
<td></td>
<td>singleValue = 'value'</td>
</tr>
</tbody>
</table>
|               | 'value_n']]* ']'

Default value: None
Table 3-4  (Cont.) Attributes of the Scheduled Jobs for Reconciliation of User Records for FA Identity Service

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incremental Recon Attribute</td>
<td>Attribute that holds the date on which the token record was modified.</td>
</tr>
<tr>
<td>IT Resource Name</td>
<td>Enter the name of the IT resource for the target system installation from where the connector must reconcile data. If you are running the FA User Request Service Trusted User Reconciliation scheduled job, then enter the name of the IT resource instance that you create for trusted source reconciliation in Configuring the IT Resource for the Target System. Default value: FA Identity Service</td>
</tr>
<tr>
<td>Latest Token</td>
<td>This attribute holds the value of the attribute that is specified as the value of the Incremental Recon Attribute. The Latest Token attribute is used for internal purposes. By default, this value is empty. Do not enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute. Sample value: 1354753427000</td>
</tr>
<tr>
<td>Object Type</td>
<td>This attribute holds the name of the object type for the reconciliation run. Default value: User Do not change the default value.</td>
</tr>
<tr>
<td>Resource Object Name</td>
<td>This attribute holds the name of the resource object used for reconciliation. Default value: FA Identity Do not change the default value.</td>
</tr>
<tr>
<td>Scheduled Task Name</td>
<td>Name of the scheduled task used for reconciliation. Default value: FA Identity Service User Reconciliation</td>
</tr>
</tbody>
</table>

3.2.4.2 Scheduled Job for Reconciliation of Deleted Users Records

To perform FA Identity Service user delete reconciliation, you must specify values for Fusion Apps User Delete Reconciliation scheduled job. This scheduled job is used to reconcile data about deleted users in the trusted source (identity management) mode of the connector. During a reconciliation run, for each deleted target system user account, the corresponding OIM User is deleted.

Table 3-5 describes attributes of both scheduled jobs.
### Table 3-5  Attributes of the Scheduled Job for Delete User Reconciliation

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Resource Name</td>
<td>Enter the name of the IT resource instance that the connector must use to reconcile user data. Default value: FA Identity Service</td>
</tr>
<tr>
<td>Object Type</td>
<td>This attribute holds the name of the object type for the reconciliation run. Default value: User Do not change the default value.</td>
</tr>
<tr>
<td>Resource Object Name</td>
<td>This attribute holds the name of the resource object used for reconciliation. Default value: FA User Do not change the default value.</td>
</tr>
</tbody>
</table>

### 3.3 Configuring Scheduled Jobs

Configure scheduled jobs to perform reconciliation runs that check for new information on your target system periodically and replicates the data in Oracle Identity Manager.

You can apply this procedure to configure the scheduled jobs for lookup field synchronization and reconciliation.

To configure a scheduled job:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled job as follows:
   a. 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.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the parameters of the scheduled task:
   - **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.
In addition to modifying the job details, you can enable or disable a job.

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

**Note:**
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.
- See Reconciliation Scheduled Jobs for Fusion Apps Connector for the list of scheduled tasks and their attributes.

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

**Note:**
The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

### 3.4 Performing Provisioning Operations

Provisioning operation for Fusion Apps connector is performed through access policies.

Oracle Identity Manager Users created in case of FA as the source of truth, have an Access Policy named FA Access Policy for FA User associated to them. When the policy is evaluated, SSO account creation for the user is triggered. The Oracle Identity Manager User is then linked with the existing FA User and the SSO email is propagated to the target system correspondingly.

Oracle Identity Manager Users created in case of an external HRMS as the source of truth, have an Access Policy named FA Access Policy for External User associated to them. When the policy is evaluated, SSO account creation for the user is triggered. This triggers creation of a FA account and the SSO email is propagated to FA correspondingly.

To perform provisioning operations in Oracle Identity Manager, see detailed information in Updating Access Policies.

### 3.5 Uninstalling the Fusion Apps Connector

Uninstalling the connector deletes all the account related data associated with resource objects of the connector.

If you want to uninstall the connector for any reason, see Uninstalling Connectors in Oracle Fusion Middleware Administering Oracle Identity Manager.
Extending the Functionality of the Fusion Apps Connector

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

Note:

From Oracle Identity Manager Release 11.1.2 onward, lookup queries are not supported. See Managing Lookups in *Oracle Fusion Middleware Administering Oracle Identity Manager* for information about managing lookups by using the Form Designer in the Oracle Identity Manager System Administration console.

• Adding New User Attributes for Reconciliation
• Adding New User Attributes for Provisioning
• Configuring Transformation of Data During User Reconciliation
• Configuring Validation of Data During Reconciliation and Provisioning

4.1 Adding New User Attributes for Reconciliation

The connector provides a default set of attribute mappings for reconciliation between Oracle Identity Manager and the target system. If required, you can add new user or group attributes for reconciliation.

By default, the attributes listed in Table 1-7 are mapped for reconciliation between Oracle Identity Manager and the target system.

Note:

- This connector supports configuration of already existing (standard) attributes of Fusion Apps for reconciliation.
- Only single-valued attributes can be mapped for reconciliation.

The following topics discuss the procedure to add new attributes for users:

• Adding New Attributes on the Process Form
• Adding Attributes to the Resource Object
• Creating Reconciliation Field Mapping
Creating Entries in Lookup Definitions
Performing Changes in a New UI Form

4.1.1 Adding New Attributes on the Process Form

You can add a new attribute on the process form in the Form Designer section of Oracle Identity Manager Design Console.

To add a new attribute on the process form:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand Development Tools, and double-click Form Designer.
3. Search for and open the UD_FAUSER process form for users.
4. Click Create New Version, and then Add.
5. Enter the details of the field.
   For example, if you are adding the EMAIL field, enter UD_FAUSER_EMAIL in the Name field and then enter other details such as Variable Type, Length, Field Label, and Field Type.
6. Click the Save icon, and then click Make Version Active. The following screenshot shows the new field added to the process form.

![Figure 4-1   Adding a New Field on the Process Form](image)

4.1.2 Adding Attributes to the Resource Object

You can add the new attribute to the resource object in the Resource Objects section of Oracle Identity Manager Design Console.

To add the new attribute to the list of reconciliation fields in the resource object:

2. Search for and open the **FA User** resource object for users.

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

4. Enter the details of the field.

   For example, enter **EMAIL** in the Name field and select **String** from the Field Type list. Later in this procedure, you enter the field name as the Code value of the entry that you create in the lookup definition for reconciliation.

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

   ![Figure 4-2 Newly Added Reconciliation Field](image)

6. Click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.

### 4.1.3 Creating Reconciliation Field Mapping

You can create reconciliation field mapping for the new attribute in the Process Definition section of Oracle Identity Manager Design Console.

To create a reconciliation field mapping for the new attribute in the process definition:

1. Expand **Process Management** and double-click **Process Definition**.

2. Search for and open the **FA User** process definition.

3. On the Reconciliation Field Mappings tab of the process definition, click **Add Field Map**.

4. From the Field Name list, select the field that you want to map.
5. Double-click the **Process Data Field** field and select the column for the attribute. For example, select **UD_FAUSER_EMAIL**.

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

**Figure 4-3  New Reconciliation Field Mapped to a Process Data Field**

![Screenshot of new reconciliation field mapped to process data field]

### 4.1.4 Creating Entries in Lookup Definitions

You must create an entry for the newly added attribute in the lookup definition that holds attribute mappings for reconciliation.

To create an entry for the newly added attribute in the lookup definition:

1. **Expand Administration.**
2. **Double-click Lookup Definition.**
3. **Search for and open the** **Lookup.FAIdentityService.UM.ReconAttrMap** **lookup definition.**
4. **Click Add and enter the Code Key and Decode values for the field. The Code Key value must be the name of the field in the resource object.**
5. **Click the Save icon. The following screenshot shows the entry added to the lookup definition:**

![Screenshot of entry added to lookup definition]
4.1.5 Performing Changes in a New UI Form

You must replicate all changes made to the Form Designer of the Design Console in a new UI form.

To perform all changes made to the Form Designer of the Design Console in a new UI form, perform the following procedure:

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. See Creating a Sandbox and Activating and Deactivating a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.
3. Create a new UI form to view the newly added field along with the rest of the fields. See Creating Forms By Using the Form Designer in Oracle Fusion Middleware Administering Oracle Identity Manager.
4. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource from the Form field, select the form, and then save the application instance.
5. Publish the sandbox. See Publishing a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.

4.2 Adding New User Attributes for Provisioning

The connector provides a default set of attribute mappings for provisioning between Oracle Identity Manager and the target system. If required, you can add new user or group attributes for provisioning.

By default, the attributes listed in Table 1-10 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional user attributes for provisioning.
The following topics discuss the procedure to add new user or group attributes for provisioning:

- Adding New Attributes for Provisioning
- Creating Entries in Lookup Definitions for Provisioning
- Creating a Task to Enable Update Operations
- Replicating Form Designer Changes to a New UI Form

### 4.2.1 Adding New Attributes for Provisioning

To add a new attribute on the process form, perform the following procedure:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools** and double-click **Form Designer**.
3. Search for and open the **UD_FAUSER** process form.
4. Click **Create New Version**, and then click **Add**.
5. Enter the details of the attribute.
   - For example, if you are adding the **EMAIL** field, enter **UD_FAUSER_EMAIL** in the Name field, and then enter the rest of the details of this field.
6. Click the Save icon, and then click **Make Version Active**.

---

Note:

If you have already added an attribute for reconciliation, then you need not repeat steps performed as part of that procedure.
4.2.2 Creating Entries in Lookup Definitions for Provisioning

You must create an entry for the newly added attribute in the lookup definition that holds attribute mappings for provisioning.

To create an entry for the newly added attribute in the lookup definition that holds attribute mappings for provisioning:

1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open the **Lookup.FAIdentityService.UM.ProvAttrMap** the lookup definition.
4. Click **Add** and then enter the Code Key and Decode values for the attribute.

For example, enter **EMAIL** in the Code Key column and then enter **emails.value** in the Decode column. The following screenshot shows the entry added to the lookup definition:
4.2.3 Creating a Task to Enable Update Operations

Create a task to enable updates on the new user or group attribute during provisioning operations.

If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of the attribute during provisioning operations, add a process task for updating the new user or group attribute as follows:

1. Expand **Process Management** and double-click **Process Definition**.
2. Search for and open the **FA User** process definition.
3. Click **Add**.
4. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:
   - Conditional
   - Allow Cancellation while Pending
   - Allow Multiple Instances
   - Required for Completion
5. Click the Save icon.
The following screenshot shows the new task added to the process definition:

**Figure 4-7  Newly Added Task to the Process Definition**

6. In the provisioning process, select the adapter name in the Handler Type section as follows:
   a. Go to the Integration tab, click **Add**.
   b. In the Handler Selection dialog box, select **Adapter**.
   c. From the Handler Name column, select **adpFAIDENTITYSERVICEUPDATEUSE**.
   d. Click Save and close the dialog box.

   The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:

**Figure 4-8  List of Adapter Variables**

7. In the Adapter Variables region, click the **ParentFormProcessInstanceKey** variable.
8. In the dialog box that is displayed, create the following mapping:

- **Variable Name**: ParentFormProcessInstanceKey
- **Map To**: Process Data
- **Qualifier**: Process Instance

9. Click **Save** and close the dialog box.

10. If you are enabling update provisioning operations for a User attribute, then repeat Steps 7 through 9 for the remaining variables listed in the Adapter Variables region.

The following table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Data Type</th>
<th>Map To</th>
<th>Qualifier</th>
<th>Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter Return Value</td>
<td>Object</td>
<td>Response Code</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Object Type</td>
<td>String</td>
<td>Literal</td>
<td>String</td>
<td>User</td>
</tr>
<tr>
<td>itResourceFieldName</td>
<td>String</td>
<td>Literal</td>
<td>String</td>
<td>UD_FAUSER_IT RESOURCE</td>
</tr>
<tr>
<td>attributeFieldName</td>
<td>String</td>
<td>Literal</td>
<td>String</td>
<td>EMAIL</td>
</tr>
<tr>
<td>processInstanceKey</td>
<td>Long</td>
<td>Process Data</td>
<td>Process Instance</td>
<td>NA</td>
</tr>
</tbody>
</table>

11. On the Responses tab, click **Add** to add at least the SUCCESS response code, with Status C. This ensures that if the task is successfully run, then the status of the task is displayed as **Completed**.

12. Click the Save icon and close the dialog box, and then save the process definition.

### 4.2.4 Replicating Form Designer Changes to a New UI Form

You must replicate all changes made to the Form Designer of the Design Console in a new UI form.

To replicate all changes made to the Form Designer of the Design Console in a new UI form:

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. See Creating a Sandbox and Activating and Deactivating a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.
3. Create a new UI form to view the newly added field along with the rest of the fields. See Creating Forms By Using the Form Designer in Oracle Fusion Middleware Administering Oracle Identity Manager.
4. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource from the Form field, select the form, and then save the application instance.
5. Publish the sandbox. See Publishing a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.
4.3 Configuring Transformation of Data During User Reconciliation

You can configure transformation of reconciled single-valued account data according to your requirements.

For example, you can use User Name and Last Name values to create a value for the Full Name field in Oracle Identity Manager.

**Note:**

This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

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

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

   The transformation class must implement the transform method with the following method signature:

   ```java
   Object transform(HashMap hmUserDetails, HashMap hmEntitlementDetails, String sField)
   ```

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

   ```java
   package oracle.iam.connectors.common.transform;
   import java.util.HashMap;
   public class TransformAttribute {
   /*
   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").
   *To fetch child data values, loop through the
   * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
   * Return the transformed attribute.
   */
   String sUserName= (String)hmUserDetails.get("User Name"); String
sLastName= (String)hmUserDetails.get("Last Name"); String sFullName=sUserName+"."+sLastName; return sFullName;
}
}

2. Create a JAR file to hold the Java class.

3. Copy the JAR file to 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.

4. If you created the Java class for transforming a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Expand Administration, and then double-click Lookup Definition.
   c. In the Code Key column, enter Lookup.RESOURCE.UM.ReconTransformation as the name of the lookup definition.

   Note:

   The value for the RESOURCE parameter in the Lookup.RESOURCE.UM.ReconTransformation or Lookup.RESOURCE.UM.Configuration lookup definitions will be FAIdentityService or FAUserRequestService depending on the bundle being configured.

   d. Select the Lookup Type option
   e. On the Lookup Code Information tab, click Add. A new row is added.
   f. In the Code Key column, enter the name of the resource object field into which you want to store the transformed value. For example, FirstName.
   g. In the Decode column, enter the name of the class that implements the transformation logic. For example, oracle.iam.connectors.common.transform.TransformAttribute.
h. Save the changes to the lookup definition.

5. Add an entry in the Lookup.RESOURCE.UM.Configuration lookup definition to enable transformation as follows:
   a. Expand Administration, and then double-click Lookup Definition.
   b. Search for and open the Lookup.RESOURCE.UM.Configuration lookup definition.
   c. Create an entry that holds the name of the lookup definition used for transformation as follows:
      Code Key: Recon Transformation Lookup
      Decode: Lookup.RESOURCE.UM.ReconTransformation
   d. Save the changes to the lookup definition.

### 4.4 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements.

For example, you can validate data fetched from the User Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the User Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations. For data that fails the validation check, the following message is displayed or recorded in the log file: Validation failed for attribute ATTRIBUTE_NAME.

Note:

This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.
   The validation class must implement validate method with the following method signature:

   ```java
   boolean validate(HashMap hmUserDetails, HashMap hmEntitlementDetails, String field)
   ```

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

   ```java
   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)
   * For child data values, loop through the
   ```
ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")

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 sUserName=(String) hmUserDetails.get(field);
    for(int i=0;i<sUserName.length();i++){
        if (sUserName.charAt(i) == '#'){ valid=false;
            break;
        }
        return valid;
    }

2. Create a JAR file to hold the Java class.

3. Copy the JAR file to 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.

4. If you created the Java class for validating a process form field for reconciliation,
then:
   a. Log in to the Design Console.
   b. Expand Administration, and then double-click Lookup Definition.
   c. In the Code Key column, enter Lookup.RESOURCE.UM.ReconValidation as the
      name of the lookup definition.
Note:
The value for the RESOURCE parameter in the 
Lookup.RESOURCE.UM.ReconTransformation or 
Lookup.RESOURCE.UM.Validation lookup definitions will be 
FAIdentityService or FAUserRequestService depending on the 
bundle being configured.

d. Select the Lookup Type option
e. On the Lookup Code Information tab, click Add. A new row is added.
f. In the Code Key column, enter the name of the resource object field into which 
you want to store the transformed value. For example, FirstName.
g. In the Decode column, enter the name of the class that implements the 
transformation logic. For example, com.validate.MyValidation..
h. Save the changes to the lookup definition.
i. Search for and open the Lookup.RESOURCE.UM.Configuration lookup 
definition.
j. Create an entry with the following values:
   Code Key: Recon Validation Lookup
   Decode: Lookup.RESOURCE.UM.ReconValidation
k. Save the changes to the lookup definition.

5. If you created the Java class for validating a process form field for provisioning, then:
   a. Log in to the Design Console.
   b. Expand Administration, and then double-click Lookup Definition.
   c. In the Code Key column, enter Lookup.RESOURCE.UM.ProvValidation as the 
      name of the lookup definition.
   d. Select the Lookup Type option
e. On the Lookup Code Information tab, click Add. A new row is added.
f. In the Code Key column, enter the process form field name. In the Decode 
   column, enter the class name.
g. Save the changes to the lookup definition.
h. Search for and open the Lookup.RESOURCE.UM.Configuration lookup 
definition.
i. Create an entry with the following values:
   Code Key: Provisioning Validation Lookup
   Decode: Lookup.RESOURCE.UM.ProvValidation
j. Save the changes to the lookup definition.
Files and Directories on the Fusion Apps Connector Installation Media

These are the components of the connector installation media that comprise the connector.

Table A-1  Files and Directories on the Fusion Apps Connector Installation Media

<table>
<thead>
<tr>
<th>File in the Installation Media Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• org.identityconnectors.faidentityservice-1.0.1115.jar</td>
<td>These JAR files contain the connector bundle.</td>
</tr>
<tr>
<td>• org.identityconnectors.fauserrequestservice-1.0.1115.jar</td>
<td>configuration</td>
</tr>
<tr>
<td>xml/FusionApps-ConnectorConfig.xml</td>
<td>This XML file contains configuration information that is used during the connector installation process</td>
</tr>
<tr>
<td></td>
<td>This XML file contains definitions for the following components of the connector:</td>
</tr>
<tr>
<td></td>
<td>• IT resource types</td>
</tr>
<tr>
<td></td>
<td>• IT resource instance</td>
</tr>
<tr>
<td></td>
<td>• Process forms</td>
</tr>
<tr>
<td></td>
<td>• Process tasks and adapters</td>
</tr>
<tr>
<td></td>
<td>• Lookup definitions</td>
</tr>
<tr>
<td></td>
<td>• Resource objects</td>
</tr>
<tr>
<td></td>
<td>• Process definition</td>
</tr>
<tr>
<td></td>
<td>• Scheduled jobs</td>
</tr>
<tr>
<td></td>
<td>• Reconciliation rules</td>
</tr>
<tr>
<td></td>
<td>• Prepopulate rules</td>
</tr>
</tbody>
</table>
Index

C

certified components, 1-2

certified languages, 1-2

configure scheduled jobs, 3-11

certified languages, 1-2

connector architecture topologies, 1-3

connector files and directories, A-1

connector installation media, A-1

F

features of connector connector features, 1-9

I

identity management account management provisioning operations target resource reconciliation, 1-1

L

limited reconciliation filtered reconciliation, 1-10

localizing, 2-15

logging, 2-19

enable logging, 2-20

log levels, 2-19

logging (continued)

lookup field synchronization, 1-11

P

preconfigured lookup definitions other lookup definitions, 1-12

S

scheduled job lookup field synchronization, 3-1

stages of connector deployment installation, 2-2

Postinstallation, 2-7

support for the connector server, 1-11

T

transformation, 4-11

U

uninstall connector uninstall, 3-12

V

validation, 4-13

validation of account data transformation of account data, 1-10