Oracle® Identity Manager

Connector Guide for Oracle Internet Directory

Release 11.1.1

E28603-22

June 2021

Oracle Identity Manager Connector Guide for Oracle Internet Directory, Release 11.1.1

E28603-22

Primary Author: Gowri.G.R

Contributing Authors: Alankrita Prakash

Contents

Preface

Audience xvii
Documentation Accessibility xvii
Related Documents xvii
Documentation Updates xvii
Conventions xviii

What's New in Oracle Identity Manager Connector for OID?

Software Updates xix
Documentation-Specific Updates xx

1 About the Connector

1.1 Introduction to the OID Connector 1-1
1.2 Certified Components 1-2
1.3 Usage Recommendations for the OID Connector 1-4
1.4 Certified Languages for the OID Connector 1-4
1.5 Architecture of the OID Connector 1-5
1.6 Features of the OID Connector 1-6
1.6.1 Dependent Lookup Fields 1-7
1.6.2 Full and Incremental Reconciliation 1-7
1.6.3 Limited Reconciliation 1-7
1.6.4 Transformation and Validation of Account Data 1-7
1.6.5 Support for the Connector Server 1-8
1.6.6 Support for High-Availability Configuration of the Target System 1-8
1.6.7 Support for Bulk Update of Attributes 1-8
1.6.8 Reconciliation of Deleted User Records 1-8
1.6.9 Reconciliation of Deleted Groups, Roles, and Organizations 1-8
1.6.10 Connection Pooling 1-9
1.6.11 Support for Groovy Scripts 1-9
1.7 Security Considerations for the Connector 1-9
1.7.1 Secure Communication to the Target System 1-9

1.7.2 Administrator Account for the Target System 1-9
1.8 Lookup Definitions Used During Reconciliation and Provisioning 1-9
1.8.1 Lookup Definitions Synchronized with the Target System 1-10
1.8.2 Preconfigured Lookup Definitions for Languages 1-12
1.9 Connector Objects Used During Target Resource Reconciliation 1-12
1.9.1 User Fields for Target Resource Reconciliation 1-12
1.9.2 Group Fields for Reconciliation 1-15
1.9.3 Role Fields for Reconciliation 1-16
1.9.4 Organizational Unit (OU) Fields for Reconciliation 1-16
1.9.5 Reconciliation Rules for Target Resource Reconciliation 1-17
1.9.5.1 About Reconciliation Rules for Target Resource Reconciliation 1-17
1.9.5.2 Viewing the Reconciliation Rule for Target Resource Reconciliation 1-18
1.9.6 Reconciliation Action Rules for Target Resource Reconciliation 1-19
1.9.6.1 About Reconciliation Actions Rules for Target Resource Reconciliation 1-20
1.9.6.2 Viewing Reconciliation Actions Rules for Target Resource Reconciliation 1-20
1.10 Connector Objects Used During Provisioning 1-21
1.10.1 Provisioning Functions 1-21
1.10.2 User Fields for Provisioning 1-23
1.10.2.1 User Fields for Provisioning an ODSEE Target System 1-23
1.10.2.2 User Fields for Provisioning an OUD Target System 1-24
1.10.2.3 User Fields for Provisioning an OID Target System 1-24
1.10.2.4 User Fields for Provisioning an eDirectory Target System 1-25
1.10.3 Group Fields for Provisioning 1-26
1.10.4 Role Fields for Provisioning 1-27
1.10.5 Organizational Unit Fields for Provisioning 1-28
1.11 Connector Objects Used During Trusted Source Reconciliation 1-29
1.11.1 User Fields for Trusted Source Reconciliation 1-29
1.11.2 Reconciliation Rule for Trusted Source Reconciliation 1-31
1.11.2.1 About Reconciliation Rule for Trusted Source Reconciliation 1-31
1.11.2.2 Viewing Reconciliation Rules for Trusted Source Reconciliation 1-32
1.11.3 Reconciliation Action Rules for Trusted Source Reconciliation 1-33
1.11.3.1 About Reconciliation Action Rules for Trusted Source Reconciliation 1-34
1.11.3.2 Viewing Reconciliation Action Rules for Trusted Source Reconciliation 1-34
1.12 Roadmap for Deploying and Using the Connector 1-35

2 Deploying the Connector

2.1 Preinstallation 2-1
2.1.1 Preinstallation on the Target System 2-1
2.1.2 Installing and Configuring the Connector Server 2-2
2.1.2.1 About Installing and Configuring the Connector Server 2-2

2.1.2.2 Installing and Configuring the Java Connector Server 2-2
2.1.3 Running the Connector Server 2-4
2.1.3.1 Running the Connector Server on UNIX and Linux Systems 2-4
2.1.3.2 Running the Connector Server on Microsoft Windows Systems 2-5
2.1.4 Configuring SSL for the Connector 2-5
2.1.4.1 Configuring SSL on the Target System 2-6
2.1.4.2 Configuring the Connector Server for SSL 2-6
2.1.4.3 Configuring Oracle Identity Manager for SSL 2-7
2.1.5 Enabling Logging for the Connector 2-8
2.1.5.1 Enabling Logging on Oracle Identity Manager 2-8
2.1.5.2 Enabling Logging on the Connector Server 2-10
2.2 Installation 2-11
2.2.1 Installing the Connector in Oracle Identity Manager 2-11
2.2.1.1 Running the Connector Installer 2-11
2.2.1.2 Configuring the IT Resource for the Target System 2-13
2.2.2 Installing the Connector in the Connector Server 2-16
2.3 Postinstallation 2-17
2.3.1 Postinstallation on Oracle Identity Manager 2-17
2.3.1.1 Configuring Oracle Identity Manager 11.1.2 or Later 2-17
2.3.1.2 Localizing Field Labels in UI Forms 2-20
2.3.1.3 Clearing Content Related to Connector Resource Bundles from the Server Cache 2-21
2.3.1.4 Setting up the Lookup Definition for Connection Pooling 2-22
2.3.1.5 Setting Up the OID Configuration Lookup Definition for LDAP Operation Timeouts 2-24
2.3.1.6 Configuring Oracle Identity Manager for Request-Based Provisioning 2-24
2.3.2 Creating the IT Resource for the Connector Server 2-27
2.4 Uninstalling the Connector 2-34
2.5 Upgrading the Connector 2-34
2.5.1 Preupgrade Steps 2-35
2.5.2 Upgrade Steps 2-35
2.5.3 Postupgrade Steps 2-35
2.5.4 Running the Form Version Control (FVC) Utility to Migrate eDirectory Forms 2-36
2.6 Postcloning Steps 2-37
2.6.1 About Postcloning Steps 2-37
2.6.2 Postcloning Configuration for User Accounts 2-38

3 Using the Connector

3.1 Guidelines on Using the Connector 3-1
3.1.1 Guidelines on Configuring Reconciliation 3-1
3.1.2 Guidelines on Performing Provisioning Operations 3-2

3.2 Scheduled Jobs for Lookup Field Synchronization 3-3
3.2.1 Scheduled Jobs for Lookup Field Synchronization for ODSEE 3-3
3.2.2 Scheduled Jobs for Lookup Field Synchronization for Oracle Internet Directory 3-4
3.2.3 Scheduled Jobs for Lookup Field Synchronization for Novell eDirectory 3-4
3.2.4 Scheduled Job Attributes 3-5
3.3 Configuring Reconciliation 3-5
3.3.1 Full Reconciliation and Incremental Reconciliation 3-6
3.3.2 Limited Reconciliation 3-6
3.3.2.1 Limited Reconciliation By Using Filters 3-7
3.3.2.2 Limited Reconciliation Based on Group Membership 3-7
3.3.3 Reconciliation Scheduled Jobs 3-7
3.3.3.1 Scheduled Jobs for Reconciliation of User Records 3-7
3.3.3.2 Scheduled Jobs for Reconciliation of Deleted User Records 3-12
3.3.3.3 Scheduled Jobs for Reconciliation of Groups, OUs, and Roles 3-12
3.3.3.4 Scheduled Jobs for Reconciliation of Deleted Groups, OUs, and Roles 3-16
3.4 Configuring Scheduled Jobs 3-17
3.4.1 Configuring a Scheduled Job 3-17
3.4.2 Configuring the Search Base and Search Scope in Scheduled Jobs and Tasks 3-19
3.4.2.1 Exporting the Scheduled Job and Task 3-19
3.4.2.2 Adding Additional Parameters to the Job and Task 3-19
3.4.2.3 Importing the Updated XML 3-21
3.5 Performing Provisioning Operations in Oracle Identity Manager Release 11.1.1.x 3-21
3.5.1 About Provisioning Operation in Oracle Identity Manager 3-21
3.5.2 Direct Provisioning 3-22
3.5.3 Direct Provisioning for Groups, Roles, and Organizations 3-26
3.5.4 Request-Based Provisioning 3-27
3.5.4.1 End User's Role in Request-Based Provisioning 3-27
3.5.4.2 Approver's Role in Request-Based Provisioning 3-28
3.5.5 Switching Between Request-Based Provisioning and Direct Provisioning 3-28
3.5.5.1 Switching From Request-Based to Direct Provisioning 3-29
3.5.5.2 Switching From DIrect to Request-Based Provisioning 3-29
3.6 Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later 3-30
3.7 Uninstalling the Connector 3-30

4 Using the Connector with Oracle Directory Server Enterprise Edition

4.1 Configuring Secure Communications 4-1
4.2 Preconfigured Lookup Definitions for an ODSEE Target System 4-1
4.2.1 Lookup.LDAP.Configuration 4-1
4.2.2 Lookup.LDAP.Configuration.Trusted 4-5
4.2.3 Preconfigured Lookup Definitions for User Operations 4-6

4.2.3.1 Lookup.LDAP.UM.Configuration 4-6
4.2.3.2 Lookup.LDAP.UM.Configuration.Trusted 4-7
4.2.3.3 Lookup.LDAP.UM.ProvAttrMap 4-8
4.2.3.4 Lookup.LDAP.UM.ReconAttrMap 4-8
4.2.3.5 Lookup.LDAP.UM.ProvValidation 4-8
4.2.3.6 Lookup.LDAP.UM.ReconTransformation 4-8
4.2.3.7 Lookup.LDAP.UM.ReconValidation 4-8
4.2.3.8 Lookup.LDAP.UM.ReconAttrMap.Trusted 4-8
4.2.3.9 Lookup.LDAP.UM.TrustedDefaults 4-9
4.2.4 Preconfigured Lookup Definitions for Group Operations 4-9
4.2.4.1 Lookup.LDAP.Group.Configuration 4-9
4.2.4.2 Lookup.LDAP.Group.ProvAttrMap 4-10
4.2.4.3 Lookup.LDAP.Group.ReconAttrMap 4-10
4.2.5 Preconfigured Lookup Definitions for Organizational Unit Operations 4-10
4.2.5.1 Lookup.LDAP.OU.Configuration 4-10
4.2.5.2 Lookup.LDAP.OU.ProvAttrMap 4-11
4.2.5.3 Lookup.LDAP.OU.ReconAttrMap 4-11
4.2.6 Preconfigured Lookup Definitions for Role Operations 4-11
4.2.6.1 Lookup.LDAP.Role.Configuration 4-11
4.2.6.2 Lookup.LDAP.Role.ProvAttrMap 4-12
4.2.6.3 Lookup.LDAP.Role.ReconAttrMap 4-12
4.3 Reconciling ODSEE Users Under Their Corresponding Organizations in Oracle Identity Manager 4-12
4.4 Reconciling ODSEE Groups and Roles Under One Organization in Oracle Identity Manager 4-13
4.4.1 Reconciling ODSEE Groups Under One Organization 4-13
4.4.2 Reconciling ODSEE Roles Under One Organization 4-13

5 Using the Connector with Oracle Unified Directory

5.1 Configuring Secure Communications 5-1
5.2 Preconfigured Lookup Definitions for an OUD Target System 5-1
5.2.1 Lookup.LDAP.OUD.Configuration 5-1
5.2.2 Lookup.LDAP.OUD.Configuration.Trusted 5-5
5.2.3 Preconfigured Lookup Definitions for User Operations 5-6
5.2.3.1 Lookup.LDAP.UM.Configuration 5-7
5.2.3.2 Lookup.LDAP.UM.Configuration.Trusted 5-7
5.2.3.3 Lookup.LDAP.UM.ProvAttrMap 5-8
5.2.3.4 Lookup.LDAP.UM.ReconAttrMap 5-8
5.2.3.5 Lookup.LDAP.UM.ProvValidation 5-8
5.2.3.6 Lookup.LDAP.UM.ReconTransformation 5-8
5.2.3.7 Lookup.LDAP.UM.ReconValidation 5-9

5.2.3.8 Lookup.LDAP.UM.ReconAttrMap.Trusted 5-9
5.2.3.9 Lookup.LDAP.UM.TrustedDefaults 5-9
5.2.4 Preconfigured Lookup Definitions for Group Operations 5-9
5.2.4.1 Lookup.LDAP.Group.Configuration 5-10
5.2.4.2 Lookup.LDAP.Group.ProvAttrMap 5-10
5.2.4.3 Lookup.LDAP.Group.ReconAttrMap 5-10
5.2.5 Preconfigured Lookup Definitions for Organizational Unit Operations 5-10
5.2.5.1 Lookup.LDAP.OU.Configuration 5-11
5.2.5.2 Lookup.LDAP.OU.ProvAttrMap 5-11
5.2.5.3 Lookup.LDAP.OU.ReconAttrMap 5-11
5.3 Reconciling OUD Users Under Their Corresponding Organizations in Oracle Identity Manager 5-12
5.4 Reconciling OUD Groups Under One Organization in Oracle Identity Manager 5-12
5.5 Reconciling Newly Created Objects for an OUD Target System 5-13
5.6 Guidelines on Using the Connector for Dynamic and Virtual Static Groups 5-13

6 Using the Connector with Oracle Internet Directory

6.1 Configuring Secure Communication 6-1
6.2 Preconfigured Lookup Definitions for an OID Target System 6-1
6.2.1 Lookup.OID.Configuration 6-1
6.2.2 Lookup.OID.Configuration.Trusted 6-5
6.2.3 Preconfigured Lookup Definitions for User Operations 6-6
6.2.3.1 Lookup.OID.UM.Configuration 6-6
6.2.3.2 Lookup.OID.UM.Configuration.Trusted 6-7
6.2.3.3 Lookup.OID.UM.ProvAttrMap 6-7
6.2.3.4 Lookup.OID.UM.ReconAttrMap 6-8
6.2.3.5 Lookup.OID.UM.ReconAttrMap.Trusted 6-9
6.2.3.6 Lookup.OID.UM.TrustedDefaults 6-10
6.2.4 Preconfigured Lookup Definitions for Group Operations 6-10
6.2.4.1 Lookup.OID.Group.Configuration 6-10
6.2.4.2 Lookup.OID.Group.ProvAttrMap 6-11
6.2.4.3 Lookup.OID.Group.ReconAttrMap 6-11
6.2.5 Preconfigured Lookup Definitions for Organizational Unit Operations 6-11
6.2.5.1 Lookup.OID.OU.Configuration 6-11
6.2.5.2 Lookup.OID.OU.ProvAttrMap 6-12
6.2.5.3 Lookup.OID.OU.ReconAttrMap 6-12
6.3 Reconciling OID Users Under Their Corresponding Organizations in Oracle Identity Manager 6-13
6.4 Reconciling OID Groups Under One Organization in Oracle Identity Manager 6-13

7 Using the Connector with Novell eDirectory

7.1 Configuring Secure Communications 7-1

7.2 Provisioning an eDirectory Target System 7-1

7.2.1 User Fields for Provisioning an eDirectory Target System 7-1

7.2.2 Group Fields for Provisioning an eDirectory Target System 7-2

7.2.3 Role Fields for Provisioning an eDirectory Target System 7-2

7.2.4 Organizational Unit (OU) Fields for Provisioning an eDirectory Target System 7-3

7.3 Performing Reconciliation for an eDirectory Target System 7-3

7.3.1 Trusted Reconciliation Fields for an eDirectory Target System 7-4

7.3.2 Reconciliation Rules for Target Resource Reconciliation 7-4

7.3.2.1 About Rules for Target Resource Reconciliation 7-4

7.3.2.2 Viewing the Reconciliation Rule for Target Resource Reconciliation 7-5

7.3.3 Reconciling eDirectory Users Under Their Corresponding Organizations in Oracle Identity Manager 7-6

7.3.4 Reconciling eDirectory Groups and Roles Under One Organization in Oracle Identity Manager 7-6

7.3.4.1 Reconciling eDirectory Groups Under One Organization 7-6

7.3.4.2 Reconciling eDirectory Roles Under One Organization 7-7

7.4 Preconfigured Lookup Definitions for an eDirectory Target System 7-7

7.4.1 Lookup.EDIR.Configuration 7-8

7.4.2 Lookup.EDIR.CommLang 7-10

7.4.3 Preconfigured Lookup Definitions for User Operations 7-10

7.4.3.1 Lookup.EDIR.UM.Configuration 7-11

7.4.3.2 Lookup.EDIR.UM.ProvAttrMap 7-11

7.4.3.3 Lookup.EDIR.UM.ReconAttrMap 7-11

7.4.3.4 Other Lookup Definitions 7-12

7.4.4 Preconfigured Lookup Definitions for Group Operations 7-13

7.4.4.1 Lookup.EDIR.Group.Configuration 7-13

7.4.4.2 Lookup.EDIR.Group.ProvAttrMap 7-13

7.4.4.3 Lookup.EDIR.Group.ReconAttrMap 7-13

7.4.5 Preconfigured Lookup Definitions for Role Operations 7-14

7.4.5.1 Lookup.EDIR.Role.Configuration 7-14

7.4.5.2 Lookup.EDIR.Role.ProvAttrMap 7-14

7.4.5.3 Lookup.EDIR.Role.ReconAttrMap 7-15

7.4.6 Preconfigured Lookup Definitions for Organizational Unit Operations 7-15

7.4.6.1 Lookup.EDIR.OU.Configuration 7-15

7.4.6.2 Lookup.EDIR.OU.ProvAttrMap 7-15

7.4.6.3 Lookup.EDIR.OU.ReconAttrMap 7-16

7.4.7 Preconfigured Lookup Definitions for Trusted Configuration Operations 7-16

7.4.7.1 Lookup.EDIR.Configuration.Trusted 7-16

7.4.7.2 Lookup.EDIR.UM.Configuration.Trusted 7-17

7.4.7.3 Lookup.EDIR.UM.ExclusionList.Trusted 7-17
7.4.7.4 Lookup.EDIR.UM.ReconAttrMap.Trusted 7-17
7.4.7.5 Lookup.EDIR.UM.ReconTransformations.Trusted 7-18
7.4.7.6 Lookup.EDIR.UM.ReconDefaults.Trusted 7-18

8 Using the Connector with an LDAPv3 Compliant Directory

8.1 Configuring Secure Communication 8-1
8.2 Creating a New IT Resource Instance 8-1
8.3 Configuring the Connector for OpenLDAP Server 8-2
8.3.1 Main Configuration Lookup 8-2
8.3.1.1 Organizational Unit (OU) Lookup Reconciliation 8-3
8.3.1.2 Group Lookup Reconciliation 8-3
8.3.2 User Provisioning 8-3
8.3.2.1 About User Provisioning With OpenLDAP 8-3
8.3.2.2 Using the Enable/Disable Feature with OpenLDAP 8-4
8.3.3 Group Provisioning 8-6
8.3.4 Organizational Unit (OU) Provisioning 8-6
8.3.5 User Search Reconciliation 8-6
8.3.5.1 About User Search Reconciliation 8-7
8.3.5.2 User Search Delete Reconciliation 8-7
8.3.5.3 Trusted User Reconciliation 8-7
8.3.5.4 Trusted User Delete Reconciliation 8-7
8.3.5.5 Group Search Reconciliation 8-8
8.3.5.6 Group Search Delete Reconciliation 8-8
8.3.5.7 OU Search Reconciliation 8-8
8.3.5.8 OU Search Delete Reconciliation 8-8
8.3.5.9 Unused Reconciliation Jobs 8-8

9 Extending the Functionality of the Connector

9.1 Adding Custom Fields for Target Resource Reconciliation 9-1
9.1.1 Adding the Custom Field to Resource Object Reconciliation Fields 9-2
9.1.2 Creating an Entry for the Custom Field in the Lookup Definition for Reconciliation 9-4
9.1.3 Adding the Custom Field on the Process Form 9-4
9.1.4 Associating a New Form With the Application Instance 9-5
9.1.5 Creating a Reconciliation Field Mapping for the Custom Field in the Provisioning Process 9-6
9.1.6 Creating the Reconciliation Profile 9-7
9.2 Adding New Multivalued Fields for Target Resource Reconciliation 9-7
9.2.1 Creating a Form for the Multivalued Field 9-7

9.2.2 Adding the Form as a Child Form of the Process Form 9-8
9.2.3 Associating a New Form With the Application Instance 9-9
9.2.4 Adding the New Multivalued Field to the Resource Object Reconciliation Fields 9-9
9.2.5 Creating an Entry for the Field in the Lookup Definition for Reconciliation 9-11
9.2.6 Creating a Reconciliation Field Mapping for the New Field 9-12
9.3 Adding Custom Fields for Provisioning 9-14
9.3.1 Adding the new Field to the Process Form 9-15
9.3.2 Associating a New Form With the Application Instance 9-16
9.3.3 Creating an Entry for the Field in the Lookup Definition for Provisioning 9-16
9.3.4 Enabling Update Provisioning Operations on the Custom Field 9-17
9.3.5 Updating the Request Dataset 9-22
9.3.6 Running the PurgeCache Utility and Importing the Request Dataset Definition to MDS 9-23
9.4 Adding New Multivalued Fields for Provisioning 9-23
9.4.1 Creating an Entry for the Field in the Lookup Definition for Provisioning 9-23
9.4.2 Adding the Task for Provisioning Multivalued Attributes in the Process Definition 9-25
9.4.2.1 Updating the Process Definition 9-25
9.4.2.2 Selecting the Adapter 9-26
9.4.2.3 Creating the Adapter Variables Mapping 9-26
9.4.2.4 Updating the Process Tasks 9-29
9.4.3 Updating the Request Dataset 9-30
9.4.4 Running the PurgeCache Utility and Importing the Request Dataset Definition to MDS 9-31
9.5 Adding New Fields for Trusted Source Reconciliation 9-31
9.5.1 Adding the New Field on the OIM User Process Form 9-31
9.5.2 Adding the New Field to the Resource Object Reconciliation Fields 9-32
9.5.3 Creating a Reconciliation Field Mapping 9-33
9.5.4 Creating an Entry for the Field in the Lookup Definition for Reconciliation 9-34
9.6 Configuring Transformation of Data During Reconciliation 9-35
9.7 Configuring Validation of Data During Reconciliation and Provisioning 9-37
9.8 Configuring the Connector for User-Defined Object Classes 9-39
9.9 Configuring the Connector to Use Custom Object Classes 9-40
9.10 Configuring the Connector for Multiple Trusted Source Reconciliation 9-41
9.11 Configuring the Connector to Support POSIX Groups and Accounts 9-41
9.12 Configuring the Connector to Support Provisioning of Custom Object Classes while Provisioning Organizational Unit 9-43
9.12.1 Modifying the Configuration Lookup Definition 9-43
9.12.2 About Adding Custom Object Classes 9-43

10 Troubleshooting

11 Known Issues and Workarounds

11.1 Failure in Provisioning a User with a Backslash 11-1

11.2 Incremental User Sync Reconciliation Does not Function as Expected 11-1

A Files and Directories on the OID Connector Installation Media

Index

List of Figures

1-1 Connector Architecture 1-5
1-2 Reconciliation Action Rules for Target Resource Reconciliation 1-21
1-3 Reconciliation Action Rules for Trusted Source Reconciliation 1-35
2-1 Manage IT Resource Page 2-14
2-2 Edit IT Resource Details and Parameters Page for the Target System IT Resource 2-14
2-3 Step 1: Provide IT Resource Information 2-28
2-4 Step 2: Specify IT Resource Parameter Values 2-28
2-5 Step 3: Set Access Permission to IT Resource 2-31
2-6 Step 4: Verify IT Resource Details 2-32
2-7 Step 5: IT Resource Connection Result 2-33
2-8 Step 6: IT Resource Created 2-34
3-1 User Details Page 3-22
3-2 Step 1: Select a Resource Page 3-23
3-3 Step 2: Verify Resource Selection Page 3-23
3-4 Step 5: Provide Process Data for LDAP User Form Page 3-24
3-5 Step 5: Provide Process Data for LDAP User Group Page 3-24
3-6 Step 5: Provide Process Data for LDAP User Role Page 3-25
3-7 Step 6: Verify Process Data Page 3-25
7-1 Reconciliation Rule Builder Screen for Target Resource Reconciliation 7-5

List of Tables

1-1 Certified Components 1-2
1-2 Lookup Definitions Synchronized with the Target System 1-11
1-3 Lookup Definitions Synchronized with the Target System for Oracle Internet Directory 1-11
1-4 Lookup Definitions Synchronized with the Target System for Novell eDirectory 1-11
1-5 Entries in the Lookup.LDAP.UM.ReconAttrMap Lookup Definition 1-13
1-6 Entries in the Lookup.OID.UM.ReconAttrMap Lookup Definition 1-13
1-7 Entries in the Lookup.EDIR.UM.ReconAttrMap Lookup Definition 1-14
1-8 Entries in the Lookup.LDAP.Group.ReconAttrMap Lookup Definition 1-15
1-9 Entries in the Lookup.OID.Group.ReconAttrMap Lookup Definition 1-15
1-10 Entries in the Lookup.EDIR.Group.ReconAttrMap Lookup Definition 1-15
1-11 Entries in the Lookup.LDAP.Role.ReconAttrMap Lookup Definition 1-16
1-12 Entries in the Lookup.EDIR.Role.ReconAttrMap Lookup Definition 1-16
1-13 Entries in the Lookup.LDAP.OU.ReconAttrMap Lookup Definition 1-16
1-14 Entries in the Lookup.OID.OU.ReconAttrMap Lookup Definition 1-17
1-15 Entries in the Lookup.EDIR.OU.ReconAttrMap Lookup Definition 1-17
1-16 Action Rules for Target Resource Reconciliation 1-20
1-17 Provisioning Functions for LDAP and OID Users 1-21
1-18 Provisioning Functions for eDirectory Users 1-22
1-19 Provisioning Functions for LDAP and OID Groups, Roles, and Organizational Units 1-22
1-20 Provisioning Functions for eDirectory Groups, Roles, and Organizational Units 1-22
1-21 Entries in the Lookup.LDAP.UM.ProvAttrMap Lookup Definition 1-23
1-22 Entries in the Lookup.LDAP.UM.ProvAttrMap Lookup Definition 1-24
1-23 Entries in the Lookup.OID.UM.ProvAttrMap Lookup Definition 1-24
1-24 Entries in the Lookup.EDIR.UM.ProvAttrMap Lookup Definition 1-25
1-25 Entries in the Lookup.LDAP.Group.ProvAttrMap Lookup Definition 1-26
1-26 Entries in the Lookup.OID.Group.ProvAttrMap Lookup Definition 1-27
1-27 Entries in the Lookup.EDIR.Group.ProvAttrMap Lookup Definition 1-27
1-28 Entries in the Lookup.LDAP.Role.ProvAttrMap Lookup Definition 1-27
1-29 Entries in the Lookup.EDIR.Role.ProvAttrMap Lookup Definition 1-28
1-30 Entries in the Lookup.LDAP.OU.ProvAttrMap Lookup Definition 1-28
1-31 Entries in the Lookup.OID.OU.ProvAttrMap Lookup Definition 1-28
1-32 Entries in the Lookup.EDIR.OU.ProvAttrMap Lookup Definition 1-29
1-33 Entries in the Lookup.LDAP.UM.ReconAttrMap.Trusted Lookup Definition 1-29
1-34 Entries in the Lookup.OID.UM.ReconAttrMap.Trusted Lookup Definition 1-30
1-35 Entries in the Lookup.EDIR.UM.ReconAttrMap.Trusted Lookup Definition 1-30

1-36 Action Rules for Trusted Source Reconciliation 1-34
2-1 Log Levels and ODL Message Type: Level Combinations 2-9
2-2 Parameters of the IT Resource for the Target System 2-15
2-3 Connection Pooling Properties 2-22
2-4 Parameters of the IT Resource for the Connector Server 2-29
2-5 Mappings for OID Event Handler/Adapter 2-39
3-1 Attributes of the Scheduled Jobs for Lookup Field Synchronization 3-5
3-2 Attributes of the LDAP Connector User Search Reconciliation Scheduled Job 3-9
3-3 Attributes of the LDAP Connector User Sync Reconciliation Scheduled Job 3-10
3-4 Attributes of the Scheduled Job for Reconciliation of User Data from a Trusted Source 3-11
3-5 Attributes of the Scheduled Jobs for Delete User Reconciliation 3-12
3-6 Attributes of the LDAP Connector Group Search Reconciliation, LDAP Connector OU Search Reconciliation, and LDAP Connector Role Search Scheduled Jobs 3-14
3-7 Attributes of the LDAP Connector Group Sync Reconciliation, LDAP Connector OU Sync Reconciliation, and LDAP Connector Role Sync Reconciliation Scheduled Jobs 3-15
3-8 Attributes of the Scheduled Jobs for Deleted Groups, Organizational Units, and Roles Reconciliation 3-17
4-1 Entries in the Lookup.LDAP.Configuration Lookup Definition 4-2
4-2 Entries in the Lookup.LDAP.Configuration.Trusted Lookup Definition 4-5
4-3 Entries in the Lookup.LDAP.UM.Configuration Lookup Definition 4-7
4-4 Entries in the Lookup.LDAP.UM.Configuration.Trusted Lookup Definition 4-7
4-5 Entries in the Lookup.LDAP.UM.TrustedDefaults Lookup Definition 4-9
4-6 Entries in the Lookup.LDAP.Group.Configuration Lookup Definition 4-10
4-7 Entries in the Lookup.LDAP.OU.Configuration Lookup Definition 4-11
4-8 Entries in the Lookup.LDAP.Role.Configuration Lookup Definition 4-12
5-1 Entries in the Lookup.LDAP.OUD.Configuration Lookup Definition 5-2
5-2 Entries in the Lookup.LDAP.OUD.Configuration.Trusted Lookup Definition 5-5
5-3 Entries in the Lookup.LDAP.UM.Configuration Lookup Definition 5-7
5-4 Entries in the Lookup.LDAP.UM.Configuration.Trusted Lookup Definition 5-8
5-5 Entries in the Lookup.LDAP.UM.TrustedDefaults Lookup Definition 5-9
5-6 Entries in the Lookup.LDAP.Group.Configuration Lookup Definition 5-10
5-7 Entries in the Lookup.LDAP.OU.Configuration Lookup Definition 5-11
6-1 Entries in the Lookup.OID.Configuration Lookup Definition 6-2
6-2 Entries in the Lookup.OID.Configuration.Trusted Lookup Definition 6-5
6-3 Entries in the Lookup.OID.UM.Configuration Lookup Definition 6-6
6-4 Entries in the Lookup.OID.UM.Configuration.Trusted Lookup Definition 6-7
6-5 Entries in the Lookup.OID.UM.ProvAttrMap Lookup Definition 6-7

6-6 Entries in the Lookup.OID.UM.ReconAttrMap Lookup Definition 6-8
6-7 Entries in the Lookup.OID.UM.ReconAttrMap.Trusted Lookup Definition 6-9
6-8 Entries in the Lookup.OID.UM.TrustedDefaults Lookup Definition 6-10
6-9 Entries in the Lookup.OID.Group.Configuration Lookup Definition 6-10
6-10 Entries in the Lookup.OID.Group.ProvAttrMap Lookup Definition 6-11
6-11 Entries in the Lookup.OID.Group.ReconAttrMap Lookup Definition 6-11
6-12 Entries in the Lookup.OID.OU.Configuration Lookup Definition 6-12
6-13 Entries in the Lookup.OID.OU.ProvAttrMap Lookup Definition 6-12
6-14 Entries in the Lookup.OID.OU.ReconAttrMap Lookup Definition 6-12
7-1 Entries in the Lookup.EDIR.UM.ProvAttrMap Lookup Definition 7-1
7-2 Entries in the Lookup.EDIR.Group.ProvAttrMap Lookup Definition 7-2
7-3 Entries in the Lookup.EDIR.Role.ProvAttrMap Lookup Definition 7-3
7-4 Entries in the Lookup.EDIR.OU.ProvAttrMap Lookup Definition 7-3
7-5 Entries in the Lookup.EDIR.UM.ReconAttrMap.Trusted Lookup Definition 7-4
7-6 Entries in the Lookup.EDIR.Configuration Lookup Definition 7-8
7-7 Entries in the Lookup.EDIR.CommLang Lookup Definition 7-10
7-8 Entries in the Lookup.EDIR.UM.Configuration Lookup Definition 7-11
7-9 Entries in the Lookup.EDIR.UM.ReconAttrMap Lookup Definition 7-11
7-10 Entries in the Lookup.EDIR.Group.Configuration Lookup Definition 7-13
7-11 Entries in the Lookup.EDIR.Group.ReconAttrMap Lookup Definition 7-13
7-12 Entries in the Lookup.EDIR.Role.Configuration Lookup Definition 7-14
7-13 Entries in the Lookup.EDIR.Role.ReconAttrMap Lookup Definition 7-15
7-14 Entries in the Lookup.EDIR.OU.Configuration Lookup Definition 7-15
7-15 Entries in the Lookup.EDIR.OU.ReconAttrMap Lookup Definition 7-16
7-16 Entries in the Lookup.EDIR.Configuration.Trusted Lookup Definition 7-16
7-17 Entries in the Lookup.EDIR.UM.Configuration.Trusted Lookup Definition 7-17
7-18 Entry in the Lookup.EDIR.UM.ExclusionList.Trusted Lookup Definition 7-17
7-19 Entries in the Lookup.EDIR.UM.ReconAttrMap.Trusted Lookup Definition 7-17
7-20 Entry in the Lookup.EDIR.UM.ReconTransformations.Trusted Lookup Definition 7-18
7-21 Entries in the Lookup.EDIR.UM.ReconDefaults.Trusted Lookup Definition 7-18
8-1 Parameters of the IT Resource for the OpenLDAP Server Target System 8-1
10-1 Troubleshooting for the OID Connector 10-1
A-1 Files and Directories on the Connector Installation Media A-1

Preface

This guide describes the Oracle Internet Directory (OID) connector that is used to onboard applications pertaining to LDAP directory servers such as Oracle Internet Directory (OID), Oracle Unified Directory (OUD), and Oracle Directory Server Enterprise Edition (ODSEE) to Oracle Identity Governance.

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

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

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

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

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

What's New in Oracle Identity Manager Connector for OID?

This chapter provides an overview of the updates made to the software and documentation for release 11.1.1.6.0 of the OID connector.

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

- Software Updates

  This section describes 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

  This section describes 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 sections discuss the software updates:

- Software Updates in Release 11.1.1.6.0
- Software Updates in Release 11.1.1.5.0

Software Updates in Release 11.1.1.6.0

The following are issues resolved in release 11.1.1.6.0:

Bug Number	Issue	Resolution
16519685 16519589 16518527	The following files in the xml directory of the installation media had user form information, which was not necessary: ODSEE-OUD-LDAPV3-ConnectorConfig.xml OID-ConnectorConfig.xml eDirectory-ConnectorConfig.xml	This issue has been resolved. The user form information has been removed from these files.

Bug Number	Issue	Resolution
16506154 16498633 16491429	There was no tagging of the AccountName, AccountID, and ITResource properties for the process form fields of the Novell eDirectory, Oracle Internet Directory, and Oracle Unified Directory target systems. As a result, after provisioning, the Account Name column on the Accounts tab of the My Access page in Oracle Identity Self Service for a user displayed the database numeric key, instead of the correct account name.	This issue has been resolved. The AccountName, AccountID, and ITResource properties of the process form fields have been tagged.
14324254	ODSEE/OUD or OID uninstallation removed shared adapters.	This issue has been resolved.
13925015	Debug logs were not visible.	This issue has been resolved. Debug logs are now visible.

Software Updates in Release 11.1.1.5.0

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

Documentation-Specific Updates

The following sections discuss the documentation-specific updates:

- Documentation-Specific Updates in Release 11.1.1.6.0
- Documentation-Specific Updates in Release 11.1.1.5.0

Documentation-Specific Updates in Release 11.1.1.6.0

The following documentation-specific update has been made in version "22" of release 11.1.1.6.0:

The "Target Systems" row of Certified Components has been updated for NetIQ eDirectory 8.7.3 and 8.8 and 9.2.

The following documentation-specific update has been made in version "21" of release 11.1.1.6.0:

The "Target Systems" row of Certified Components has been updated for 12*c* release (12.2.1.4.0) certification for Oracle Unified Directory.

The following documentation-specific update has been made in version "20" of release 11.1.1.6.0:

The "Oracle Identity Governance or Oracle Identity Manager" row of Certified Components has been modified to include support for Oracle Identity Governance release 12*c* PS4 (12.2.1.4.0).

The following documentation-specific update has been made in version "19" of release 11.1.1.6.0:

- The "Connector Server JDK and JRE" row of Certified Components has been modified from JRE 1.6 to JRE 1.7.

- A "Note" regarding lookup reconciliation scheduled jobs has been added at the beginning of Configuring the Search Base and Search Scope in Scheduled Jobs and Tasks.
- New code keys such as readTimeout, connectTimeout, and referrals have been added to several tables across the guide.

The following documentation-specific update has been made in version "18" of release 11.1.1.6.0:

The "Target Systems" row of Certified Components has been updated for 12*c* release (12.2.1.3.0) certification for Oracle Unified Directory and Oracle Internet Directory.

The following documentation-specific update has been made in version "17" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of Certified Components has been renamed as "Oracle Identity Governance or Oracle Identity Manager" and also updated for Oracle Identity Governance 12*c* (12.2.1.3.0) certification.

The following documentation-specific updates have been made in revision "16" of release 11.1.1.6.0:

- The "Target systems" row of Certified Components has been updated.
- All contents of Section 2.1.1.1, "Files and Directories On the Installation Media" have been moved to Files and Directories on the OID Connector Installation Media.

The following documentation-specific update has been made in revision "15" of release 11.1.1.6.0:

The "JDK and JRE" row of Certified Components has been renamed to "Connector Server JDK and JRE".

The following documentation-specific update has been made in revision "14" of release 11.1.1.6.0:

A "Note" regarding trusted source IT resource has been added at the beginning of Configuring the IT Resource for the Target System.

The following documentation-specific updates have been made in revision "13" of release 11.1.1.6.0:

- Setting Up the OID Configuration Lookup Definition for LDAP Operation Timeouts has been added.
- A guideline regarding Oracle Identity Manager release 11.1.2.3 and OID target system has been added to Guidelines on Configuring Reconciliation.
- The "Target systems" row of Certified Components has been updated.
- Adding New Multivalued Fields for Provisioning has been updated.
- Configuring the Connector to Support Provisioning of Custom Object Classes while Provisioning Organizational Unit has been added.

The following documentation-specific updates have been made in revision "12" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of Certified Components has been updated.
- Information specific to Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) has been added to Usage Recommendations for the OID Connector.

The following documentation-specific updates have been made in revision "11" of release 11.1.1.6.0:

- A "Note" has been added at the beginning of Extending the Functionality of the Connector.
- A "Note" regarding lookup queries has been removed from Lookup Definitions Used During Reconciliation and Provisioning.

The following are documentation-specific updates in revision "10" of release 11.1.1.6.0:

- A "Note" regarding lookup queries has been added to Lookup Definitions Used During Reconciliation and Provisioning.
- Guidelines on Using the Connector for Dynamic and Virtual Static Groups is added.

The following is a documentation-specific update in revision "9" of release 11.1.1.6.0:

A "Note" related to OID and AD has been added to Direct Provisioning for Groups, Roles, and Organizations.

The following are documentation-specific updates in revision "8" of release 11.1.1.6.0:

- The "accountObjectClasses" row has been added to Table 5-2.
- The lookup definition values for "OID" have been modified in the Description column of the "Configuration Lookup" row in Table 2-2.
- The "Oracle Identity Manager" row of Certified Components has been modified to include Oracle Identity Manager 11*g* Release 2 PS1 (11.1.2.1.0) or later.

The following are documentation-specific updates in revision "7" of release 11.1.1.6.0:

- Information about limited reconciliation has been modified in Limited Reconciliation.
- The "Oracle Identity Manager" row of Certified Components has been modified to include Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0).
- Information specific to Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) has been added to Step 5 of Localizing Field Labels in UI Forms.

The following is a documentation-specific update in revision "6" of release 11.1.1.6.0:

The `ds-privilege-name: -data-sync` privilege has been removed from Preinstallation on the Target System.

The following are documentation-specific updates in release 11.1.1.6.0:

- The "Oracle Identity Manager" row in Certified Components has been updated.
- A note has been added in the "xml/ODSEE-OUD-LDAPV3-Datasets.xml" row of Files and Directories on the OID Connector Installation Media.
- The following sections have been added:
  - Usage Recommendations for the OID Connector
  - Configuring Oracle Identity Manager 11.1.2 or Later
  - Localizing Field Labels in UI Forms
  - Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later

  - Configuring the Connector to Use Custom Object Classes
- Instructions specific to Oracle Identity Manager release 11.1.2.*x* have been added in the following sections:
  - Running the Connector Installer
  - Configuring the IT Resource for the Target System
  - Creating the IT Resource for the Connector Server
  - Postupgrade Steps
  - Configuring Scheduled Jobs
  - Adding Custom Fields for Target Resource Reconciliation
  - Adding New Multivalued Fields for Target Resource Reconciliation
  - Adding Custom Fields for Provisioning
  - Adding New Multivalued Fields for Provisioning
- The issue tracked by bug 14224953 has been removed from Known Issues and Workarounds as it is not an issue. However, the information specific to the bug is present in a note in Guidelines on Performing Provisioning Operations.
- The issue tracked by bug 13925015 has been removed from Known Issues and Workarounds as it has been resolved.
- Changes have been made to the code in Step 1, in the procedure "To create the admin user, group, and ACIs for connector operations" in Creating an Application Instance.
- A note has been added to User Provisioning.
- Information has been added to the "Description" column of the "Latest Token" row, in Table 3-4.
- A note has been added to Scheduled Jobs for Lookup Field Synchronization, under the "LDAP Connector Role Lookup Recon" bullet item.
- A note has been added to LDAP Connector Group Search Reconciliation, LDAP Connector OU Search Reconciliation, and LDAP Connector Role Search Reconciliation Scheduled Jobs.
- A note has been to Lookup.EDIR.UM.ReconAttrMap.Trusted.
- A note has been added to Configuring SSL on the Target System.
- The name of the "Known Issues" chapter has been changed to "Known Issues and Workarounds." In addition, Known Issues and Workarounds has been restructured.

Documentation-Specific Updates in Release 11.1.1.5.0

The following documentation-specific updates have been made in the revision "2" of the release 11.1.1.5.0:

- Preinstallation on the Target System, is updated to use Oracle Internet Directory command-line utilities to create and configure the target system administrator.
- Extending the Functionality of the Connector, adds information including resource objects, process form names, adapter names, and lookup definitions for Oracle Internet Directory (OID) and Novell eDirectory target systems.
- In #unique_22/unique_22_Connect_42_BABJEIFJ, Oracle Identity Manager patch versions are corrected.

- In the "Configuration lookup" row of Table 2-2, the name of the configuration lookup for Novell eDirectory has been added.

1 About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications.
This chapter contains the following sections:

- Introduction to the OID Connector
- Certified Components
- Usage Recommendations for the OID Connector
- Certified Languages for the OID Connector
- Architecture of the OID Connector
- Features of the OID Connector
- Security Considerations for the Connector
- Lookup Definitions Used During Reconciliation and Provisioning
- Connector Objects Used During Target Resource Reconciliation
- Connector Objects Used During Provisioning
- Connector Objects Used During Trusted Source Reconciliation
- Roadmap for Deploying and Using the Connector

1.1 Introduction to the OID Connector

This guide discusses the procedures to deploy and use the OID connector, which integrates Oracle Identity Manager with LDAP directories such as Oracle Directory Server Enterprise Edition (ODSEE), Oracle Internet Directory (OID), Oracle Unified Directory (OUD), and Novell eDirectory.

The connector uses the LDAPv3 protocol, so you can also use the connector for an LDAPv3 compliant directory server.

> **Note:**
>
> At some places in this guide, ODSEE, OID, OUD, eDirectory, and an LDAPv3 compliant directory are referred to as the **target system**.

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. In addition, you can use Oracle Identity Manager to perform provisioning operations on 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.

> **Note:**
>
> It is recommended that you do not configure the target system as both an authoritative (trusted) source and a managed (target) resource.

1.2 Certified Components

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

Table 1-1 Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) **Note:** If you are using Oracle Identity Governance 12c (12.2.1.3.0), then ensure to download and apply patches 26616250 and 25323654 from My Oracle Support.	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0)

Table 1-1 (Cont.) Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Target systems	The target system can be any one of the following: • Oracle Unified Directory 11*g* release (11.1.1.5.0, 11.1.2.0.0, 11.1.2.2.0, and 11.1.2.3.0) and 12c release (12.2.1.3.0 and 12.2.1.4.0) • Oracle Internet Directory release 9.*x*, 10.1.4.*x*, and 11*g* release 1 (11.1.1.5.0, 11.1.1.6.0, 11.1.1.7.0 and 11.1.1.9.0) • Oracle Directory Server Enterprise Edition 11*g* release 1 (11.1.1.5.0 and 11.1.1.7.2) • An LDAPv3-compliant directory server	The target system can be any one of the following: • Oracle Unified Directory 11*g* release (11.1.1.5.0, 11.1.2.0.0, 11.1.2.2.0, and 11.1.2.3.0) and 12c release (12.2.1.3.0 and 12.2.1.4.0) • Oracle Internet Directory release 9.*x*, 10.1.4.*x*, and 11*g* release 1 (11.1.1.5.0, 11.1.1.6.0, 11.1.1.7.0 and 11.1.1.9.0) • Oracle Directory Server Enterprise Edition 11*g* release 1 (11.1.1.5.0 and 11.1.1.7.2) • An LDAPv3-compliant directory server • NetIQ eDirectory 8.7.3, 8.8 • NetIQ eDirectory 9.2 **Note:** Currently certified with OID11.1.1.6.0L patch 31366708 only • Oracle Virtual Directory 10*g* and 11*g* release 1 (11.1.1.5.0) • Sun Java System Directory Server Enterprise Edition 6.3 and 7.0 • Sun ONE Directory Server 5.2
Connector Server	11.1.2.1.0	11.1.2.1.0
Connector Server JDK and JRE	JDK or JRE 1.6 and above	JDK or JRE 1.6 and above

1.3 Usage Recommendations for the OID Connector

These are the recommendations for the OID connector versions that you can deploy and use depending on the Oracle Identity Manager version you are using.

- If you are using an Oracle Identity Manager release that is earlier than Oracle Identity Manager 11*g* Release 1 (11.1.1), then depending on the target system that you are using, install and use one of the following connectors:
  - For Oracle Internet Directory, use the 9.0.4.*x* version of the Oracle Internet Directory connector.
  - For Novell eDirectory, use the 9.0.4.*x* version of the Novell eDirectory connector.
  - For Sun ONE Directory Server and Sun Java System Directory Server Enterprise Edition, use the 9.0.4.*x* version of the Sun Java System Directory connector.
- If you are using Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) or later, Oracle Identity Manager 11*g* Release 2 (11.1.2.0.4) or later, or Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0), then use the latest 11.1.1.*x* version of this connector for target systems Oracle Internet Directory, Sun Java System Directory Server Enterprise Edition, and Novell eDirectory.

1.4 Certified Languages for the OID Connector

These are the languages that the connector supports.

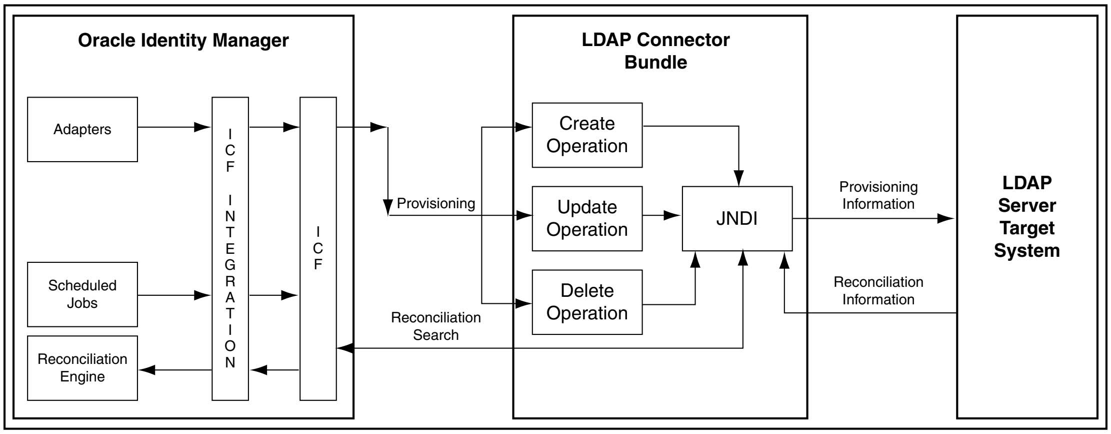
- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish

- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

1.5 Architecture of the OID Connector

The OID 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. The ICF is shipped along with Oracle Identity Manager. Therefore, you need not configure or modify the ICF.

Figure 1-1 Connector Architecture



The OID connector uses JNDI to access the target system.

This connector can be configured to run in one of the following modes:

- Identity reconciliation

  Identity reconciliation is also known as authoritative or trusted source reconciliation. In this form of reconciliation, OIM Users are created or updated corresponding to the creation of and updates to users on the target system. Note that the identity reconciliation mode supports reconciliation of user objects only.

  See Reconciliation Scheduled Jobs for information about the LDAP Connector Trusted User Reconciliation scheduled job that is used in this mode.

- Account Management

  Account management is also known as target resource management. This mode of the connector enables the following operations:

- Provisioning

  Provisioning involves creating, updating, or deleting users, groups, roles, and organizational units (OUs) on the target system through Oracle Identity Manager.

  When you allocate (or provision) a target system resource to an OIM User, the operation results in the creation of an account on the target system for that user. In the Oracle Identity Manager context, the term "provisioning" is also used to mean updates (for example enabling or disabling) made to the target system account through Oracle Identity Manager.

  Users and organizations are organized in hierarchical format on the target system. Before you can provision users to (that is, create users in) the required organizational units (OUs) on the target system, you must fetch into Oracle Identity Manager the list of OUs used on the target system. This is achieved by using the LDAP Connector OU Lookup Reconciliation scheduled job for lookup synchronization.

  Similarly, before you can provision users to the required groups or roles on the target system, you must fetch into Oracle Identity Manager the list of all groups and roles used on the target system. This is achieved by using the LDAP Connector Group Lookup Reconciliation and LDAP Connector Role Lookup Recon scheduled jobs for lookup synchronization.

- Target resource reconciliation

  To perform target resource reconciliation, the LDAP Connector User Search Reconciliation or LDAP Connector User Sync Reconciliation scheduled jobs is used. The connector applies filters to locate users to be reconciled from the target system and then fetches the attribute values of these users.

  Depending on the data that you want to reconcile, you use different scheduled jobs. For example, you use the LDAP Connector User Search Reconciliation scheduled job to reconcile user data in the target resource mode. See Reconciliation Scheduled Jobs for more information about scheduled jobs used in this mode.

1.6 Features of the OID Connector

The features of the connector include support for connector server, support for high-availability configuration of the target system, support for bulk update of target systems, reconciliation of deleted user records, and support for groovy scripts, and so on.

The following are features of the connector:

- Dependent Lookup Fields
- Full and Incremental Reconciliation
- Limited Reconciliation
- Transformation and Validation of Account Data
- Support for the Connector Server
- Support for High-Availability Configuration of the Target System
- Support for Bulk Update of Attributes
- Reconciliation of Deleted User Records

- Reconciliation of Deleted Groups, Roles, and Organizations
- Connection Pooling
- Support for Groovy Scripts

1.6.1 Dependent Lookup Fields

If you have multiple installations of the target system, the entries in lookup definitions (used as an input source for lookup fields during provisioning) can be linked to the target system installation from which they are copied. Therefore, during a provisioning operation, you can select lookup field values that are specific to the target system installation on which the provisioning operation is being performed.

See Lookup Definitions Synchronized with the Target System for more information about the format in which data is stored in dependent lookup definitions.

1.6.2 Full and Incremental Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. In incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into 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.

After you create the application, you can first perform full reconciliation. After the first full reconciliation run, incremental reconciliation is automatically enabled.

See Full Reconciliation and Incremental Reconciliation for more information.

1.6.3 Limited Reconciliation

You can set a reconciliation filter as the value of the Filter attribute of a reconciliation scheduled job. This filter specifies the subset of added and modified target system records that must be reconciled.

See Limited Reconciliation for more information.

1.6.4 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:

- Configuring Transformation of Data During Reconciliation
- Configuring Validation of Data During Reconciliation and Provisioning

1.6.5 Support for the Connector Server

Connector Server is a component provided by ICF. By using one or more connector servers, the connector architecture permits your application to communicate with externally deployed bundles. In other words, a connector server enables remote execution of an Oracle Identity Manager connector.

When you deploy the connector bundle in a connector server, the connector bundle code runs in the same Java Virtual Machine (JVM) as the connector server, rather than in the JVM used by Oracle Identity Manager. Running the Java connector server on a different host can provide performance benefits.

See the following sections for more information:

- Installing and Configuring the Connector Server
- Running the Connector Server
- Installing the Connector in the Connector Server

1.6.6 Support for High-Availability Configuration of the Target System

You can configure the connector for compatibility with high-availability target system environments.

It can read information about backup target system hosts from the failover parameter of the target system IT resource and apply this information when it is unable to connect to the primary host.

For more information about the Failover parameter of the IT resource, see Table 2-2 of Configuring the IT Resource for the Target System.

1.6.7 Support for Bulk Update of Attributes

The connector supports the bulk update of attributes. That is, the connector allows you to update multiple attributes in one operation. With earlier connectors, you could update only one attribute at a time. However, if you specify an invalid value for any of the attributes, none of the attributes are updated. The entire update operation is unsuccessful, and an error is returned. You must then correct any errors in the attribute values and repeat the bulk update operation.

1.6.8 Reconciliation of Deleted User Records

User records that are deleted on the target system are reconciled in Oracle Identity Manager.

1.6.9 Reconciliation of Deleted Groups, Roles, and Organizations

Groups, roles, and organizations that are deleted on the target system are also reconciled in Oracle Identity Manager.

1.6.10 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Manager connectors can use these connections to communicate with target systems. At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads such as network latency, memory allocation, and authentication.

One connection pool is created for each IT resource. For example, if you have three IT resources for three installations of the target system, then three connection pools are created, one for each target system installation.

1.6.11 Support for Groovy Scripts

The connector supports scripts written in the Groovy scripting language.

1.7 Security Considerations for the Connector

These are the security considerations and best practices for the connector.

- Secure Communication to the Target System
- Administrator Account for the Target System

1.7.1 Secure Communication to the Target System

To provide secure communication to the target system, SSL is required. You can configure SSL between Oracle Identity Manager and the Connector Server and between the Connector Server and the target system.

If you do not configure SSL, passwords can be transmitted over the network in clear text. For example, this problem can occur when you are creating a user or modifying a user's password.

For more information, see Configuring SSL for the Connector.

1.7.2 Administrator Account for the Target System

To connect to the target resource using the connector and to perform connector operations such as provisioning and reconciliation, you must specify a target system administrator with specific administrative permissions.

For more information, see Preinstallation on the Target System.

1.8 Lookup Definitions Used During Reconciliation and Provisioning

Lookup definitions used during connector operations are either preconfigured or can be synchronized with the target system.

Lookup definitions used during reconciliation and provisioning can be divided into the following categories:

- Lookup Definitions Synchronized with the Target System
- Preconfigured Lookup Definitions for Languages
- Lookup definitions used with a specific target system:
  - Preconfigured Lookup Definitions for an ODSEE Target System
  - Preconfigured Lookup Definitions for an OUD Target System
  - Preconfigured Lookup Definitions for an OID Target System
  - Preconfigured Lookup Definitions for an eDirectory Target System

1.8.1 Lookup Definitions Synchronized with the Target System

When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the 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 Group Name lookup field to select a group from the list of groups in the lookup field.

The following is the format in which data is stored after lookup definition synchronization:

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 value defined for the code key entry.

Sample value: `3~cn=marketing,ou=groups,dc=example,dc=com`

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 value defined for the decode entry.

Sample value: `DSEE Server~marketing`

For example, in the Lookup.LDAP.Role lookup definition, values will be stored in the following format:

Code Key: <*IT_RESOURCE_KEY*>~<*DISTINGUISHED_NAME*>

Decode: <*IT_RESOURCE_NAME*>~<*DESCRIPTION*>

During a provisioning operation, lookup fields are populated with values corresponding to the target system that you select for the operation.

The following tables list the Oracle Identity Manager lookup definitions that correspond to target system lookup fields and their description:

Table 1-2   Lookup Definitions Synchronized with the Target System

Lookup Definition	Scheduled Task for Synchronization
Lookup.LDAP.Group	You use the LDAP Connector Group Lookup Reconciliation scheduled job to synchronize this lookup definition. This scheduled job is discussed in Scheduled Jobs for Lookup Field Synchronization.
Lookup.LDAP.Role	You use the LDAP Connector Role Lookup Recon scheduled job to synchronize this lookup definition. This scheduled job is discussed in Scheduled Jobs for Lookup Field Synchronization.
Lookup.LDAP.Organization	You use the LDAP Connector OU Lookup Reconciliation scheduled job to synchronize this lookup definition. This scheduled job is discussed in Scheduled Jobs for Lookup Field Synchronization.

Table 1-3   Lookup Definitions Synchronized with the Target System for Oracle Internet Directory

Lookup Definition	Scheduled Task for Synchronization
Lookup.OID.Group	You use the OID Connector Group Lookup Reconciliation scheduled job to synchronize this lookup definition. This scheduled job is discussed in Scheduled Jobs for Lookup Field Synchronization.
Lookup.OID.Organization	You use the OID Connector OU Lookup Reconciliation scheduled job to synchronize this lookup definition. This scheduled job is discussed in Scheduled Jobs for Lookup Field Synchronization.

Table 1-4   Lookup Definitions Synchronized with the Target System for Novell eDirectory

Lookup Definition	Scheduled Task for Synchronization
Lookup.EDIR.UserGroup	You use the eDirectory Connector Group Lookup Reconciliation scheduled job to synchronize this lookup definition. This scheduled job is discussed in Scheduled Jobs for Lookup Field Synchronization.
Lookup.EDIR.AssignedRole	You use the eDirectory Connector Role Lookup Recon scheduled job to synchronize this lookup definition. This scheduled job is discussed in Scheduled Jobs for Lookup Field Synchronization.
Lookup.EDIR.DomainScope	You use the eDirectory Connector Domain Scope Lookup Reconciliation scheduled job to synchronize this lookup definition. This lookup acts as the domain scope for role actions. This scheduled job is discussed in Scheduled Jobs for Lookup Field Synchronization.
Lookup.EDIR.Organization	You use the eDirectory Connector Org Lookup Reconciliation scheduled job to synchronize this lookup definition. This scheduled job is discussed in Scheduled Jobs for Lookup Field Synchronization.
Lookup.EDIR.Profile	You use the eDirectory Connector Profile Lookup Reconciliation scheduled job to synchronize this lookup definition. User can have pre-defined set of profiles in Novell eDirectory and they can be associated while user provisioning. This scheduled job is discussed in Scheduled Jobs for Lookup Field Synchronization.

Note:

Novell eDirectory has additional lookups such as profile, role containers, and domain scope. See Preconfigured Lookup Definitions for an eDirectory Target System.

1.8.2 Preconfigured Lookup Definitions for Languages

The connector comes with preconfigured values of supported languages.

The following lookup definitions contain the language values:

- Lookup.LDAP.Language
- Lookup.OID.Language
- Lookup.EDIR.CommLang

See Certified Languages for the OID Connector for a list of supported languages.

1.9 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.

This section discusses the following topics:

- User Fields for Target Resource Reconciliation
- Group Fields for Reconciliation
- Role Fields for Reconciliation
- Organizational Unit (OU) Fields for Reconciliation
- Reconciliation Rules for Target Resource Reconciliation
- Reconciliation Action Rules for Target Resource Reconciliation

1.9.1 User Fields for Target Resource Reconciliation

The reconciliation attribute map lookup definitions map user resource object fields and target system attributes. These lookup definitions are used for performing target resource user reconciliation runs.

In these lookup definitions, entries are in the following format:

- **Code Key:** Reconciliation field of the resource object
- **Decode:** Name of the target system attribute

Table 1-5 lists the LDAP attributes from which values are fetched during reconciliation. The LDAP Connector User Search Reconciliation or LDAP Connector User Sync Reconciliation scheduled job is used to reconcile user data.

Table 1-5   Entries in the Lookup.LDAP.UM.ReconAttrMap Lookup Definition

Resource Object Field	Target System Field
Common Name	cn
Communication Language	preferredlanguage
Container DN[LOOKUP]	__parentDN__
Department	departmentnumber
Email	mail
First Name	givenname
Group~Group Name[LOOKUP]	ldapGroups
Last Name	sn
Location	l
Middle Initial	initials
NsuniqueID	__UID__
Role~Role Name[LOOKUP]	nsroledn
Status	__ENABLE__
Telephone	telephonenumber
Title	title
User ID	uid

Table 1-6 lists the Oracle Internet Directory attributes from which values are fetched during reconciliation. The OID Connector User Search Reconciliation or OID Connector User Sync Reconciliation scheduled job is used to reconcile user data.

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

Resource Object Field	Target System Field
Common Name	cn
Container DN[LOOKUP]	__parentDN__
Department	departmentnumber
Email	mail
End Date[Date]	orclActiveEndDate=binding.variables.containsKey("orclActiveEndDate")&&orclActiveEndDate!=null?Date.parse('yyyyMMddHHmmss',orclActiveEndDate).getTime():null
First Name	givenname
Last Name	sn
Location	l
manager	manager
Middle Name	initials
orclGuid	__UID__
Preferred Language	preferredlanguage

Table 1-6 (Cont.) Entries in the Lookup.OID.UM.ReconAttrMap Lookup Definition

Resource Object Field	Target System Field
Start Date[Date]	orclActiveStartDate=binding.variables.containsKey("orclActiveStartDate")&&orclActiveStartDate!=null?Date.parse('yyyyMMddHHmmss',orclActiveStartDate).getTime():null
Status	__ENABLE__
Telephone	telephonenumber
TimeZone	orclTimeZone
Title	title
UserGroup~GroupName[LOOKUP]	ldapGroups
User ID	uid

Table 1-7 lists the Novell eDirectory attributes from which values are fetched during reconciliation. The eDirectory Connector User Search Reconciliation scheduled job is used to reconcile user data.

Table 1-7 Entries in the Lookup.EDIR.UM.ReconAttrMap Lookup Definition

Resource Object Field	Target System Field
Communication Language	preferredLanguage
Container DN[LOOKUP]	__PARENTDN__
Department	departmentNumber
Email	mail
entryDN[IGNORE]	entryDN
First Name	givenName
Guid	__UID__
Last Name	sn
Location	l
Logon Script	loginScript
Middle Initial	initials
parentDN[IGNORE]	__PARENTDN__
Profile	profile
refid	__UID__
Role~Inheritance	rbsAssignedRoles~rbsRole~inheritable
Role~Role Name[LOOKUP]	rbsAssignedRoles~rbsRole~__NAME__
Role~Scope[LOOKUP]	rbsAssignedRoles~rbsRole~domainScope
Security Group~Group Name[LOOKUP]	ldapGroups
Status	__ENABLE__
Telephone	telephoneNumber
TimeZone	timezone

Table 1-7 (Cont.) Entries in the Lookup.EDIR.UM.ReconAttrMap Lookup Definition

Resource Object Field	Target System Field
Title	title
User ID	entryDN

1.9.2 Group Fields for Reconciliation

The group lookup definitions map group resource object fields and target system attributes. These lookup definitions are used for performing target resource group reconciliation runs.

Table 1-8 lists the LDAP attributes from which values are fetched during reconciliation. The LDAP Connector Group Search Reconciliation or LDAP Connector Group Sync Reconciliation scheduled job is used to reconcile group data.

Table 1-8 Entries in the Lookup.LDAP.Group.ReconAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Target System Field
Container DN[LOOKUP]	__parentDN__
Group Name	cn
NsuniqueID	__UID__
Org Name	__PARENTRDNVALUE__

Table 1-9 lists the Oracle Internet Directory attributes from which values are fetched during reconciliation. The OID Connector Group Search Reconciliation or OID Connector Group Sync Reconciliation scheduled job is used to reconcile group data.

Table 1-9 Entries in the Lookup.OID.Group.ReconAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Target System Field
Container DN[LOOKUP]	__parentDN__
Group Name	cn
OrclGuid	__UID__
Org Name	__PARENTRDNVALUE__

Table 1-10 lists the Novell eDirectory attributes from which values are fetched during reconciliation. The eDirectory Connector Group Search Reconciliation scheduled job is used to reconcile group data.

Table 1-10 Entries in the Lookup.EDIR.Group.ReconAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Target System Field
GroupName	cn
Guid	__UID__
Organization[LOOKUP]	__PARENTDN__

1.9.3 Role Fields for Reconciliation

The role lookup definitions map role resource object fields and target system attributes. These lookup definitions are used for performing target resource role reconciliation runs.

Table 1-11 lists the LDAP role fields from which values are fetched during reconciliation. The LDAP Connector Role Search Reconciliation or LDAP Connector Role Sync Reconciliation scheduled job is used to reconcile role data.

Table 1-11 Entries in the Lookup.LDAP.Role.ReconAttrMap Lookup Definition

Role Field on Oracle Identity Manager	Target System Field
Container DN[LOOKUP]	__parentDN__
NsuniqueID	__UID__
Org Name	__PARENTRDNVALUE__
Role Name	cn

Table 1-12 lists the Novell eDirectory attributes from which values are fetched during reconciliation. The eDirectory Connector Role Search Reconciliation scheduled job is used to reconcile role data.

Table 1-12 Entries in the Lookup.EDIR.Role.ReconAttrMap Lookup Definition

Role Field on Oracle Identity Manager	Target System Field
Guid	__UID__
Organization[LOOKUP]	__PARENTDN__
RoleName	cn

1.9.4 Organizational Unit (OU) Fields for Reconciliation

The organizational unit fields lookup definitions map organization resource object fields and target system attributes. These lookup definitions are used for performing target resource organization reconciliation runs.

Table 1-13 lists the LDAP organizational unit fields from which values are fetched during reconciliation. The LDAP Connector OU Search Reconciliation or LDAP Connector OU Sync Reconciliation scheduled job is used to reconcile organization data.

Table 1-13 Entries in the Lookup.LDAP.OU.ReconAttrMap Lookup Definition

OU Field on Oracle Identity Manager	Target System Field
Container DN[LOOKUP]	__parentDN__
NsuniqueID	__UID__
Organisation Unit Name	ou
Org Name	__PARENTRDNVALUE__

Table 1-14 lists the Oracle Internet Directory attributes from which values are fetched during reconciliation. The OID Connector OU Search Reconciliation or OID Connector OU Sync Reconciliation scheduled job is used to reconcile organization data.

Table 1-14 Entries in the Lookup.OID.OU.ReconAttrMap Lookup Definition

OU Field on Oracle Identity Manager	Target System Field
Container DN[LOOKUP]	__parentDN__
OrclGuid	__UID__
Organization Unit Name	ou
Org Name	__PARENTRDNVALUE__

Table 1-15 lists the Novell eDirectory attributes from which values are fetched during reconciliation. The eDirectory Connector Org Search Reconciliation scheduled job is used to reconcile organization data.

Table 1-15 Entries in the Lookup.EDIR.OU.ReconAttrMap Lookup Definition

OU Field on Oracle Identity Manager	Target System Field
Container	__PARENTDN__
Guid	__UID__
OrgName	ou

1.9.5 Reconciliation Rules for Target Resource Reconciliation

The connector uses reconciliation rules to determine the identity to which Oracle Identity Manager must assign a resource.

Reconciliation rules for target resource reconciliation are described in the following topics:

- About Reconciliation Rules for Target Resource Reconciliation
- Viewing the Reconciliation Rule for Target Resource Reconciliation

1.9.5.1 About Reconciliation Rules for Target Resource Reconciliation

> **See Also:**
>
> Reconciliation Engine in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for generic information about reconciliation matching and action rules

The reconciliation matching rules are primarily based on the unique identification attribute for the user in the directory. If this attribute match doesn't occur, second level matching is done based on User Login.

The following are the process matching rules:

- **LDAP Rule element:** (NsuniqueID Equals NsuniqueID) OR (User Login Equals User ID)

- **OID Rule element:** (OrclGuid Equals orclGuid) OR (User Login Equals User ID)
- **eDirectory Rule element:** (GUID Equals refid) OR (User Login Equals User ID)

In the first rule component:

- GUID on the left of Equals is the unique ID of the user.
- refid on the right of Equals is the reference ID of the user on the target system.

In the second rule component:

- User Login is the User Login field on the OIM User form.
- User ID is the uid field of the target system.

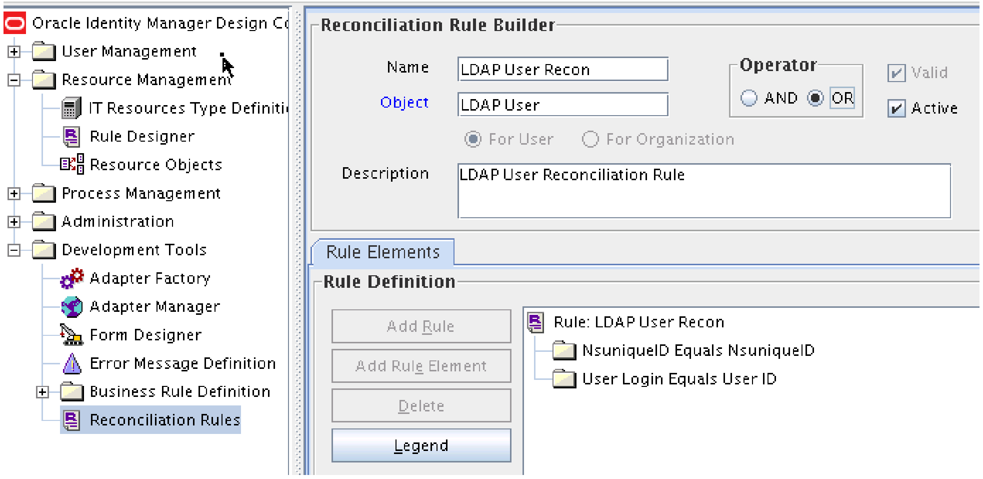
1.9.5.2 Viewing the Reconciliation Rule for Target Resource Reconciliation

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

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

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **LDAP User Recon.** For OID, use **OID User Recon Rule** and for eDirectory, use **eDir Recon User.**

   The following screenshots show the reconciliation rules for target resource reconciliation.



Name: LDAP User Recon

Object: LDAP User

Operator: ○ AND ● OR

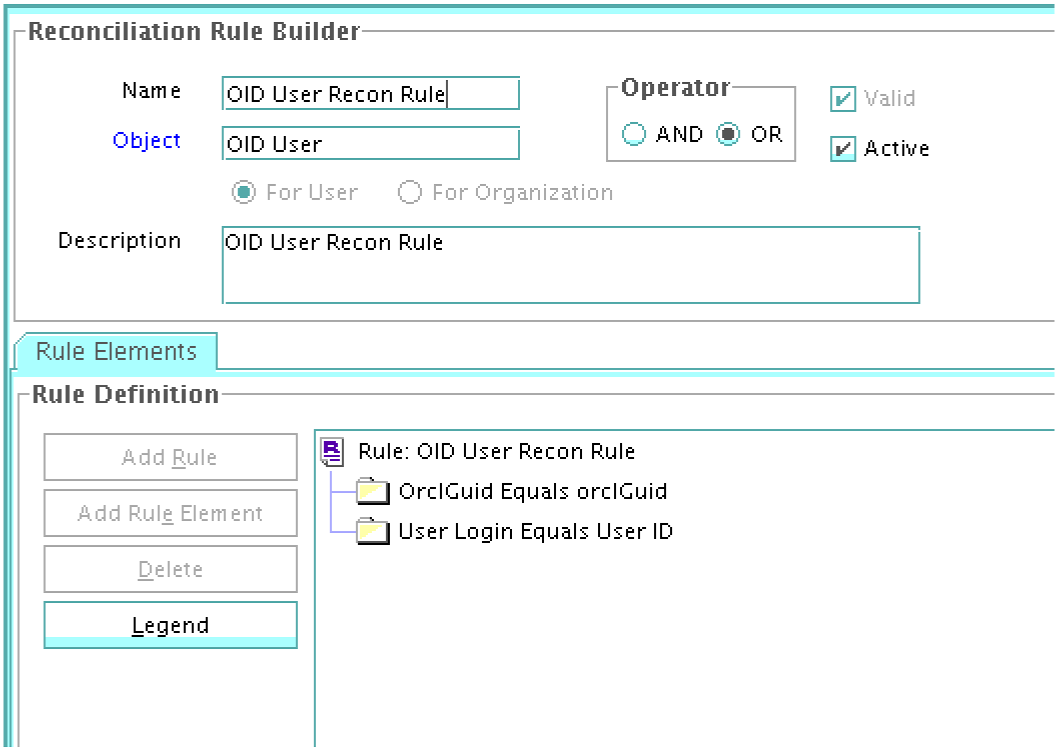
☑ Valid

☑ Active

● For User ○ For Organization

Description: LDAP User Reconciliation Rule

Rule: LDAP User Recon
- NsuniqueID Equals NsuniqueID
- User Login Equals User ID



Name: OID User Recon Rule

Object: OID User

Operator: ○ AND ● OR

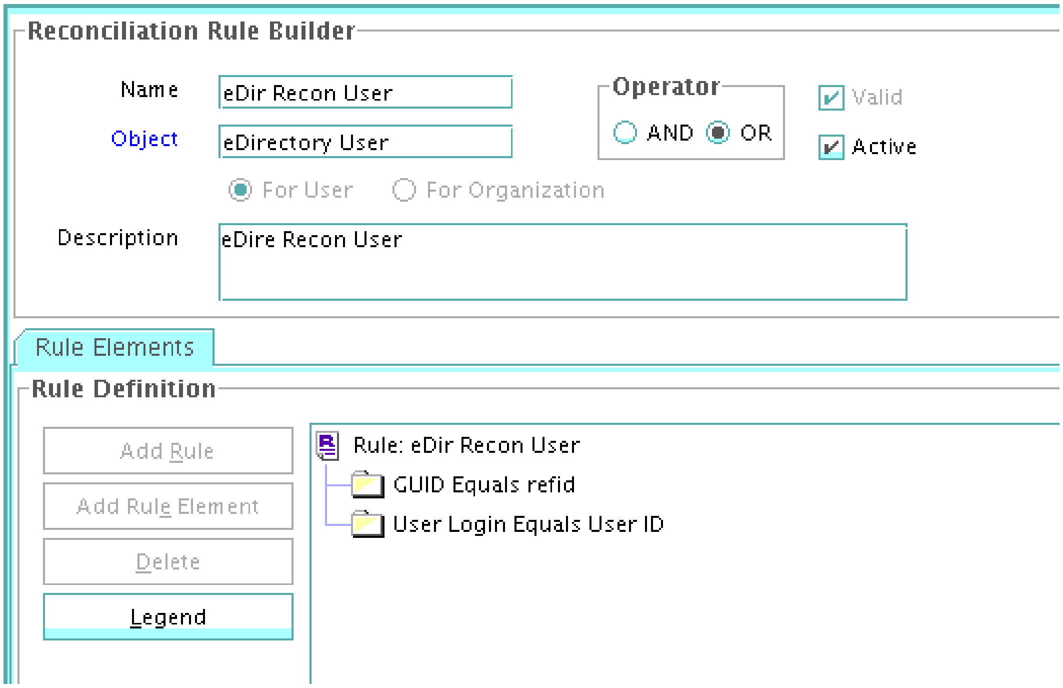
☑ Valid

☑ Active

● For User ○ For Organization

Description: OID User Recon Rule

Rule: OID User Recon Rule
- OrclGuid Equals orclGuid
- User Login Equals User ID



Name: eDir Recon User

Object: eDirectory User

Operator: ○ AND ● OR

☑ Valid

☑ Active

● For User ○ For Organization

Description: eDire Recon User

Rule: eDir Recon User
- GUID Equals refid
- User Login Equals User ID

1.9.6 Reconciliation Action Rules for Target Resource Reconciliation

Reconciliation action rules define the actions the connector must perform based on the reconciliation rules defined for users.

Reconciliation action rules for target resource reconciliation is described in the following topics:

- About Reconciliation Actions Rules for Target Resource Reconciliation
- Viewing Reconciliation Actions Rules for Target Resource Reconciliation

1.9.6.1 About Reconciliation Actions Rules for Target Resource Reconciliation

Table 1-16 lists the action rules for target resource reconciliation.

Table 1-16 Action Rules for Target Resource Reconciliation

Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

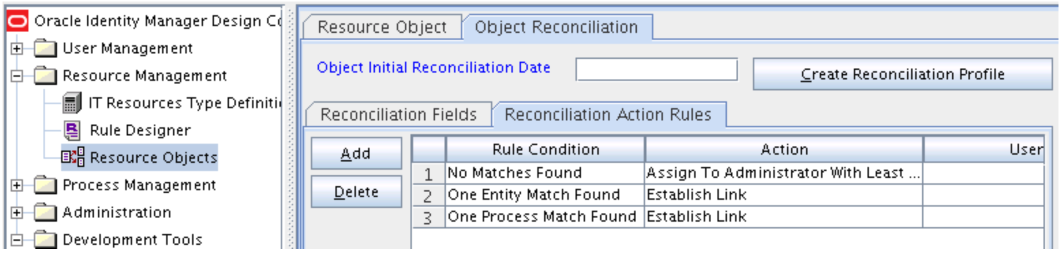
> **Note:**
>
> No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See
>
> - Setting a Reconciliation Action Rule (Developing Identity Connectors using Java)
> - Setting a Reconciliation Action Rule (Developing Identity Connectors using .net)
>
> in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about setting a reconciliation action rule.

1.9.6.2 Viewing Reconciliation Actions Rules for Target Resource Reconciliation

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

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **LDAP User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1-2 shows the reconciliation action rule for target resource reconciliation.

Figure 1-2 Reconciliation Action Rules for Target Resource Reconciliation



	Rule Condition	Action	User
1	No Matches Found	Assign To Administrator With Least ...	
2	One Entity Match Found	Establish Link	
3	One Process Match Found	Establish Link	

1.10 Connector Objects Used During Provisioning

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

This section discusses the following topics:

- Provisioning Functions
- User Fields for Provisioning
- Group Fields for Provisioning
- Role Fields for Provisioning
- Organizational Unit Fields for Provisioning

> **Note:**
>
> The following characters have special considerations for an LDAP DN: , (comma), = (equals), + (plus), < (less than), > (greater than), # (number sign), ; (semicolon), \ (backslash), and " " (quotation marks). If you use any of these characters in User, Group, Organization, or Role process forms, you must escape the character with a backslash (\).

1.10.1 Provisioning Functions

Table 1-17 and Table 1-18 list the supported user provisioning functions and the adapters that perform these functions. The functions listed in the table correspond to either a single or multiple process tasks.

Table 1-17 Provisioning Functions for LDAP and OID Users

Function	Adapter
Create a user account	LDAP CREATE OBJECT
Update a user account	LDAP Update Single - for updating only a single attribute LDAP Update Multi - for updating two or more attributes
Delete a user account	LDAP Delete

Table 1-17 (Cont.) Provisioning Functions for LDAP and OID Users

Function	Adapter
Enable a disabled user account	LDAP Enable
Disable a user account	LDAP Disable
Change or reset the password	LDAP Return Text

Table 1-18 Provisioning Functions for eDirectory Users

Function	Adapter
Create a user account	EDIR CREATE OBJECT
Update a user account	EDIR Update Single - for updating only a single attribute EDIR Update Multi - for updating two or more attributes
Delete a user account	EDIR Delete
Enable a disabled user account	EDIR Enable
Disable a user account	EDIR Disable
Child table operations	EDIR Child Update

Table 1-19 and Table 1-20 list the provisioning functions for groups, roles, and organizational units and the adapters that perform these functions.

Table 1-19 Provisioning Functions for LDAP and OID Groups, Roles, and Organizational Units

Function	Adapter
Create Group, Create Role, and Create Organization	LDAP CREATE OBJECT
Delete Group, Delete Organization, and Delete Role	LDAP Delete
Group Name Update, Role Name Update, and Organization Name Update	LDAP Update
Container DN Update	LDAP Update Single

Table 1-20 Provisioning Functions for eDirectory Groups, Roles, and Organizational Units

Function	Adapter
Create Group, Create Role, and Create Organization	EDIR CREATE OBJECT
Delete Group, Delete Organization, and Delete Role	EDIR Delete
Group Name Update, Role Name Update, and Organization Name Update	EDIR Update

Table 1-20 (Cont.) Provisioning Functions for eDirectory Groups, Roles, and Organizational Units

Function	Adapter
Container DN Update	EDIR Update Single

1.10.2 User Fields for Provisioning

This section discusses the following topics:

- User Fields for Provisioning an ODSEE Target System
- User Fields for Provisioning an OUD Target System
- User Fields for Provisioning an OID Target System
- User Fields for Provisioning an eDirectory Target System

1.10.2.1 User Fields for Provisioning an ODSEE Target System

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

Table 1-21 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-21 Entries in the Lookup.LDAP.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Common Name	cn
Communication Language	preferredlanguage
Container DN[IGNORE,LOOKUP]	ContainerDN
Department	departmentnumber
Email	mail
First Name	givenname
Last Name	sn
Location	l
Login Disabled	__ENABLED__
Middle Name	initials
Name	__NAME__="uid=${User_ID},${Container_DN}"
NsuniqueID	__UID__
Password	__PASSWORD__
Telephone	telephonenumber
Title	title
UD_LDAP_GRP~Group Name[LOOKUP]	ldapGroups
UD_LDAP_ROL~Role[LOOKUP]	nsroledn
User ID	uid

1.10.2.2 User Fields for Provisioning an OUD Target System

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

Table 1-22 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-22 Entries in the Lookup.LDAP.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Common Name	cn
Communication Language	preferredlanguage
Container DN[IGNORE,LOOKUP]	ContainerDN
Department	departmentnumber
Email	mail
First Name	givenname
Last Name	sn
Location	l
Login Disabled	__ENABLED__
Middle Name	initials
Name	__NAME__="uid=${User_ID},${Container_DN}"
NsuniqueID	__UID__
Password	__PASSWORD__
Telephone	telephonenumber
Title	title
UD_LDAP_GRP~Group Name[LOOKUP]	ldapGroups
UD_LDAP_ROL~Role[LOOKUP]	nsroledn
User ID	uid

1.10.2.3 User Fields for Provisioning an OID Target System

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

Table 1-23 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-23 Entries in the Lookup.OID.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Common Name	cn
Container DN[IGNORE,LOOKUP]	ContainerDN
Department	departmentnumber

Table 1-23 (Cont.) Entries in the Lookup.OID.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Email ID	mail
EndDate	orclActiveEndDate=End_Date!=null&&! End_Date.startsWith("1969-12-31")?Date.parse('yyyy-MM-dd', End_Date).format('yyyyMMddHHmmss') + 'Z':null
End Date[IGNORE]	enddate
First Name	givenname
Last Name	sn
Location	l
Login Disabled	__ENABLED__
manager	manager
Middle Name	initials
Name	__NAME__="uid=${User_ID},${Container_DN}"
orclGuid	__UID__
Password	__PASSWORD__
Preferred Language	preferredLanguage
StartDate	orclActiveStartDate=Start_Date!=null&&! Start_Date.startsWith("1969-12-31")?Date.parse('yyyy-MM-dd', Start_Date).format('yyyyMMddHHmmss') + 'Z':null
Start Date[IGNORE]	startdate
Telephone	telephonenumber
Time Zone	orclTimeZone
Title	title
UD_OID_GRP~Group Name[LOOKUP]	ldapGroups
User ID	uid

1.10.2.4 User Fields for Provisioning an eDirectory Target System

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

Table 1-24 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-24 Entries in the Lookup.EDIR.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Password	__PASSWORD__
UD_EDIR_ROL~Role Name[LOOKUP]	rbsAssignedRoles~rbsRole~__NAME__
UD_EDIR_ROL~Inheritable	rbsAssignedRoles~rbsRole~inheritable

Table 1-24 (Cont.) Entries in the Lookup.EDIR.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Logon Script	loginScript
Timezone	timezone
Title	title
Department	departmentNumber
UD_EDIR_ROL~Scope[LOOKUP]	rbsAssignedRoles~rbsRole~domainScope
First Name	givenName
Communication Language	preferredLanguage
Profile[LOOKUP]	profile
Last Name	sn
Guid	__NAME__="cn=${User_ID},${Container_DN}"
User ID	cn
Container DN[IGNORE,LOOKUP]	ContainerDN
Email	mail
Location	l
Telephone	telephonenumber
Reference ID	__UID__
UD_EDIR_GRP~Group Name[LOOKUP]	ldapGroups
Middle Name	initials

1.10.3 Group Fields for Provisioning

The Lookup.LDAP.Group.ProvAttrMap lookup definition maps process form fields for groups and target system attributes from an LDAP target system. This lookup definition is used for performing group provisioning operations.

Table 1-25 lists the group fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-25 Entries in the Lookup.LDAP.Group.ProvAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Target System Field
Container DN[IGNORE,LOOKUP]	container
Group Name	cn
Name	__NAME__="cn=${Group_Name},${Container_DN}"
NsuniqueID	__UID__

The Lookup.OID.Group.ProvAttrMap lookup definition maps process form fields for groups and target system attributes for an Oracle Internet Directory target system. This lookup definition is used for performing group provisioning operations.

Table 1-26 lists the group fields of the OID target system for which you can specify or modify values during provisioning operations.

Table 1-26 Entries in the Lookup.OID.Group.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Container DN[IGNORE,LOOKUP]	container
Group Name	cn
Name	__NAME__="cn=${Group_Name},${Container_DN}"
OrclGuid	__UID__

The Lookup.EDIR.Group.ProvAttrMap lookup definition maps process form fields for groups and target system attributes for an eDirectory target system. This lookup definition is used for performing group provisioning operations.

Table 1-27 lists the group fields of the eDirectory target system for which you can specify or modify values during provisioning operations.

Table 1-27 Entries in the Lookup.EDIR.Group.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Reference ID	__UID__
Container DN[IGNORE,LOOKUP]	ContainerDN
Group Name	cn
Guid	__NAME__="cn=${Group_Name},${Container_DN}"

1.10.4 Role Fields for Provisioning

The Lookup.LDAP.Role.ProvAttrMap lookup definition maps process form fields for roles and target system attributes from an LDAP target system. This lookup definition is used for performing role provisioning operations.

Table 1-28 lists the role fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-28 Entries in the Lookup.LDAP.Role.ProvAttrMap Lookup Definition

Role Field on Oracle Identity Manager	Target System Field
Container DN[IGNORE,LOOKUP]	not used
Name	__NAME__="cn=${Role_Name},${Container_DN}"
NsuniqueID	__UID__
Role Name	cn

The Lookup.EDIR.Role.ProvAttrMap lookup definition maps process for fields for roles and target system attributes for an eDirectory target system. This lookup definition is used for performing role provisioning operations.

Table 1-29 lists the role fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-29   Entries in the Lookup.EDIR.Role.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Role Container[IGNORE,LOOKUP]	ContainerDN
Reference ID	__UID__
Guid	__NAME__="cn=${Role_Name},${Role_Container}"
Role Name	cn

1.10.5 Organizational Unit Fields for Provisioning

The Lookup.LDAP.OU.ProvAttrMap lookup definition maps process form fields for organizations and target system attributes for an LDAP target system. This lookup definition is used for performing organizational unit provisioning operations.

Table 1-30 lists the organizational unit fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-30   Entries in the Lookup.LDAP.OU.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Container DN[IGNORE,LOOKUP]	not used
Name	__NAME__="ou=${Organisation_Unit_Name},${Container_DN}"
NsuniqueID	__UID__
Organisation Unit Name	ou

The Lookup.OID.OU.ProvAttrMap lookup definition maps process form fields for organizations and target system attributes for an Oracle Internet Directory target system. This lookup definition is used for performing group provisioning operations.

Table 1-31 lists the organizational unit fields of the OID target system for which you can specify or modify values during provisioning operations.

Table 1-31   Entries in the Lookup.OID.OU.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Container DN[IGNORE,LOOKUP]	not used
Name	__NAME__="ou=${Organisation_Unit_Name},${Container_DN}"
OrclGuid	__UID__
Organisation Unit Name	ou

The Lookup.EDIR.OU.ProvAttrMap lookup definition maps process form fields for organizations and target system attributes for an eDirectory target system. This lookup definition is used for performing organizational unit provisioning operations.

Table 1-32 lists the organizational unit fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-32 Entries in the Lookup.EDIR.OU.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Organisation Name	ou
Reference ID	__UID__
Guid	__NAME__="ou=${Organisation_Name},${Container_DN}"
Container DN[LOOKUP,IGNORE]	Not used

1.11 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 LDAP Connector Trusted User Reconciliation scheduled job is used to initiate a trusted source reconciliation run. This scheduled task is discussed in Scheduled Jobs for Reconciliation of User Records.

> **See Also:**
>
> Managing Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for conceptual information about trusted source reconciliation.

This section discusses the following topics:

- User Fields for Trusted Source Reconciliation
- Reconciliation Rule for Trusted Source Reconciliation
- Reconciliation Action Rules for Trusted Source Reconciliation

1.11.1 User Fields for Trusted Source Reconciliation

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

Table 1-33 lists the user identity fields whose values are fetched from the LDAP target system during a trusted source reconciliation run.

Table 1-33 Entries in the Lookup.LDAP.UM.ReconAttrMap.Trusted Lookup Definition

OIM User Form Field	Target System Field
Email	mail
First Name	givenname
Last Name	sn

Table 1-33 (Cont.) Entries in the Lookup.LDAP.UM.ReconAttrMap.Trusted Lookup Definition

OIM User Form Field	Target System Field
Middle Name	initials
NsuniqueID	__UID__
Status[TRUSTED]	__ENABLE__
User Login	uid

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

Table 1-34 lists the user identity fields whose values are fetched from the OID target system during a trusted source reconciliation run.

Table 1-34 Entries in the Lookup.OID.UM.ReconAttrMap.Trusted Lookup Definition

OIM User Form Field	Target System Field
Email	mail
First Name	givenname
Last Name	sn
Manager	manager=matcher=java.util.regex.Pattern.compile("uid=(\\w*).*").matcher(manager==null?"":manager);matcher.matches()?matcher[0][1]:null
Middle Name	initials
OrclGuid	__UID__
Status[TRUSTED]	__ENABLE__
User Login	uid

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

Table 1-35 lists the user identity fields whose values are fetched from the eDirectory target system during a trusted source reconciliation run.

Table 1-35 Entries in the Lookup.EDIR.UM.ReconAttrMap.Trusted Lookup Definition

OIM User Form Field	Target System Field
Department Number	departmentNumber
Email	mail
entryDN[IGNORE]	entryDN
Fax	facsimileTelephoneNumber
First Name	givenName
GUID	__UID__

Table 1-35 (Cont.) Entries in the Lookup.EDIR.UM.ReconAttrMap.Trusted Lookup Definition

OIM User Form Field	Target System Field
Last Name	sn
location	l
Pager	pager
parentDN[IGNORE]	__PARENTDN__
Postal Address	postalAddress
Postal Code	postalCode
Status[TRUSTED]	__ENABLE__
Street	street
Telephone	telephoneNumber
Title	title
User ID	entryDN

1.11.2 Reconciliation Rule for Trusted Source Reconciliation

Reconciliation rule for trusted source reconciliation is described in the following topics:

- About Reconciliation Rule for Trusted Source Reconciliation
- Viewing Reconciliation Rules for Trusted Source Reconciliation

> **See Also:**
>
> Reconciliation Engine in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for generic information about reconciliation matching and action rules

1.11.2.1 About Reconciliation Rule for Trusted Source Reconciliation

The following are the process matching rules:

- **LDAP Rule element:** User Login Equals User Login
- **OID Rule element:** User Login Equals User Login
- **eDirectory Rule element:** (GUID Equals GUID) OR (User Login Equals User ID)

  For eDirectory, if the attribute match does not occur, second level matching is done based on User Login.

In this rule element:

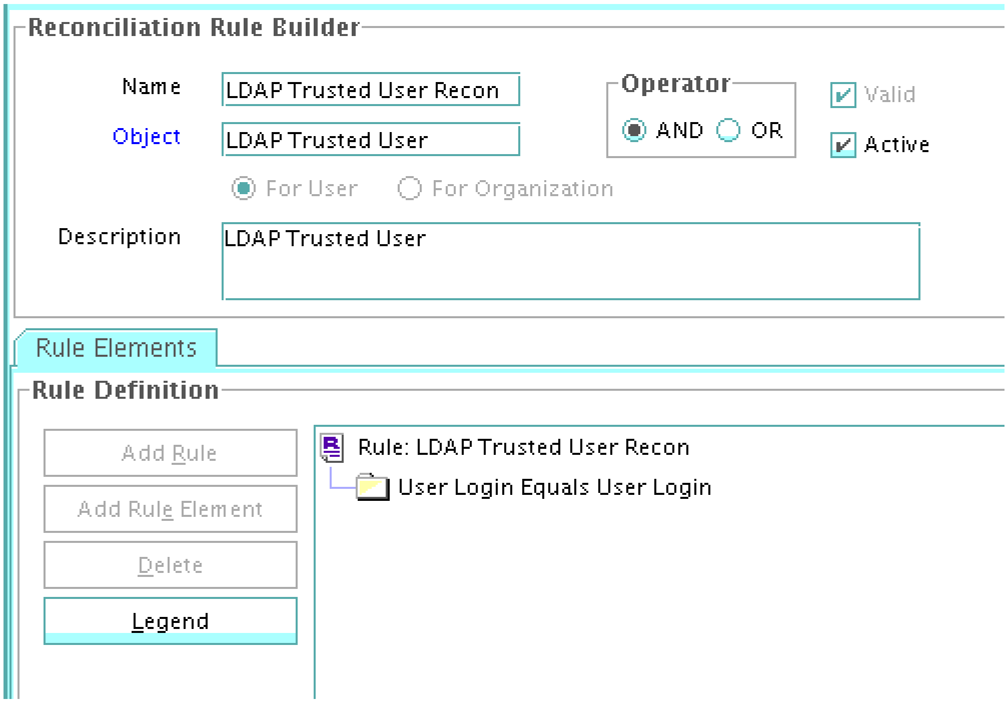
- User Login is the User Login field on the OIM User form.
- User Login is the uid field of the target system.

1.11.2.2 Viewing Reconciliation Rules for Trusted Source Reconciliation

After you deploy the connector, you can view the reconciliation rule for trusted source reconciliation by performing the following steps:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **LDAP Trusted User Recon.** For OID, use **OID Trusted User Recon** and for eDirectory, use **eDirectory User Trusted.**

   The following screenshot shows the reconciliation rule for LDAP trusted source reconciliation:



Reconciliation Rule Builder

Name: LDAP Trusted User Recon

Object: LDAP Trusted User

Operator: ● AND ○ OR

☑ Valid

☑ Active

● For User ○ For Organization

Description: LDAP Trusted User

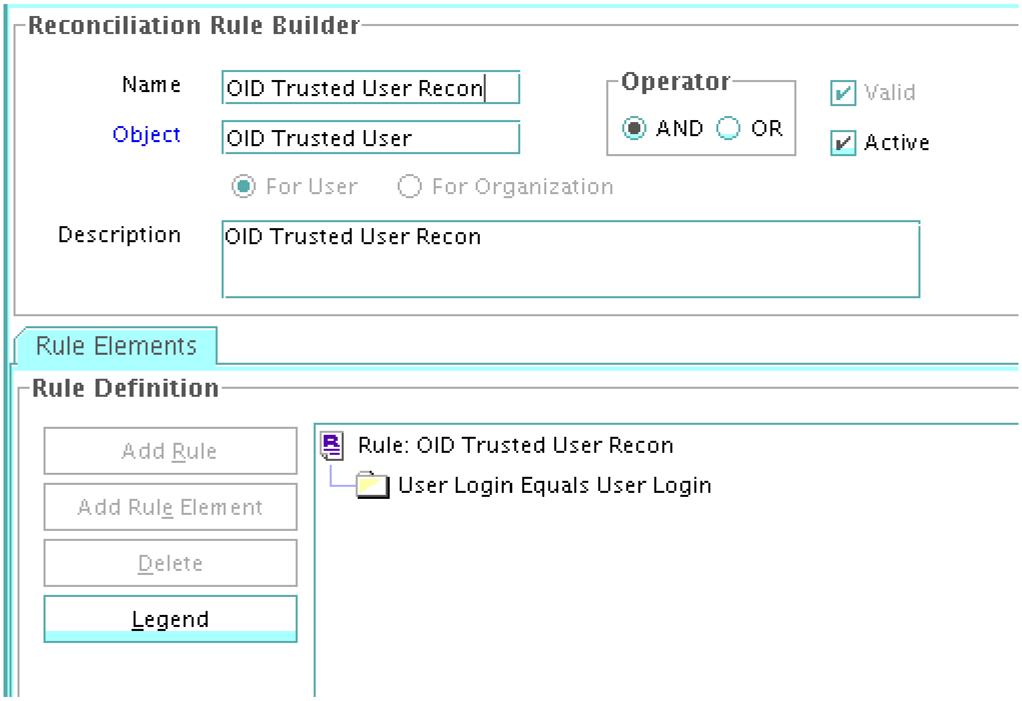
Rule Elements

Rule Definition

Rule: LDAP Trusted User Recon

User Login Equals User Login

The following screenshot shows the reconciliation rule for OID trusted source reconciliation:



Reconciliation Rule Builder

Name: OID Trusted User Recon

Object: OID Trusted User

Operator: ● AND ○ OR

☑ Valid

☑ Active

● For User ○ For Organization

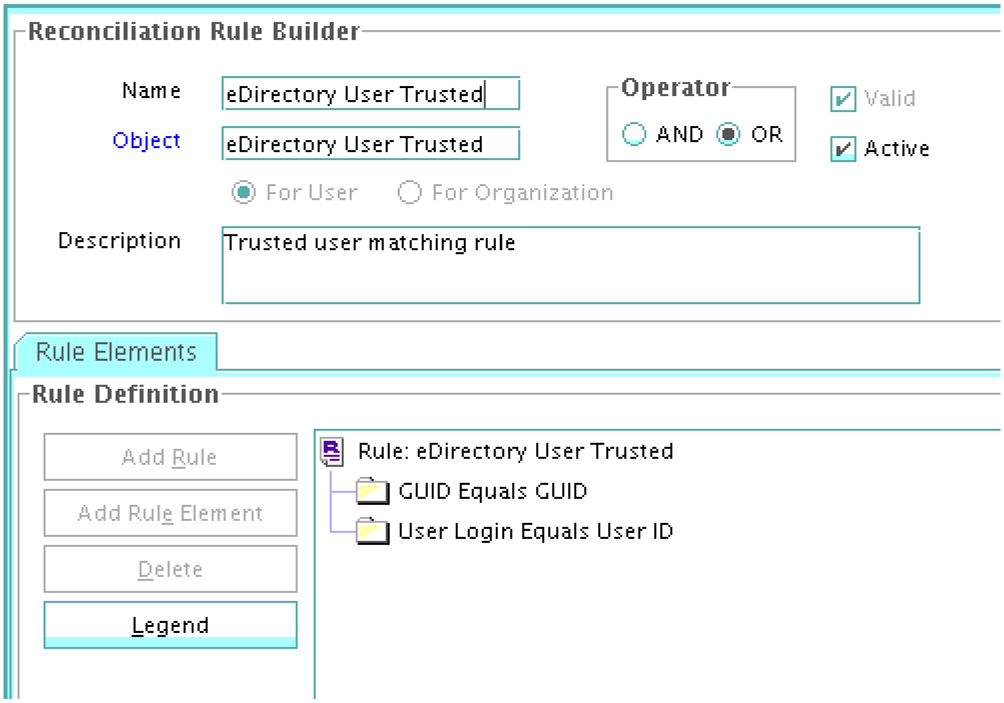
Description: OID Trusted User Recon

Rule Elements

Rule Definition

Rule: OID Trusted User Recon
- User Login Equals User Login

The following screenshot shows the reconciliation rule for eDirectory trusted source reconciliation:



Reconciliation Rule Builder

Name: eDirectory User Trusted

Object: eDirectory User Trusted

Operator: ○ AND ● OR

☑ Valid

☑ Active

● For User ○ For Organization

Description: Trusted user matching rule

Rule Elements

Rule Definition

Rule: eDirectory User Trusted
- GUID Equals GUID
- User Login Equals User ID

1.11.3 Reconciliation Action Rules for Trusted Source Reconciliation

Reconciliation actions rules for trusted source reconciliation is described in the following topics:

- About Reconciliation Action Rules for Trusted Source Reconciliation
- Viewing Reconciliation Action Rules for Trusted Source Reconciliation

1.11.3.1 About Reconciliation Action Rules for Trusted Source Reconciliation

Table 1-36 lists the action rules for trusted source reconciliation.

Table 1-36 Action Rules for Trusted Source Reconciliation

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

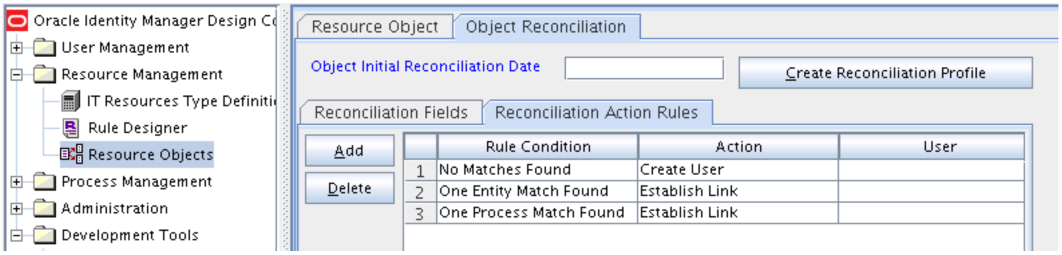
> **Note:**
>
> No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See
>
> - Setting a Reconciliation Action Rule (Developing Identity Connectors using Java)
> - Setting a Reconciliation Action Rule (Developing Identity Connectors using .net)
>
> in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about setting a reconciliation action rule.

1.11.3.2 Viewing Reconciliation Action Rules for Trusted Source Reconciliation

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

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Locate the **LDAP User Trusted** resource object.
5. Click the **Object Reconciliation** tab, and then the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1-3 shows the reconciliation action rule for trusted source reconciliation.

Figure 1-3 Reconciliation Action Rules for Trusted Source Reconciliation



	Rule Condition	Action	User
1	No Matches Found	Create User	
2	One Entity Match Found	Establish Link	
3	One Process Match Found	Establish Link	

1.12 Roadmap for Deploying and Using the Connector

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

- Deploying the Connector describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Using the Connector provides information that is common to all target systems.
- Using the Connector with Oracle Directory Server Enterprise Edition provides information about using the connector with Oracle Directory Server Enterprise Edition (ODSEE).
- Using the Connector with Oracle Unified Directory provides information about using the connector with Oracle Unified Directory (OUD).
- Using the Connector with Oracle Internet Directory provides information about using the connector with Oracle Internet Directory (OID).
- Using the Connector with Novell eDirectory provides information about using the connector with Novell eDirectory.
- Using the Connector with an LDAPv3 Compliant Directory provides information about using the connector with an with an LDAPv3 compliant directory.
- Extending the Functionality of the Connector describes procedures that you can perform if you want to extend the functionality of the connector.
- Troubleshooting lists solutions to errors that you may encounter while using the connector.
- Known Issues and Workarounds lists known issues associated with this release of the connector.

2
Deploying the Connector

The procedure to deploy the connector is divided across three stages namely preinstallation, installation, postinstallation. upgrading the Oracle Internet Directory Connector, and cloning the Oracle Internet Directory Connector.

The following topics discuss these stages:

- Preinstallation
- Installation
- Postinstallation
- Uninstalling the Connector
- Upgrading the Connector
- Postcloning Steps

2.1 Preinstallation

Preinstallation of the Oracle Internet Directory connector involves creating a target system user account for creating, modifying, and deleting entries related to the managed objects, including accounts, groups, roles (if supported), and organizational units (OU), update passwords for users; installing and configuring the connector server; running the connector server; configuring SSL for the connector; and enabling logging for the connector.

Preinstallation information is divided across the following sections:

- Preinstallation on the Target System
- Installing and Configuring the Connector Server
- Running the Connector Server
- Configuring SSL for the Connector
- Enabling Logging for the Connector

2.1.1 Preinstallation on the Target System

The connector uses a target system account to connect to the target system during reconciliation and provisioning operations. Preinstallation involves creating a target system user account for performing the following functions:

- Create, modify, and delete entries related to the managed objects, including accounts, groups, roles (if supported), and organizational units (ou).
- Update passwords for users.
- Use paging controls that have been configured in the IT resource.

Depending on the target system, create the specific target system account for connector operations as follows:

- Create an admin user account on the ODSEE target system.
- Create an admin user account on the OUD target system.
- Create an admin user, admin group, and ACIs on the OID target system.

  To perform this task, you must be an administrator on the OID target system who is familiar with command-line utilities such as `ldapsearch` and `ldapmodify`. If you prefer, you can also use Oracle Directory Services Manager to perform these functions.
- Create an admin user account on the eDirectory target system.

The detailed instructions for performing these preinstallation tasks are available in the product documentation of the target system.

2.1.2 Installing and Configuring the Connector Server

This section contains the following topics:

- About Installing and Configuring the Connector Server
- Installing and Configuring the Java Connector Server

2.1.2.1 About Installing and Configuring the Connector Server

You can deploy this connector either locally in Oracle Identity Manager or remotely in the Connector Server. A **Connector Server** enables remote execution of an Identity Connector.

Connector Servers are available in two implementations:

- As a .Net implementation that is used by Identity Connectors implemented in .Net
- As a Java implementation that is used by Java-based Identity Connectors

2.1.2.2 Installing and Configuring the Java Connector Server

Use the following steps to install and configure the Java Connector Server:

> **Note:**
>
> Before you deploy the Java Connector Server, ensure that you install JDK or JRE on the same computer where you are installing the Java Connector Server and that your *JAVA_HOME* or *JRE_HOME* environment variable points to this installation.

1. Download the Java Connector Server package from the Oracle Technology Network.
2. Create a new directory on the computer where you want to install the Connector Server.

> **Note:**
>
> In this guide, *CONNECTOR_SERVER_HOME* represents this directory.

3. Unzip the Java Connector Server package in the new directory created in Step 1.
4. Open the ConnectorServer.properties file located in the conf directory. In the ConnectorServer.properties file, set the following properties, as required by your deployment.

Property	Description
connectorserver.port	Port on which the Java Connector Server listens for requests. Default value: `8759`
connectorserver.bundleDir	Directory where the connector bundles are deployed. Default value: `bundles`
connectorserver.libDir	Directory in which to place dependent libraries. Default value: `lib`
connectorserver.usessl	If set to **`true`**, the Java Connector Server uses SSL for secure communication. Default value: `false` If you specify **`true`**, use the following options on the command line when you start the Java Connector Server: • `-Djavax.net.ssl.keyStore` • `-Djavax.net.ssl.keyStoreType` (*optional*) • `-Djavax.net.ssl.keyStorePassword` When you run the preceding options on the command line, you must set values for them. To set values for these options on the command line, you must prefex them with `-J.` Sample value: `-J-Djavax.net.ssl.keyStore=mykeystore.jks` See also Configuring SSL for the Connector.
connectorserver.ifaddress	Bind address. To set this property, uncomment it in the file (if necessary). The bind address can be useful if there are more NICs installed on the computer.
connectorserver.key	Java Connector Server key.

5. Set the properties in the ConnectorServer.properties file, as follows:
   - To set the connectorserver.key, run the Java Connector Server with the `/setKey` option.

     > **Note:**
     >
     > For more information, see Running the Connector Server.

   - For all other properties, edit the ConnectorServer.properties file manually.
6. The conf directory also contains the logging.properties file, which you can edit if required by your deployment.

Note:

Oracle Identity Manager has no built-in support for testing the Connector Server configuration.

2.1.3 Running the Connector Server

This section describes how to run the Connector Server, depending on your operating system:

- Running the Connector Server on UNIX and Linux Systems
- Running the Connector Server on Microsoft Windows Systems

See Also:

Using the Java Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about a Java Connector Server.

2.1.3.1 Running the Connector Server on UNIX and Linux Systems

To run the Connector Server on UNIX and Linux systems, use the connectorserver.sh script, as follows:

1. Make sure that you have set the properties required by your deployment in the ConnectorServer.properties file, as described in Installing and Configuring the Connector Server.
2. Navigate to the *CONNECTOR_SERVER_HOME*/bin directory.
3. Use the `chmod` command to set the permissions to make the connectorserver.sh script executable.
4. Run the connectorserver.sh script. The script supports the following options.

Option	Description
`/run [ -Jjava-option]`	Runs the Connector Server in the console. Optionally, you can specify one or more Java options. For example, to run the Connector Server with SSL: `./connectorserver.sh /run -J-Djavax.net.ssl.keyStore=mykeystore.jks -J-Djavax.net.ssl.keyStorePassword=password`
`/start [ -Jjava-option ]`	Runs the Connector Server in the background. Optionally, you can specify one or more Java options.
`/stop`	Stops the Connector Server, waiting up to 5 seconds for the process to end.
`/stop n`	Stops the Connector Server, waiting up to *n* seconds for the process to end.

Option	Description
`/stop -force`	Stops the Connector Server. Waits up to 5 seconds and then uses the kill -KILL command, if the process is still running.
`/stop` *`n`* `-force`	Stops the Connector Server. Waits up to *n* seconds and then uses the kill -KILL command, if the process is still running.
`/setKey` *`key`*	Sets the Connector Server key. The connectorserver.sh script stores the hashed value of *key* in the connectorserver.key property in the ConnectorServer.properties file.

2.1.3.2 Running the Connector Server on Microsoft Windows Systems

To run the Connector Server on Microsoft Windows systems, use the ConnectorServer.bat script as follows:

1. Make sure that you have set the properties required by your deployment in the ConnectorServer.properties file, as described in Installing and Configuring the Connector Server.
2. Navigate to the *CONNECTOR_SERVER_HOME*\bin directory and run the ConnectorServer.bat script.

   The ConnectorServer.bat script supports the following options:

Option	Description
`/install [`*`serviceName`*`] ["-J` *`java-option`*`"]`	Installs the Connector Server as a Windows service. Optionally, you can specify a service name and Java options. If you do not specify a service name, the default name is ConnectorServerJava.
`/run ["-J` *`java-option`*`"]`	Runs the Connector Server from the console. Optionally, you can specify Java options. For example, to run the Connector Server with SSL: `ConnectorServer.bat /run "-J-Djavax.net.ssl.keyStore=mykeystore.jks" "-J-Djavax.net.ssl.keyStorePassword=`***`password`***`"`
`/setKey [`*`key`*`]`	Sets the Connector Server key. The ConnectorServer.bat script stores the hashed value of the key in the connectorserver.key property in the ConnectorServer.properties file.
`/uninstall [`*`serviceName`*`]`	Uninstalls the Connector Server. If you do not specify a service name, the script uninstalls the ConnectorServerJava service.

3. To stop the Connector Server, stop the respective Windows service.

2.1.4 Configuring SSL for the Connector

This section describes how to configure SSL for the connector, including:

- Configuring SSL on the Target System
- Configuring the Connector Server for SSL
- Configuring Oracle Identity Manager for SSL

> **Caution:**
>
> Configuring SSL is an optional procedure; however, it is recommended that you configure SSL. If you do not configure SSL, passwords can be transmitted over the network in clear text. For example, this problem can occur when you are creating a user or modifying a user's password.

2.1.4.1 Configuring SSL on the Target System

To configure SSL on the target system:

1. On the target system, ensure that SSL is enabled and a port is specified for the Directory Server to accept connections from LDAPS clients.

   For more information, refer to the documentation for your specific target system .
2. Generate a self-signed certificate.
3. Export the public key for the certificate you generated in the previous step.

   For example, on an OUD target system:

   ```
   keytool -exportcert -alias server-cert -file config/server-cert.txt -rfc
   -keystore config/keystore -storetype JKS
   ```

   Or, on an ODSEE target system:

   ```
   odsee-instance/bin/dsadm export-cert -o /tmp/odsee.cert . defaultCert
   ```

   Or, on an eDirectory target system, you can export the trust certificate from the JDK key store on which eDirectory is installed:

   ```
   keytool -J-ns -import -alias ALIAS_NAME -file FULL_PATH\trustedrootcert.der -
   keystore sys:java\lib\security\cacerts
   ```

   Choose and confirm the PKCS#12 file password.
4. Import the server certificate into the JRE of the target system.

   For example, on an OUD target system:

   ```
   keytool -importcert -alias server-cert -file config/server-cert.txt
   -keystore config/truststore -storetype JKS
   ```

2.1.4.2 Configuring the Connector Server for SSL

To configure the Connector Server for SSL:

1. Create a certificate store and add the certificate generated on the target system to the store. For example, on a Windows system:

   ```
   C:\>certutil -f -addstore sslstore C:\target.cert
   ```

   This command creates a new certificate store named sslstore and adds the certificate in target.cert to this store.

> **Note:**
>
> Ensure that the certificate store with the name used in the preceding command does not already exist. That is, the certificate store used in the ConnectorServer.properties file must have only one certificate. If more than one certificate exists in the certificate store, the Connector Server will not start.
>
> To view the number of certificates in the certificate store, use the certutil command. For example, on Windows:
>
> ```
> C:\>certutil -viewstore sslstore
> ```

2. In the ConnectorServer.properties file, set the following values:

   ```
   <add key="connectorserver.usessl" value="true" />
   <add key="connectorserver.certificatestorename" value="sslstore" />
   ```

   In this example, sslstore is the name of the certificate store.

3. Restart the Connector Server.

   On a Windows system, use the ConnectorServer.bat script. For example:

   ```
   ConnectorServer.bat /run
   "-J-Djavax.net.ssl.keyStore=sslstore
   "-J-Djavax.net.ssl.keyStorePassword=password"
   ```

   On a UNIX or Linux system, use the ConnectorServer.sh script. For example:

   ```
   ./connectorserver.sh /run
   -J-Djavax.net.ssl.keyStore=sslstore
   -J-Djavax.net.ssl.keyStorePassword=password
   ```

4. Set the `UseSSL` IT Resource parameter for the Connector Server to true, as described in Creating the IT Resource for the Connector Server.

2.1.4.3 Configuring Oracle Identity Manager for SSL

To configure Oracle Identity Manager for SSL:

1. Import the target system certificate into the JDK (or JRE) used by Oracle Identity Manager. For example:

   ```
   keytool -import -keystore my_cacerts -file cert_file_name -storepass password
   ```

   In this command:

   - *`my_cacerts`* is the full path and name of the certificate store (the default is cacerts).
   - *`cert_file_name`* is the full path and name of the certificate file.
   - *`password`* is the password of the keystore.

   For example:

   ```
   keytool -import -keystore /home/OIM/java/jdk/lib/security/cacerts
   -file /home/target.cert -storepass kspassword
   ```

2. Import the target system certificate into the Oracle WebLogic Server keystore. For example:

```
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.

For example:

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

2.1.5 Enabling Logging for the Connector

This section describes the following topics:

- Enabling Logging on Oracle Identity Manager
- Enabling Logging on the Connector Server

2.1.5.1 Enabling Logging on Oracle Identity Manager

This section contains the following topics:

- About Enabling Logging on Oracle Identity Manager
- Enabling Logging on Oracle WebLogic Server

2.1.5.1.1 About Enabling Logging on Oracle Identity Manager

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. Oracle Identity Manager uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger.

To specify the type of event for which you want logging to take place, 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 prevent Oracle Identity Manager from 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 2-1.

Table 2-1 Log Levels and ODL Message Type: Level Combinations

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

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

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

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

2.1.5.1.2 Enabling Logging on Oracle WebLogic Server

To enable logging on Oracle WebLogic Server:

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

```
<log_handler name='OIMCP.LDAP' 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.LDAP" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="OIMCP.LDAP"/>
     <handler name="console-handler"/>
   </logger>
```

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2-1 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='OIMCP.LDAP' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers
\oim_server1\logs\oim_server1-diagnostic-1.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="ORG.IDENTITYCONNECTORS.LDAP" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="OIMCP.LDAP"/>
     <handler name="console-handler"/>
   </logger>
```

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

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

   For Microsoft Windows:

   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:

   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

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

2.1.5.2 Enabling Logging on the Connector Server

This section contains the following topics:

- About Enabling Logging on the Connector Server
- Enabling Logging for the Connector Server

2.1.5.2.1 About Enabling Logging on the Connector Server

When you enable logging, the connector server stores in a log file information about events that occur during the course of provisioning and reconciliation operations for different statuses. By default, the connector server logs are set at INFO level and you can change this level to any one of the following:

- Error

  This level enables logging of information about errors that might allow connector server 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 operation.
- FINE, FINER, FINEST

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

2.1.5.2.2 Enabling Logging for the Connector Server

To enable the logging information for the Connector Server:

1. Navigate to the *CONNECTOR_SERVER_HOME*/Conf directory.
2. Open the logging.properties file in a text editor.
3. Edit the following entry by replacing INFO with the required level of logging:

   ```
   .level=INFO
   ```
4. Save and close the file.
5. Restart the connector server.

2.2 Installation

You must install the Oracle Internet Directory connector in Oracle Identity Manager and if required, place the connector code bundle in the Connector Server.

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

- To run the connector code locally in Oracle Identity Manager, perform the procedure described in Installing the Connector in Oracle Identity Manager.
- To run the connector code remotely in a Connector Server, perform the procedures described in Installing the Connector in Oracle Identity Manager and Installing the Connector in the Connector Server.

2.2.1 Installing the Connector in Oracle Identity Manager

Installation on Oracle Identity Manager consists of the following procedures:

- Running the Connector Installer
- Configuring the IT Resource for the Target System

2.2.1.1 Running the Connector Installer

To run the Connector Installer:

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

   OIM_HOME/server/ConnectorDefaultDirectory

2. If you are using Oracle Identity Manager release 11.1.1.*x*, then:

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

   b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector.**

3. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then:

   a. Log in to Oracle Identity System Administration.

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

4. In the Connector Management page, click **Install.**

5. From the Connector List list, select **OID/LDAP/EDIR Connector *RELEASE_NUMBER.***

   This list displays the names and release numbers of connectors whose installation files you copied into the default connector installation directory in Step 1. Select the connector for your specific target system.

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

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

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

   c. From the Connector List list, select **ODSEE/OUD/LDAPV3 Connector *RELEASE_NUMBER.***

6. Click **Load**.

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

   The following tasks are performed, in sequence:

   a. Configuration of Connector Libraries

   b. Import of the Connector XML Files (Using Deployment Manager)

   c. Compilation of Adapter Definitions

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure is displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

   - Retry the installation by clicking **Retry.**
   - Cancel the installation and begin again from Step 1.

8. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of steps that you must perform after the installation is displayed. These steps are as follows:

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

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

b. Configuring the IT resource for the connector

   The procedure to configure the IT resource is described later in this guide.

c. Configuring the scheduled jobs

   The procedure to configure these scheduled jobs is described later in this guide.

When you run the Connector Installer, it copies the connector files to destination directories on the Oracle Identity Manager host computer. These files are listed in Files and Directories on the OID Connector Installation Media.

2.2.1.2 Configuring the IT Resource for the Target System

> **Note:**
>
> If you have configured your target system as a trusted source, then create an IT resource of type **OID.** For example, OID Trusted. The parameters of this IT resource are the same as the parameters of the IT resources described in Table 2-2 of this section. See Creating IT Resources in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about creating an IT resource.

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

You must specify values for the parameters of the target system IT resource as follows:

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

   - For Oracle Identity Manager release 11.1.1.*x*:

     Log in to the Administrative and User Console

   - For Oracle Identity Manager release 11.1.2.*x* or later:

     Log in to Oracle Identity System Administration

2. If you are using Oracle Identity Manager release 11.1.1.*x*, then:

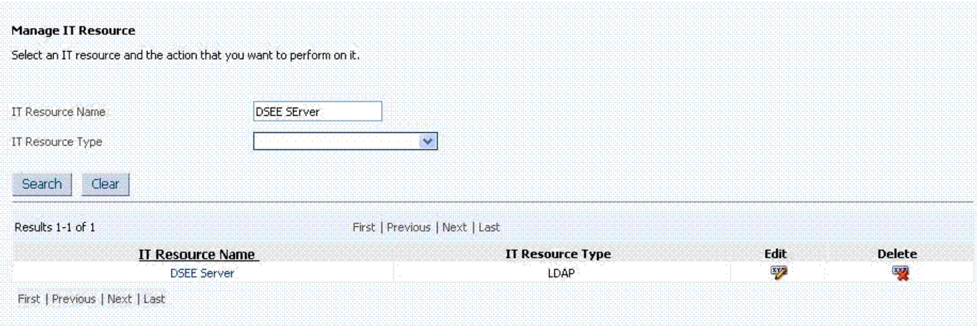
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.

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

3. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then:
   a. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see Managing Sandboxes of *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
   b. In the left pane, under Configuration, click **IT Resource.**
4. In the IT Resource Name field on the Manage IT Resource page, enter `DSEE Server`, `OID Server`, or `eDirectory Server` and click **Search.**

   Alternatively, from the IT Resource Type list, you can select **LDAP**, **OID Server**, or **eDirectory Server** and then click **Search.** Figure 2-1 shows the Manage IT Resource page.

Figure 2-1   Manage IT Resource Page



Manage IT Resource

Select an IT resource and the action that you want to perform on it.

IT Resource Name	DSEE SErver
IT Resource Type	

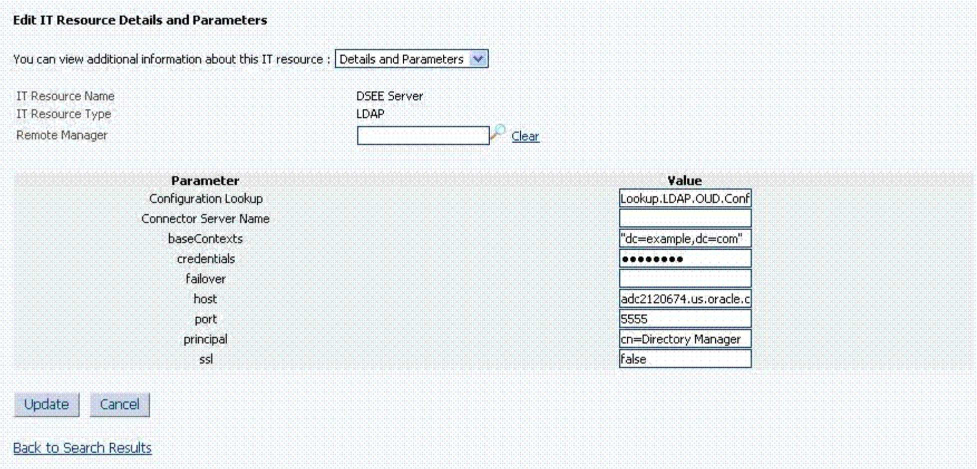
Results 1-1 of 1   First | Previous | Next | Last

IT Resource Name	IT Resource Type	Edit	Delete
DSEE Server	LDAP		

First | Previous | Next | Last

5. Click the edit icon corresponding to the DSEE Server or OID Server IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Figure 2-2 shows the Edit IT Resource Details and Parameters page.

Figure 2-2   Edit IT Resource Details and Parameters Page for the Target System IT Resource



Edit IT Resource Details and Parameters

You can view additional information about this IT resource : Details and Parameters

IT Resource Name	DSEE Server
IT Resource Type	LDAP
Remote Manager	

Parameter	Value
Configuration Lookup	Lookup.LDAP.OUD.Conf
Connector Server Name	
baseContexts	"dc=example,dc=com"
credentials	••••••••
failover	
host	adc2120674.us.oracle.c
port	5555
principal	cn=Directory Manager
ssl	false

Table 2-2 describes each parameter of the IT resource.

Table 2-2 Parameters of the IT Resource for the Target System

Parameter	Description

host	Enter the host name or IP address of the target system.
	Sample values:
	`myhost`
	`172.20.55.120`

port	Enter the port number to connect to the target system. Sample value: `1389`
ssl	Specifies whether communication with the target system must be secured using SSL. Default value: `true` **Note:** You can set the value to true, when SSL is enabled between Oracle Identity Manager and the Connector Server or between Oracle Identity Manager and the target system.To configure SSL between Oracle Identity Manager and the Connector Server, see the "connectorserver.usessl" property in Step 4 of Installing and Configuring the Connector Server. See also Configuring SSL for the Connector.
principal	Enter the bind DN for performing operations on the target system. For example: For ODSEE or OUD: `cn=Directory Manager` For OID: `cn=orcladmin` For eDirectory: `cn=Admin,dc=idc` **Note**. For eDirectory, the bind DN should be the complete DN name.
credentials	Enter the bind password associated with the bind DN.
failover	Enter the complete URL of LDAP backup server or servers that the connector must switch to if the primary LDAP server fails or becomes unavailable. The URL is a fully qualified host name or an IP address in the following format: ldap://*host*:*port* The following example shows an IP address for one backup LDAP server: `ldap://172.20.55.191:389` If you specify more than one URL, each URL must be enclosed in double quotes (") and separated by a comma (,). For example: `"ldap://172.20.55.191:389","ldap://172.20.55.171:387"`
baseContexts	Enter the base contexts for operations on the target system. Sample value: `"dc=example,dc=com"` **Note:** In a multilevel base context, each base context must be specified within double quotes (") and separated by a comma (,). For example, `"dc=example,dc=com","dc=mydc,dc=com"`

Table 2-2 (Cont.) Parameters of the IT Resource for the Target System

Parameter	Description
Configuration Lookup	Enter the name of the lookup definition that stores configuration information used during reconciliation and provisioning. If you have configured your target system as a target resource, then enter one of the following values: • For ODSEE: `Lookup.LDAP.Configuration` • For OUD: `Lookup.LDAP.OUD.Configuration` • For OID: `Lookup.OID.Configuration` • For eDirectory: `Lookup.EDIR.Configuration` If you have configured your target system as a trusted source, then enter one of the following values: • For ODSEE: `Lookup.LDAP.Configuration.Trusted` • For OUD: `Lookup.LDAP.OUD.Configuration.Trusted` • For OID: `Lookup.OID.Configuration.Trusted` • For eDirectory: `Lookup.EDIR.Configuration.Trusted`
Connector Server Name	Name of the IT resource of the type "Connector Server." You create an IT resource for the Connector Server in Creating the IT Resource for the Connector Server. **Note:** Enter a value for this parameter only if you have deployed this connector in the Connector Server.

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

2.2.2 Installing the Connector in the Connector Server

To deploy the connector bundle remotely in a Connector Server, you must first deploy the connector in Oracle Identity Manager, as described in Installing the Connector in Oracle Identity Manager.

> **Note:**
>
> You can download the Connector Server from the Oracle Technology Network web page. If you need to set up the Connector Server, see Installing and Configuring the Connector Server.

To install the connector in the Connector Server:

1. Stop the Connector Server.
2. Copy the connector bundle to the Connector_Server_Home/bundles directory.
3. Restart the Connector Server.
4. Create an IT resource of type "Connector Server" and point it to the Connector Server.
5. Update the "Connector Server" field name in the connector IT resource with the Connector Server IT resource name.
6. Stop the Connector Server.

> **Note:**
>
> You can download the necessary Connector Server from the Oracle Technology Network web page.

7. From the installation media, copy the bundle/org.identityconnectors.ldap-1.0.6380.jar file to the *CONNECTOR_SERVER_HOME*/bundles directory.
8. Start the Connector Server for the connector bundle to be picked up by the Connector Server.

2.3 Postinstallation

Postinstallation steps are divided across the following sections:

- Postinstallation on Oracle Identity Manager
- Creating the IT Resource for the Connector Server

2.3.1 Postinstallation on Oracle Identity Manager

Configuring Oracle Identity Manager involves performing the following procedures:

- Configuring Oracle Identity Manager 11.1.2 or Later
- Localizing Field Labels in UI Forms
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Setting up the Lookup Definition for Connection Pooling
- Setting Up the OID Configuration Lookup Definition for LDAP Operation Timeouts
- Configuring Oracle Identity Manager for Request-Based Provisioning

2.3.1.1 Configuring Oracle Identity Manager 11.1.2 or Later

> **Note:**
>
> You need not perform the procedures described in this section if you have configured your target system as a trusted source.

If you are using Oracle Identity Manager release 11.1.2 or later, you must create additional metadata such as a UI form and an application instance. 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
- Publishing a Sandbox
- Harvesting Entitlements and Sync Catalog

2.3.1.1.1 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see Managing Sandboxes of *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

1. Log in to Oracle Identity System Administration.
2. In the upper right corner of the page, click the **Sandboxes** link.

   The Manage Sandboxes page is displayed.
3. On the toolbar, click **Create Sandbox.**
4. In the Create Sandbox dialog box, enter values for the following fields:
   - **Sandbox Name:** Enter a name for the sandbox.
   - **Sandbox Description:** Enter a description of the sandbox.
5. Click **Save and Close.**
6. Click **OK** on the confirmation message that is displayed.

   The sandbox is created and displayed in the Available Sandboxes section of the Manage Sandboxes page.
7. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.
8. On the toolbar, click **Activate Sandbox.**

   The sandbox is activated.

2.3.1.1.2 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see Managing Forms in *Oracle Fusion Middleware Administering Oracle Identity Manager.*

1. In the left pane, under Configuration, click **Form Designer.** The Form Designer page is displayed.
2. From the Actions menu, select **Create.** Alternatively, click **Create** on the toolbar. The Create Form page is displayed.
3. On the Create Form page, enter values for the following UI fields:
   - **Resource Type:** Select the resource object that you want to associate the form with. For example, **AD User.**
   - **Form Name:** Enter a name for the form.
4. Click **Create.**

   A message is displayed stating that the form is created.

2.3.1.1.3 Creating an Application Instance

Create an application instance as follows. For detailed instructions, see Managing Application Instances in *Oracle Fusion Middleware Administering Oracle Identity Manager.*

1. In the left pane of Identity System Administration, 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 **AD User.**
   - **IT Resource Instance:** The IT resource instance name. Click the search icon next to this field to search for and select **Active Directory.**
   - **Form:** Select the form name (created in Creating a New UI Form). If the newly created form is not visible, then click the **Refresh** icon adjacent to the Form field.
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 Managing Organizations Associated With Application Instances in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed instructions.

2.3.1.1.4 Publishing a Sandbox

To publish the sandbox that you created in Creating and Activating a Sandbox:

1. Close all the open tabs and pages.
2. In the upper right corner of the page, click the **Sandboxes** link.

   The Manage Sandboxes page is displayed.
3. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in Creating and Activating a Sandbox.
4. On the toolbar, click **Publish Sandbox.** A message is displayed asking for confirmation.
5. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

2.3.1.1.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Scheduled Jobs for Lookup Field Synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

2.3.1.2 Localizing Field Labels in UI Forms

> **Note:**
>
> Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2.*x* or later and you want to localize UI form field labels.

To localize 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 one of the following files in a text editor:
   - For Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0):

     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf
   - For releases prior to Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0):

     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
6. Edit the BizEditorBundle.xlf file in the following manner:

   a. Search for the following text:

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

   b. Replace with the following text:

   ```
   <file source-language="en" target-language="LANG_CODE"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   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:

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

   c. Search for the application instance code. This procedure shows a sample edit for Oracle Internet Directory application instance. The original code is:

   ```
   <trans-unit id="$
   {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
   e']
   ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
   ```

```
UD_OID_USR_FNAME__c_description']}">
<source>Username</source>
</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.adform.entity.oidformEO.UD_OID_U
SR_FNAME__c_LABEL">
<source>Username</source>
</target>
</trans-unit>
```

d. Open the resource file from the connector package, for example OID_ja.properties, and get the value of the attribute from the file, for example, global.udf.UD_OID_USR_FNAME=\u540D.

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_OID_
USR_FNAME__c_description']}">
<source>Username</source>
<target>\u30E6\u30FC\u30B6\u30FC\u540D</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.OracleDBForm.entity.OracleDBForm
.UD_OID_USR_FNAME__c_LABEL">
<source>Username</source>
<target>\u30E6\u30FC\u30B6\u30FC\u540D</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.

> **See Also:**
>
> Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager,* for more information about exporting and importing metadata files

8. Log out of and log in to Oracle Identity Manager.

2.3.1.3 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:

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

   On Microsoft Windows: `PurgeCache.bat All`

   On UNIX: `PurgeCache.sh All`

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

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

   In this format:

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

2.3.1.4 Setting up the Lookup Definition for Connection Pooling

This section contains the following properties:

- Connection Pooling Properties
- Modifying the Connection Pooling Properties

2.3.1.4.1 Connection Pooling Properties

By default, this connector uses the ICF connection pooling. Table 2-3 lists the connection pooling properties, their description, and default values set in ICF.

Table 2-3 Connection Pooling Properties

Property	Description
Pool Max Idle	Maximum number of idle objects in a pool. Default value: `10`

Table 2-3 (Cont.) Connection Pooling Properties

Property	Description
Pool Max Size	Maximum number of connections that the pool can create. Default value: `10`
Pool Max Wait	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. Default value: `150000`
Pool Min Evict Idle Time	Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: `120000`
Pool Min Idle	Minimum number of idle objects in a pool. Default value: 1

2.3.1.4.2 Modifying the Connection Pooling Properties

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to modify the default connection pooling properties.

If you want to modify the connection pooling properties to use values that suit requirements in your environment, then:

1. Log in to the Design Console.
2. Expand **Administration,** and then double-click **Lookup Definition.**
3. Search for and open one of the following lookup definitions:

   For the trusted source mode:

   - For ODSEE: **Lookup.LDAP.Configuration.Trusted**
   - For OUD: **Lookup.LDAP.OUD.Configuration.Trusted**
   - For OID: **Lookup.OID.Configuration.Trusted**
   - For eDirectory: **Lookup.EDIR.Configuration.Trusted**

   For target resource mode:

   - For ODSEE: **Lookup.LDAP.Configuration**
   - For OUD: **Lookup.LDAP.OUD.Configuration**
   - For OID: **Lookup.OID.Configuration**
   - For eDirectory: **Lookup.EDIR.Configuration**
4. On the Lookup Code Information tab, click **Add.**

   A new row is added.
5. In the **Code Key** column of the new row, enter `Pool Max Idle.`

6. In the **Decode** column of the new row, enter a value corresponding to the Pool Max Idle property.
7. Repeat Steps 4 through 6 for adding each of the connection pooling properties listed in Table 2-3.
8. Click the Save icon.

2.3.1.5 Setting Up the OID Configuration Lookup Definition for LDAP Operation Timeouts

When an LDAP request is made by a client to a server and the server does not respond, the client waits forever for the server to respond until the TCP connection times out. On the client-side, you encounter read timed out exceptions while performing lookup field synchronization such as OID Connector Group Lookup Reconciliation. To avoid encountering such an issue, you must configure read and connect timeouts for your JNDI/LDAP service provider. To do so:

1. Log in to the Design Console.
2. Expand **Administration,** and then double-click **Lookup Definition.**
3. Search for and open the **Lookup.OID.Configuration** lookup definition.
4. On the Lookup Code Information tab, click **Add.**

   A new row is added.
5. In the **Code Key** column of the new row, enter `readTimeout`.
6. In the **Decode** column of the new row, enter a value corresponding to the readTimeout property. This property represents an integer value that specifies the number of milliseconds after which the LDAP provider must abort attempts to read an LDAP operation.
7. On the Lookup Code Information tab, click **Add.**

   A new row is added.
8. In the **Code Key** column of the new row, enter `connectTimeout`.
9. In the **Decode** column of the new row, enter a value corresponding to the connectTimeout property. This property represents an integer value that specifies the number of milliseconds after which the connection between the LDAP server and client times out.
10. Click the Save icon.

2.3.1.6 Configuring Oracle Identity Manager for Request-Based Provisioning

See About Request-Based Provisioning for information about request-based provisioning.

To configure request-based provisioning, perform the following procedures:

- Copying Predefined Request Datasets
- Importing Request Datasets
- Enabling the Auto Save Form Feature
- Running the PurgeCache Utility

> **Note:**
>
> Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1.*x*.

2.3.1.6.1 About Request-Based Provisioning

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

  > **Note:**
  >
  > Direct provisioning allows the provisioning of multiple LDAP server accounts on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

2.3.1.6.2 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following files contain predefined request datasets available in the xml directory on the installation media:

- For ODSEE or OUD target systems: ODSEE-OUD-LDAPV3-Datasets.xml
- For an OID target system: OID-Datasets.xml
- For an eDirectory target system: eDirectory-Datasets.xml

Copy this file from the installation media to any directory on the Oracle Identity Manager host computer. It is recommended that you create a directory structure as follows:

/custom/connector/*RESOURCE_NAME*

For example:

E:\MyDatasets\custom\connector\LDAP

> **Note:**
>
> Until you complete the procedure to configure request-based provisioning, ensure that there are no other files or directories inside the parent directory in which you create the directory structure. In the preceding example, ensure that there are no other files or directories inside the E:\MyDatasets directory.

The directory structure to which you copy the dataset files is the MDS location into which these files are imported after you run the Oracle Identity Manager MDS Import utility. The procedure to import dataset files is described in the next section.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets.

2.3.1.6.3 Importing Request Datasets

The request datasets (predefined or generated) can be imported by using the Deployment Manager (DM). The predefined request dataset is stored in the xml directory on the installation media.

To import a request dataset definition by using the Deployment Manager:

1. Log in to Oracle Identity Manager Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.
4. Depending on the target system that you are using, locate and open one of the following files, which are located in the xml directory of the installation media.
   - For ODSEE or OUD target systems: ODSEE-OUD-LDAPV3-Datasets.xml
   - For an OID target system: OID-Datasets.xml
   - For an eDirectory target system: eDirectory-Datasets.xml

   Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

The request datasets are imported into MDS.

2.3.1.6.4 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management,** and then double-click **Process Definition.**

3. Search for and open the **LDAP User** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.3.1.6.5 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Clearing Content Related to Connector Resource Bundles from the Server Cache for instructions.

The procedure to configure request-based provisioning ends with this step.

2.3.2 Creating the IT Resource for the Connector Server

To create the IT resource for the Connector Server:

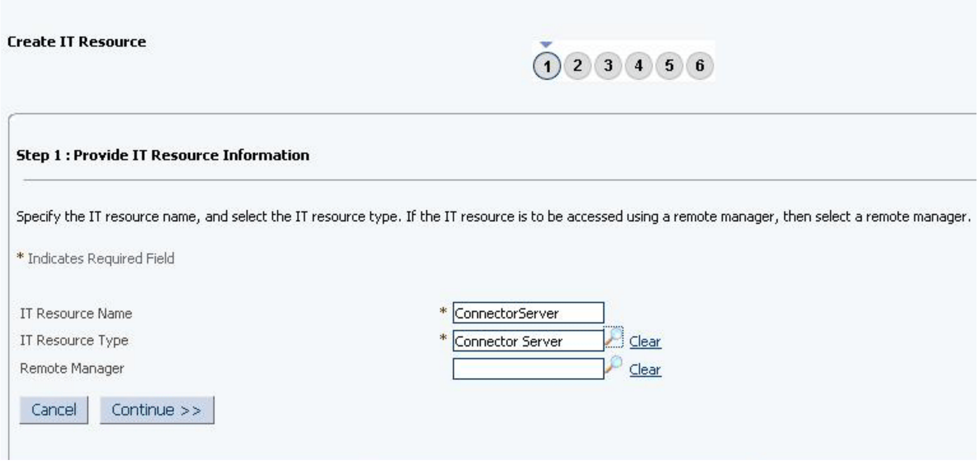
1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1.*x*:

     Log in to the Administrative and User Console
   - For Oracle Identity Manager release 11.1.2.*x* or later:

     Log in to Oracle Identity System Administration
2. If you are using Oracle Identity Manager release 11.1.1.*x*, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Create IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then:
   a. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see Managing Sandboxes of *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
   b. In the left pane, under Configuration, click **IT Resource.**

      The Manage IT Resource page is displayed.
   c. Click **Create IT Resource.**
4. On the Step 1: Provide IT Resource Information page, perform the following steps:
   - **IT Resource Name**: Enter a name for the IT resource.
   - **IT Resource Type**: Select **Connector Server** from the IT Resource Type list.
   - **Remote Manager**: Do not enter a value in this field.
5. Click **Continue**. Figure 2-3 shows the IT resource values added on the Create IT Resource page.

Figure 2-3 Step 1: Provide IT Resource Information



Create IT Resource

Step 1 : Provide IT Resource Information

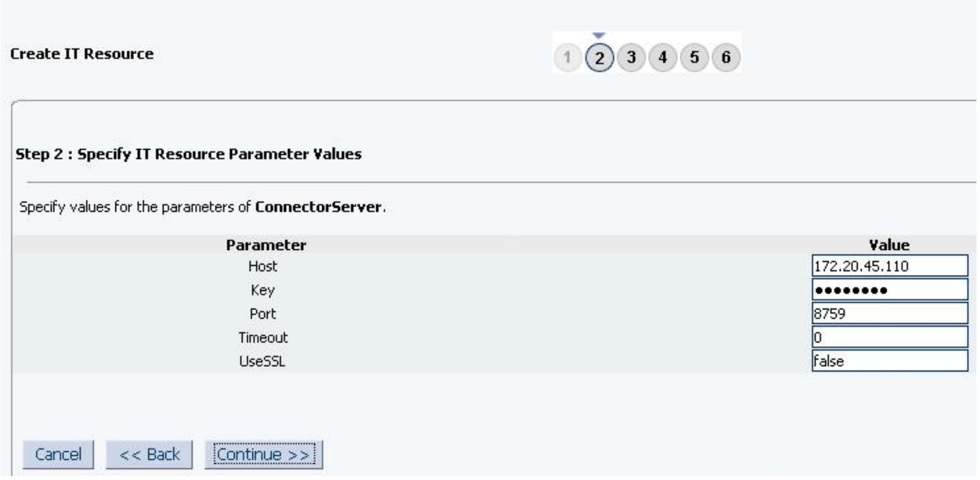
Specify the IT resource name, and select the IT resource type. If the IT resource is to be accessed using a remote manager, then select a remote manager.

* Indicates Required Field

IT Resource Name	* ConnectorServer
IT Resource Type	* Connector Server Clear
Remote Manager	Clear

6. On the Step 2: Specify IT Resource Parameter Values page, specify values for the parameters of the IT resource and then click **Continue**. Figure 2-4 shows the Step 2: Specify IT Resource Parameter Values page.

Figure 2-4 Step 2: Specify IT Resource Parameter Values



Create IT Resource

Step 2 : Specify IT Resource Parameter Values

Specify values for the parameters of **ConnectorServer**.

Parameter	Value
Host	172.20.45.110
Key	••••••••
Port	8759
Timeout	0
UseSSL	false

Figure 2-5 provides information about the parameters of the IT resource.

> **Note:**
>
> See Step 8 of Installing and Configuring the Connector Server for the values to be specified for the parameters of the IT resource.

Table 2-4   Parameters of the IT Resource for the Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the connector server. Sample value: `myhost.com`
Key	Enter the key for the connector server.
Port	Enter the number of the port at which the connector server is listening. Default value: `8759`
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the connector server and Oracle Identity Manager times out. Sample value: `0` A value of 0 means that the connection never times out.
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter `false.` Default value: `false` **Note:** It is recommended that you configure SSL to secure communication with the Connector Server. See also Configuring SSL for the Connector.

7. On the Step 3: Set Access Permission to IT Resource page, the `SYSTEM ADMINISTRATORS` group is displayed by default in the list of groups that have Read, Write, and Delete permissions on the IT resource that you are creating.

   > **Note:**
   >
   > This step is optional.

   If you want to assign groups to the IT resource and set access permissions for the groups, then:

   a. Click **Assign Group**.

   b. For the groups that you want to assign to the IT resource, select **Assign** and the access permissions that you want to set. For example, if you want to assign the `ALL USERS` group and set the Read and Write permissions to this group, then you must select the respective check boxes in the row, as well as the Assign check box, for this group.

   c. Click **Assign**.

8. On the Step 3: Set Access Permission to IT Resource page, if you want to modify the access permissions of groups assigned to the IT resource, then:

> **Note:**
>
> - This step is optional.
> - You cannot modify the access permissions of the `SYSTEM ADMINISTRATORS` group. You can modify the access permissions of only other groups that you assign to the IT resource.

   a. Click **Update Permissions**.

   b. Depending on whether you want to set or remove specific access permissions for groups displayed on this page, select or deselect the corresponding check boxes.

   c. Click **Update**.

9. On the Step 3: Set Access Permission to IT Resource page, if you want to unassign a group from the IT resource, then:

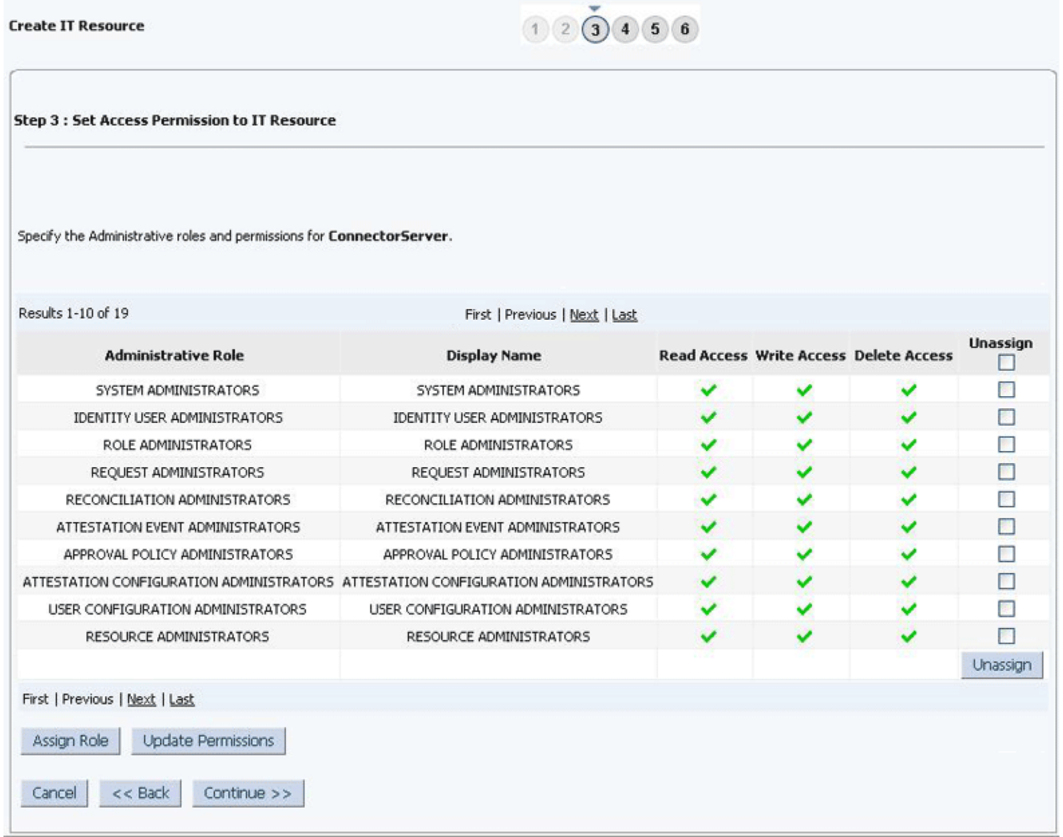
> **Note:**
>
> - This step is optional.
> - You cannot unassign the `SYSTEM ADMINISTRATORS` group. You can unassign only other groups that you assign to the IT resource.

   a. Select the **Unassign** check box for the group that you want to unassign.

   b. Click **Unassign**.

10. Click **Continue**. Figure 2-5 shows the Step 3: Set Access Permission to IT Resource page.

Figure 2-5   Step 3: Set Access Permission to IT Resource



Step 3 : Set Access Permission to IT Resource

Specify the Administrative roles and permissions for **ConnectorServer**.

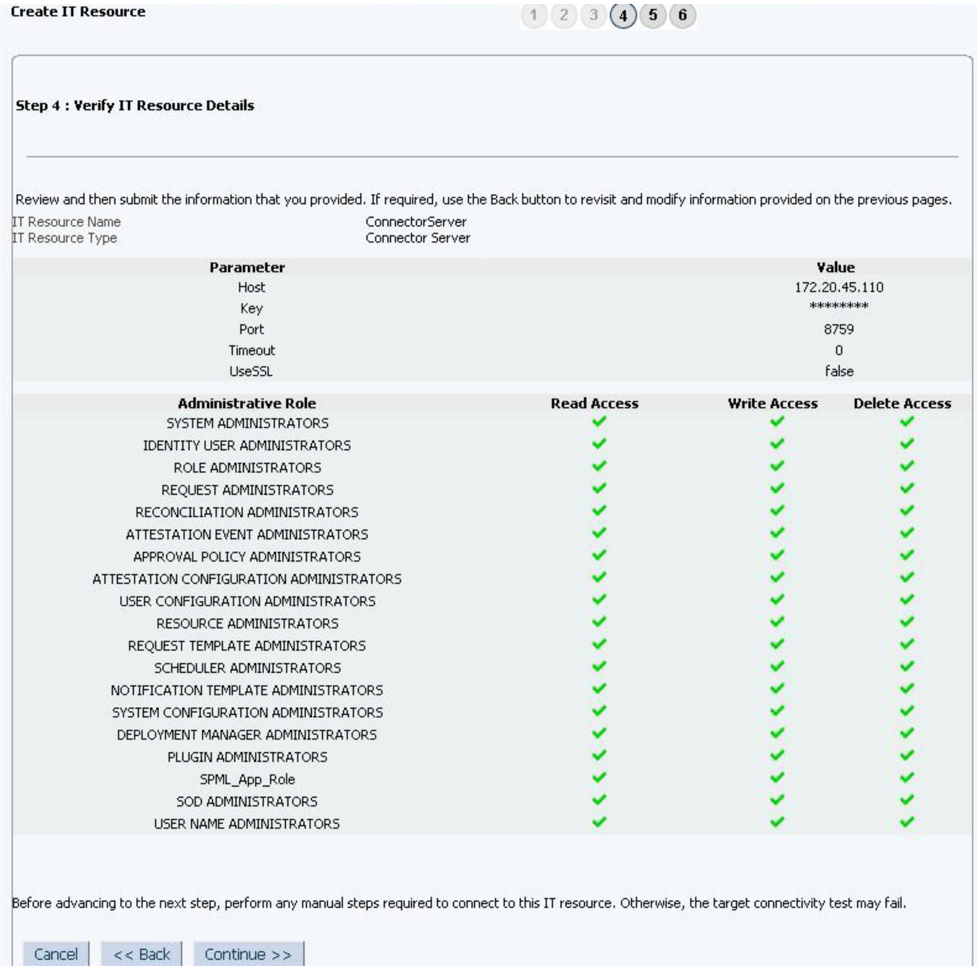
Results 1-10 of 19   First | Previous | Next | Last

Administrative Role	Display Name	Read Access	Write Access	Delete Access	Unassign □
SYSTEM ADMINISTRATORS	SYSTEM ADMINISTRATORS	✓	✓	✓	□
IDENTITY USER ADMINISTRATORS	IDENTITY USER ADMINISTRATORS	✓	✓	✓	□
ROLE ADMINISTRATORS	ROLE ADMINISTRATORS	✓	✓	✓	□
REQUEST ADMINISTRATORS	REQUEST ADMINISTRATORS	✓	✓	✓	□
RECONCILIATION ADMINISTRATORS	RECONCILIATION ADMINISTRATORS	✓	✓	✓	□
ATTESTATION EVENT ADMINISTRATORS	ATTESTATION EVENT ADMINISTRATORS	✓	✓	✓	□
APPROVAL POLICY ADMINISTRATORS	APPROVAL POLICY ADMINISTRATORS	✓	✓	✓	□
ATTESTATION CONFIGURATION ADMINISTRATORS	ATTESTATION CONFIGURATION ADMINISTRATORS	✓	✓	✓	□
USER CONFIGURATION ADMINISTRATORS	USER CONFIGURATION ADMINISTRATORS	✓	✓	✓	□
RESOURCE ADMINISTRATORS	RESOURCE ADMINISTRATORS	✓	✓	✓	□

11. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.

12. To proceed with the creation of the IT resource, click **Continue**. Figure 2-6 shows Step 4: Verify IT Resource Details page.

Figure 2-6 Step 4: Verify IT Resource Details



Create IT Resource

Step 4 : Verify IT Resource Details

Review and then submit the information that you provided. If required, use the Back button to revisit and modify information provided on the previous pages.

IT Resource Name	ConnectorServer
IT Resource Type	Connector Server

Parameter	Value
Host	172.20.45.110
Key	********
Port	8759
Timeout	0
UseSSL	false

Administrative Role	Read Access	Write Access	Delete Access
SYSTEM ADMINISTRATORS	✓	✓	✓
IDENTITY USER ADMINISTRATORS	✓	✓	✓
ROLE ADMINISTRATORS	✓	✓	✓
REQUEST ADMINISTRATORS	✓	✓	✓
RECONCILIATION ADMINISTRATORS	✓	✓	✓
ATTESTATION EVENT ADMINISTRATORS	✓	✓	✓
APPROVAL POLICY ADMINISTRATORS	✓	✓	✓
ATTESTATION CONFIGURATION ADMINISTRATORS	✓	✓	✓
USER CONFIGURATION ADMINISTRATORS	✓	✓	✓
RESOURCE ADMINISTRATORS	✓	✓	✓
REQUEST TEMPLATE ADMINISTRATORS	✓	✓	✓
SCHEDULER ADMINISTRATORS	✓	✓	✓
NOTIFICATION TEMPLATE ADMINISTRATORS	✓	✓	✓
SYSTEM CONFIGURATION ADMINISTRATORS	✓	✓	✓
DEPLOYMENT MANAGER ADMINISTRATORS	✓	✓	✓
PLUGIN ADMINISTRATORS	✓	✓	✓
SPML_App_Role	✓	✓	✓
SOD ADMINISTRATORS	✓	✓	✓
USER NAME ADMINISTRATORS	✓	✓	✓

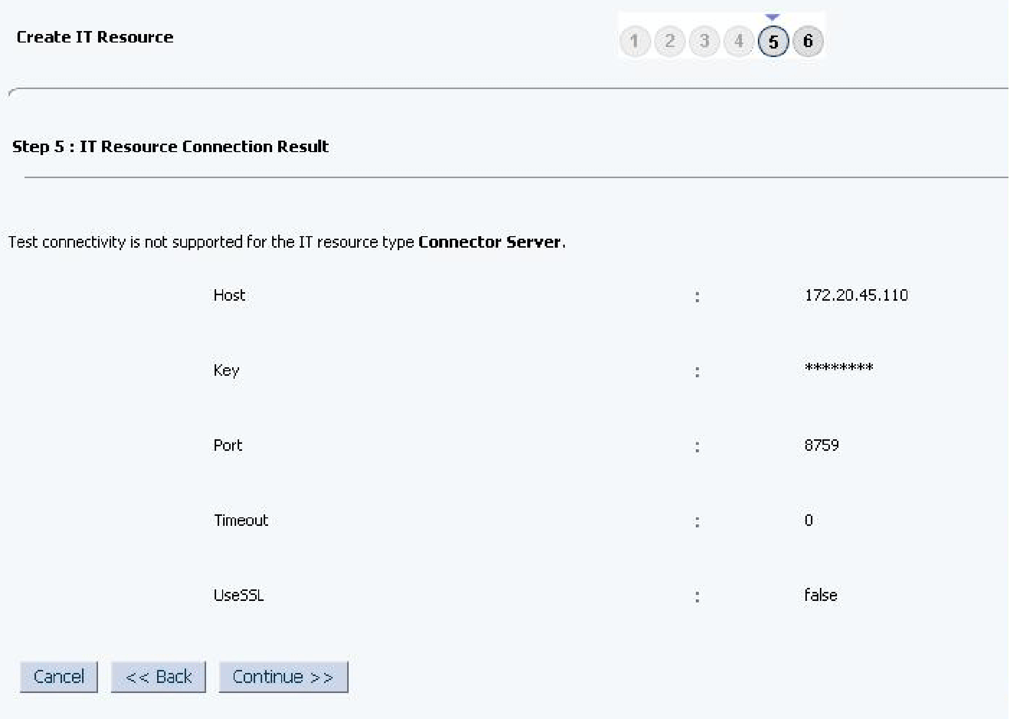
Before advancing to the next step, perform any manual steps required to connect to this IT resource. Otherwise, the target connectivity test may fail.

13. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Continue**. If the test fails, then you can perform one of the following steps:

    - Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
    - Click **Cancel** to stop the procedure, and then begin from the first step onward.

      Figure 2-7 shows the Step 5: IT Resource Connection Result page.

Figure 2-7 Step 5: IT Resource Connection Result



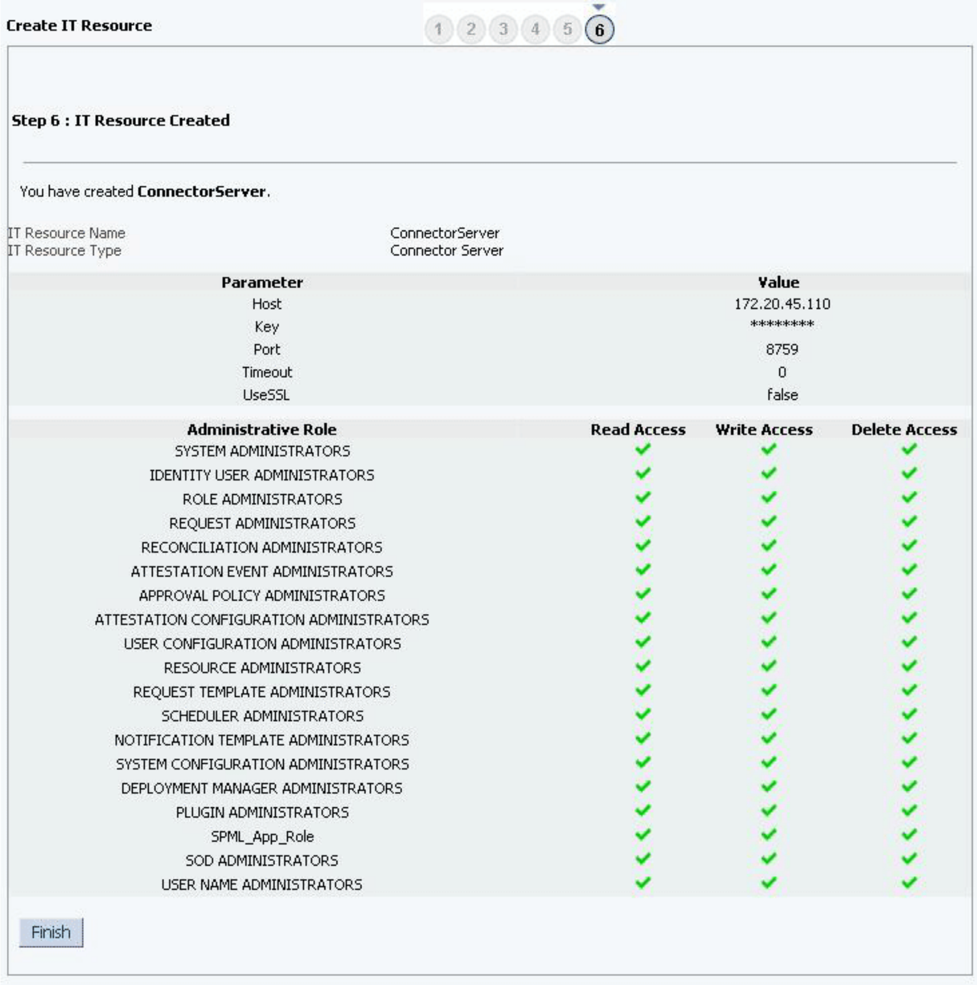
Step 5 : IT Resource Connection Result

Test connectivity is not supported for the IT resource type **Connector Server**.

Host	:	172.20.45.110
Key	:	********
Port	:	8759
Timeout	:	0
UseSSL	:	false

14. Click **Finish**. Figure 2-8 shows the IT Resource Created Page.

Figure 2-8   Step 6: IT Resource Created



Step 6 : IT Resource Created

You have created **ConnectorServer**.

IT Resource Name   ConnectorServer
IT Resource Type   Connector Server

Parameter	Value
Host	172.20.45.110
Key	********
Port	8759
Timeout	0
UseSSL	false

Administrative Role	Read Access	Write Access	Delete Access
SYSTEM ADMINISTRATORS	✓	✓	✓
IDENTITY USER ADMINISTRATORS	✓	✓	✓
ROLE ADMINISTRATORS	✓	✓	✓
REQUEST ADMINISTRATORS	✓	✓	✓
RECONCILIATION ADMINISTRATORS	✓	✓	✓
ATTESTATION EVENT ADMINISTRATORS	✓	✓	✓
APPROVAL POLICY ADMINISTRATORS	✓	✓	✓
ATTESTATION CONFIGURATION ADMINISTRATORS	✓	✓	✓
USER CONFIGURATION ADMINISTRATORS	✓	✓	✓
RESOURCE ADMINISTRATORS	✓	✓	✓
REQUEST TEMPLATE ADMINISTRATORS	✓	✓	✓
SCHEDULER ADMINISTRATORS	✓	✓	✓
NOTIFICATION TEMPLATE ADMINISTRATORS	✓	✓	✓
SYSTEM CONFIGURATION ADMINISTRATORS	✓	✓	✓
DEPLOYMENT MANAGER ADMINISTRATORS	✓	✓	✓
PLUGIN ADMINISTRATORS	✓	✓	✓
SPML_App_Role	✓	✓	✓
SOD ADMINISTRATORS	✓	✓	✓
USER NAME ADMINISTRATORS	✓	✓	✓

2.4 Uninstalling the Connector

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

2.5 Upgrading the Connector

Upgrading to the OID connector release 11.1.1.5.0 is supported for Oracle Internet Directory connector version number 9.0.4.14, and Sun Java System Directory connector version 9.0.4.15. The following sections describe the upgrade process:

- Preupgrade Steps
- Upgrade Steps
- Postupgrade Steps
- Running the Form Version Control (FVC) Utility to Migrate eDirectory Forms

> **Note:**
>
> Preupgrade considerations are:
>
> - Before you perform the upgrade procedure, it is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
> - As a best practice, first perform the upgrade procedure in a test environment.

2.5.1 Preupgrade Steps

Perform the following preupgrade steps:

1. Perform a reconciliation run to fetch all latest updates to Oracle Identity Manager.
2. Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector.
3. If required, create the connector XML file for a clone of the source connector.
4. Disable all the scheduled tasks.

2.5.2 Upgrade Steps

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

- Development Environment

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

  Perform the upgrade procedure by using the silent mode. In the silent mode, use the silent.xml file that is exported from the development environment.

See Managing Connector Lifecycle of *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the wizard and silent modes.

2.5.3 Postupgrade Steps

Perform the postupgrade procedure documented in Managing Connector Lifecycle of *Oracle Fusion Middleware Administering Oracle Identity Manager*.

To prevent errors during a child and parent table update, perform the following steps after you upgrade the connector:

> **Note:**
>
> Perform Steps 1 through 7 of the following procedure if you are using the ODSEE target system.
>
> If you are using the OID, Novell eDirectory, or OUD target systems, then skip Steps 1 through 7, and perform Step 8.

1. Log in to Oracle Identity Manager Design Console.
2. Open **Process Management** and then **Process Definition**.
3. Find the **LDAP User** process.
4. Open the **Remove User From Group** task.
5. Go to the **Integration** tab.
6. Update the **childTableName** variable value from **UD_LDAP_GRP** to **UD_IPNT_GRP**.
7. Update the **childTableName** variable in a similar manner for these tasks and values:
   - **Add Role to User**: **UD_LDAP_ROL** to **UD_IPNT_ROL**
   - **Remove Role From User**: **UD_LDAP_ROL** to **UD_IPNT_ROL**
   - **Add User to Group**: **UD_LDAP_GRP** to **UD_IPNT_GRP**
   - **Update User Role**: **UD_LDAP_ROL** to **UD_IPNT_ROL**
   - **Update User Group**: **UD_LDAP_GRP** to **UD_IPNT_GRP**
8. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:
   a. Log in to Oracle Identity System Administration.
   b. Create and active a sandbox. See Creating and Activating a Sandbox for more information.
   c. Create a new UI form to view the upgraded fields. See Creating a New UI Form for more information about creating a UI form.
   d. 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 (created in Step 5.c), and then save the application instance.
   e. Publish the sandbox. See Publishing a Sandbox for more information.

2.5.4 Running the Form Version Control (FVC) Utility to Migrate eDirectory Forms

To manage data changes on eDirectory forms after an upgrade operation, run the Form Version Control (FVC) utility. The FVC utility requires a properties file to define the data conversion actions that you want the utility to perform.

> **Note:**
>
> The following procedure applies to an eDirectory target system, but you can also run the FVC utility for other target systems.

Before you run the FVC utility, set the following entries in the properties file:

- For User forms:

  ```
  ResourceObject;eDirectory User
  FormName;UD_EDIR_USR
  FromVersion;From-Version
  ToVersion;To-Version
  ParentParent;UD_EDIR_USR_GUID;UD_EDIR_USR_REFID
  ```

- For Group forms:

  ```
  ResourceObject;eDirectory Group
  FormName;UD_EDIR_GR
  FromVersion;From-Version
  ToVersion;To-Version
  ParentParent;UD_EDIR_GR_GUID;UD_EDIR_GR_REFID
  ```

- For Role forms:

  ```
  ResourceObject;eDirectory Role
  FormName;UD_EDIR_RL
  FromVersion;From-Version
  ToVersion;To-Version
  ParentParent;UD_EDIR_RL_GUID;UD_EDIR_RL_REFID
  ```

- For Organisation Unit (OU) forms:

  ```
  ResourceObject;eDir Organisation Unit
  FormName;UD_EDIR_OU
  FromVersion;From-Version
  ToVersion;To-Version
  ParentParent;UD_EDIR_OU_GUID;UD_EDIR_OU_REFID
  ```

2.6 Postcloning Steps

This section contains the following topics:

- About Postcloning Steps
- Postcloning Configuration for User Accounts

2.6.1 About Postcloning Steps

You can clone the OID connector by setting new names for some of the objects that comprise the connector. The outcome of the process is a new connector XML file. Most of the connector objects, such as Resource Object, Process Definition, Process Form, IT Resource Type Definition, IT Resource Instances, Lookup Definitions, Adapters, Reconciliation Rules and so on in the new connector XML file have new names.

> **Note:**
>
> Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about cloning connectors.

After a copy of the connector is created by setting new names for connector objects, some objects might contain the details of the old connector objects. Therefore, you must modify the following Oracle Identity Manager objects to replace the base connector artifacts or attribute references with the corresponding cloned artifacts or attributes:

- IT Resource

  The cloned connector has its own set of IT resources. You must configure both the cloned connector IT resources and Connector Server IT resources, and provide the reference of the cloned Connector Server IT Resource in the cloned connector IT resource. Ensure you use the configuration lookup definition of the cloned connector.

- Scheduled Task

  The values of the Resource Object Name and IT Resource scheduled task attributes in the cloned connector refer to the values of the base connector. Therefore, these values (values of the Resource Object Name and IT resource scheduled task attributes that refer to the base connector) must be replaced with the new cloned connector artifacts.

- Lookup Definition

  No change is required to be made in any of the cloned lookup definitions. All cloned lookup definitions contain proper lookup entries.

- Process Tasks

  After cloning, you notice that all event handlers attached to the process tasks are the cloned ones. Therefore, no changes are required for process tasks in parent forms. This is because the adapter mappings for all process tasks related to parent forms are updated with cloned artifacts.

- Localization Properties

  You must update the resource bundle of a user locale with new names of the process form attributes for proper translations after cloning the connector. You can modify the properties file of your locale in the resources directory of the connector bundle.

- POSIX Accounts, Groups, and Roles

  If you have cloned the connector and added a group or role to an account, perform the steps in Postcloning Configuration for User Accounts.

2.6.2 Postcloning Configuration for User Accounts

This configuration change is related to a child form. When you add a group or role to an account, perform the following steps:

1. Log in to Oracle Identity Manager Design Console.

2. Go to the cloned **LDAP User Process**, **OID User Process**, **eDirectory User,** or **OUD User Process** definition.
3. Open the **Add User To Group Process** task and navigate to the **Integration** tab.
4. In the **Event Handler/Adapter** section, click **Remove**.
5. Add the same adapter again and do the mappings. Table 2-5 shows sample mappings for OID.

   Note: Open the **childTableName** mapping and change the **Literal Value** to the new value (the cloned value).
6. Repeat these steps for the **Remove User From Group** and **Update User Group** tasks.

   Similar steps can be repeated for **Add Role**, **Delete Role**, and **Update Role**, in the case of ODSEE and eDirectory targets, which support roles.

Table 2-5   Mappings for OID Event Handler/Adapter

Variable Name	Data Type	Map To	Qualifer	Literal Value
processInstanceKey	Long	Process Data	Process Instance	NA
Adapter return value	Object	Response Code	NA	NA
objectType	String	Literal	String	User
itResourceName	String	Literal	String	UD_OID_USR_SERVER
childTableName	String	Literal	String	UD_OID_GRP1

3 Using the Connector

This chapter is divided into the following sections:

- Guidelines on Using the Connector
- Scheduled Jobs for Lookup Field Synchronization
- Configuring Reconciliation
- Configuring Scheduled Jobs
- Performing Provisioning Operations in Oracle Identity Manager Release 11.1.1.*x*
- Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later
- Uninstalling the Connector

3.1 Guidelines on Using the Connector

This section discusses the following topics:

- Guidelines on Configuring Reconciliation
- Guidelines on Performing Provisioning Operations

3.1.1 Guidelines on Configuring Reconciliation

The following are guidelines that you must apply while configuring reconciliation:

- Before a target resource reconciliation run is performed, lookup definitions must be synchronized with the lookup fields of the target system. In other words, scheduled jobs for lookup field synchronization must be run before user reconciliation runs.
- The scheduled job for user reconciliation must be run before the scheduled job for reconciliation of deleted user data.
- There is no support for group entities in Oracle Identity Manager. Therefore, apply the following guidelines before you run the scheduled job for groups reconciliation:
  - If you are using the default connector configuration, for every group in the target system, create a corresponding organizational unit (with the same group name) in Oracle Identity Manager. This ensures that all groups from the target system are reconciled into their newly created organizational units, respectively.
  - You can also configure the connector to reconcile the groups under one organization. For more information see the following sections:

    Reconciling ODSEE Groups and Roles Under One Organization in Oracle Identity Manager

    Reconciling OUD Groups Under One Organization in Oracle Identity Manager

    Reconciling OID Groups Under One Organization in Oracle Identity Manager

    Reconciling eDirectory Groups and Roles Under One Organization in Oracle Identity Manager

- For OUD target systems, the OUD changelog is based on the replication database. By default, the replication keeps changelog entries for only 100 hours. The replication purge delay must be tuned based on your specific requirements. The database size on disk will vary accordingly. For more information, see the changelog documentation for the OUD target system.
- Reconciliation of roles is supported only for ODSEE and Novell eDirecotory target systems.
- Run the User Search Reconciliation scheduled job, if only changes with regard to group membership are made to a user. This is because neither the changelog nor modifiedTimestamp attribute is updated. Therefore, performing full reconciliation by running the User Search Reconciliation scheduled job should reconcile such changes.
- If you are using Oracle Identity Manager release 11.1.2.3 and you are reconciling a large number of records for an OID target system, then you must specify values for the following parameters to optimize performance:
  - **For target resource configuration**
    - Ensure you have added the readTimeout and connectTimeout entries to the Lookup.OID.Configuration lookup definition. See Setting Up the OID Configuration Lookup Definition for LDAP Operation Timeouts for more information about adding these entries.
    - Change or increase the values of the blockSize and changeLogBlockSize entries of the Lookup.OID.Configuration lookup definition to suit the requirements in your environment.
  - **For trusted source configuration**

    Ensure that you set the value of the usePagedResultControl entry in the Lookup.OID.Configuration.Trusted lookup definition to `true`.

3.1.2 Guidelines on Performing Provisioning Operations

The following are guidelines that you must apply while performing provisioning operations:

- Before you perform provisioning operations, lookup definitions must be synchronized with the lookup fields of the target system. In other words, scheduled tasks for lookup field synchronization must be run before provisioning operations.
- If you want to provision a User, Group, Role, or an Organizational Unit directly under base context, then add a new entry in the **Lookup.LDAP.Organization** lookup definition with both the Code Key and the Decode values set to the base context name.

  For OID, use **Lookup.OID.Organization** and for eDirectory, use **Lookup.EDIR.Organization**.

  Sample value:

  Code Key: `281~dc=example,dc=com` (where 281 is the IT resource key)

  Decode: `LDAP_server~dc=example,dc=com` (where LDAP_server is the IT resource name)

> **Note:**
>
> Provisioning in Non-Organization Containers for an eDirectory Target
>
> To provision an entity in a non-organization container, add that container value manually in the eDirectory container Lookup.EDIR.Organization lookup definition. For example:
>
> **Code Key**: 8~dc=home
>
> **Decode Key**: eDirectory~"randomvalue"

- On the Oracle Internet Directory target system, the Manager Name field accepts only DN values. Therefore, when you set or modify the Manager Name field in Oracle Identity Manager, you must enter the DN value.

  For example: `cn=abc,ou=lmn,dc=corp,dc=com`
- Provisioning of roles is supported only for ODSEE and Novell eDirecotory target systems.

3.2 Scheduled Jobs for Lookup Field Synchronization

This section contains the following topics:

- Scheduled Jobs for Lookup Field Synchronization for ODSEE
- Scheduled Jobs for Lookup Field Synchronization for Oracle Internet Directory
- Scheduled Jobs for Lookup Field Synchronization for Novell eDirectory
- Scheduled Job Attributes

> **Note:**
>
> The procedure to configure these scheduled jobs is described later in the guide.

3.2.1 Scheduled Jobs for Lookup Field Synchronization for ODSEE

The following are the scheduled jobs for lookup field synchronization for ODSEE:

- LDAP Connector Group Lookup Reconciliation

  This scheduled job is used to synchronize group lookup fields in Oracle Identity Manager with group data in the target system.
- LDAP Connector Role Lookup Recon

  This scheduled job is used to synchronize role lookup fields in Oracle Identity Manager with role data in the target system.

> **Note:**
>
> If you are using OUD as the Target System, then you must not run the LDAP Connector Role Lookup Recon scheduled job.

- LDAP Connector OU Lookup Reconciliation

  This scheduled job is used to synchronize organization lookup fields in Oracle Identity Manager with organization data in the target system.

3.2.2 Scheduled Jobs for Lookup Field Synchronization for Oracle Internet Directory

The following are the scheduled jobs for lookup field synchronization for Oracle Internet Directory:

- OID Connector Group Lookup Reconciliation

  This scheduled job is used to synchronize group lookup fields in Oracle Identity Manager with group data in the target system.
- OID Connector OU Lookup Reconciliation

  This scheduled job is used to synchronize organization lookup fields in Oracle Identity Manager with organization data in the target system.

3.2.3 Scheduled Jobs for Lookup Field Synchronization for Novell eDirectory

The following are the scheduled jobs for lookup field synchronization for Novell eDirectory:

- eDirectory Connector Group Lookup Reconciliation

  This scheduled job is used to synchronize group lookup fields in Oracle Identity Manager with group data in the target system.
- eDirectory Connector Role Lookup Reconciliation

  This scheduled job is used to synchronize role lookup fields in Oracle Identity Manager with role data in the target system.
- eDirectory Connector Org Lookup Reconciliation

  This scheduled job is used to synchronize organization lookup fields in Oracle Identity Manager with organization data in the target system.
- eDirectory Connector Domain Scope Lookup Reconciliation

  This scheduled job is used to synchronize organization lookup fields in Oracle Identity Manager with organization data in the target system. These domains are associated with roles as trustee.
- eDirectory Connector Profile Lookup Reconciliation

  This scheduled job is used to synchronize profile lookup fields in Oracle Identity Manager with profile data in the target system.
- eDirectory Connector Role Container Lookup Reconciliation

This scheduled job is used to synchronize Role Container lookup fields in Oracle Identity Manager with Role Containers on the target system. An eDirectory role can be provisioned only under a Role Container.

3.2.4 Scheduled Job Attributes

Table 3-1 describes the attributes of the scheduled jobs.

Table 3-1 Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Code Key Attribute	Name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). **Note:** You must not change the value of this attribute.
Decode Attribute	Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute).
Filter	Enter a filter to filter out records to be stored in the lookup definition. For more information about the Filter attribute, see Limited Reconciliation.
IT Resource Name	Name of the IT resource for the target system installation from which you reconcile records. Default values are: • ODSEE or OUD target resource: `DSEE Server` • OID target resource: `OID Server` • eDirectory target resource: `eDirectory Server`
Lookup Name	Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. **Note:** If the lookup name that you specify as the value of this attribute is not present in Oracle Identity Manager, then this lookup definition is created while the scheduled job is run.
Object Type	This attribute holds the name of the type of object you want to reconcile.

3.3 Configuring Reconciliation

When you run the Connector Installer, scheduled jobs for user reconciliation are automatically created in Oracle Identity Manager. Configuring reconciliation involves providing values for the attributes of these scheduled jobs.

The following sections provide information about the attributes of the scheduled jobs:

- Full Reconciliation and Incremental Reconciliation
- Limited Reconciliation
- Reconciliation Scheduled Jobs

Note:

Consider this scenario. You provision a user to an organization (org1) and then move the user to a second organization (org2). You run Trusted Reconciliation and Target User Sync reconciliation. As result, two resources are attached to the user: revoked and provisioned.

This behavior is normal for the connector. After moving the user to org2, the target directory considers the user in org1 to be deleted (revoked) even though the user still exists in org1. However, in org2 the user also exists and is considered to be provisioned.

3.3.1 Full Reconciliation and Incremental Reconciliation

Full reconciliation involves reconciling all existing records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation. In addition, you can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Manager.

Full reconciliation: To perform a full reconciliation run, ensure that a value is **not** specified for the Filter and Latest Token attributes of the search reconciliation scheduled job for users, groups, or roles.

Incremental reconciliation: If the target system supports changelog, Sync reconciliation can be used for performing incremental reconciliation. To perform an incremental reconciliation run, specify a value for the Sync Token attribute in the sync reconciliation scheduled job for users, groups, or roles. From the next run onward, only records created or modified after the value in the Sync Token attribute are considered for reconciliation.

Incremental reconciliation can also be performed by filtered search based on the modifyTimestamp value. The timestamp value is updated in the search reconciliation scheduled task after full reconciliation. From the next run onward, the task runs in incremental reconciliation mode.

Note:

Sync reconciliation is not supported for eDirectory target systems.

3.3.2 Limited Reconciliation

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

The following are the ways in which limited reconciliation can be achieved:

- Limited Reconciliation By Using Filters

- Limited Reconciliation Based on Group Membership

3.3.2.1 Limited Reconciliation By Using Filters

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

For detailed information about ICF Filters, see ICF Filter Syntax of *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

While deploying the connector, follow the instructions in Configuring Scheduled Jobs to specify attribute values.

3.3.2.2 Limited Reconciliation Based on Group Membership

Limited Reconciliation can be performed based on Group Membership. If you wish to reconcile only the users associated with a particular group, configure the filter as follows:

- For ODSEE and OUD:

  In the Lookup.LDAP.Configuration lookup definition, set:

  – ldapGroupFilterBehavior=accept

  – ldapGroupMembershipAttribute=ismemberof

  Specify the filter as:

  ```
  containsAllValues('ldapGroups','cn=grp1,ou=groups,dc=example,dc=com')
  ```

- For OID:

  In the Lookup.OID.Configuration lookup definition, set:

  – ldapGroupFilterBehavior=ignore

  – ldapGroupMembershipAttribute=ismemberof

  Specify the filter as:

  ```
  containsAllValues('ldapGroups','cn=grp1,ou=groups,dc=example,dc=com')
  ```

In these examples, grp1 is the group with which users are associated.

3.3.3 Reconciliation Scheduled Jobs

When you run the Connector Installer, the following reconciliation scheduled tasks are automatically created in Oracle Identity Manager:

- Scheduled Jobs for Reconciliation of User Records
- Scheduled Jobs for Reconciliation of Deleted User Records
- Scheduled Jobs for Reconciliation of Groups, OUs, and Roles
- Scheduled Jobs for Reconciliation of Deleted Groups, OUs, and Roles

3.3.3.1 Scheduled Jobs for Reconciliation of User Records

The following sections describe the scheduled jobs and their attributes for ODSEE/OUD, which are similar for other target systems:

- About Scheduled Jobs for Reconciliation of User Records
- LDAP Connector User Search Reconciliation
- LDAP Connector User Sync Reconciliation
- LDAP Connector Trusted User Reconciliation

3.3.3.1.1 About Scheduled Jobs for Reconciliation of User Records

Depending on your target system, you must specify values for the attributes of the following user reconciliation scheduled jobs.

For ODSEE/OUD:

- LDAP Connector User Search Reconciliation
- LDAP Connector User Sync Reconciliation
- LDAP Connector Trusted User Reconciliation

For OID:

- OID Connector User Search Reconciliation
- OID Connector User Sync Reconciliation
- OID Connector Trusted User Reconciliation

For eDirectory:

- eDirectory Connector User Search Reconciliation
- eDirectory Connector Trusted User Reconciliation

3.3.3.1.2 LDAP Connector User Search Reconciliation

This scheduled job is used to reconcile user data in the target resource (account management) mode of the connector. Use this scheduled job if either of the following conditions is true:

- You want to perform Full or Incremental Reconciliation.
- Your target system supports modifyTimestamp.

> **Note:**
>
> Run the User Search Reconciliation scheduled job, if only changes with regard to group membership are made to a user. This is because neither the changelog nor modifiedTimestamp attribute is updated. Therefore, performing full reconciliation by running the User Search Reconciliation scheduled job should reconcile such changes.
>
> The same information has been listed in Guidelines on Configuring Reconciliation.

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

Table 3-2 Attributes of the LDAP Connector User Search Reconciliation Scheduled Job

Attribute	Description
Filter	Expression for filtering records that must be reconciled by the scheduled job. Sample value: `startsWith('cn','Samrole1')` Default value: None See Limited Reconciliation for the syntax of this expression.
Incremental Recon Attribute	Enter the name of the target system attribute that holds the time stamp at which the last reconciliation run started. The value in this attribute is used during incremental reconciliation to determine the newest or latest record reconciled from the target system. Default value: `modifyTimestamp`
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. Values are: • ODSEE or OUD target resource: `DSEE Server` • OID target resource: `OID Server` • eDirectory target resource: `eDirectory Server`
Latest Token	This attribute holds the time stamp value of the Incremental Recon Attribute. **Note:** The reconciliation engine automatically enters a value for this attribute after execution. It is recommended that you do not change the value of this attribute. If you manually specify a value for this attribute, then only user accounts that have been modified after the time stamp specified as the value of this attribute are reconciled. If you want to perform a full reconciliation, clear the value in this field. Sample value: `<String>20120516115131Z</String>`
Object Type	This attribute holds the type of object you want to reconcile. Default value: `User`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. Default value: `LDAP User` Can also be `OID User` or `eDirectory User`
Scheduled Task Name	This attribute holds the name of the scheduled task. Default value: `LDAP Connector User Search Reconciliation`

3.3.3.1.3 LDAP Connector User Sync Reconciliation

This scheduled job is used to reconcile user data in the target resource (account management) mode of the connector. Use this scheduled job if either of the following conditions is true:

- You want to perform incremental reconciliation.
- Your target system supports the changelog attribute.

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

Table 3-3 Attributes of the LDAP Connector User Sync Reconciliation Scheduled Job

Attribute	Description
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. Values are: • ODSEE or OUD target resource: `DSEE Server` • OID target resource: `OID Server` • eDirectory target resource: `eDirectory Server`
Object Type	This attribute holds the type of object you want to reconcile. Default value: `User`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. Default value: `LDAP User` Can also be `OID User` or `eDirectory User`
Scheduled Task Name	This attribute holds the name of the scheduled task. Default value: `LDAP Connector User Sync Reconciliation`
Sync Token	You can manually enter the first Sync Token. To retrieve this token, query cn=changelog on rootDSE on the target system. Then, every time sync reconciliation is run, Sync Token is updated. Browse the changelog attribute of the target system to determine a value from the changelog that must be used to resume a reconciliation run. From the next reconciliation run onward, only data about records that are created or modified since the last reconciliation run ended are fetched into Oracle Identity Manager. Or, you can also leave this field blank, which causes the entire changelog to be read. This attribute stores values in one of the following formats: • If you are using a target system for which the value of the standardChangelog entry in the Configuration lookup definition is set to `true`, then this attribute stores values in the following format: <Integer>*VALUE*</Integer> Sample value: `<Integer>476</Integer>` • If you are using a target system (for example, OUD) for which the value of the standardChangelog entry in the Configuration lookup definition is set to `false,` then this attribute stores values in the following format: <String>*VALUE*</String> Sample value: `<String>dc=example,dc=com:0000013633e514427b6600000013;</String>`

3.3.3.1.4 LDAP Connector Trusted User Reconciliation

This scheduled job is used to reconcile user data in the trusted resource (identity management) mode of the connector.

Table 3-4 describes the attributes of this scheduled job.

Table 3-4 Attributes of the Scheduled Job for Reconciliation of User Data from a Trusted Source

Attribute	Description
Filter	Expression for filtering records that must be reconciled by the scheduled job. Sample value: `startsWith('cn','Samrole1')` Default value: None See Limited Reconciliation for the syntax of this expression.
IT Resource Name	Enter the name of the IT resource instance that the connector must use to reconcile data. Values are: • ODSEE or OUD target resource: `DSEE Server` • OID target resource: `OID Server` • eDirectory target resource: `eDirectory Server`
Object Type	This attribute holds the type of object you want to reconcile. Default value: `User`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. Default value: `LDAP Trusted User` Can also be `OID Trusted User` or `eDirectory User Trusted`
Scheduled Task Name	This attribute holds the name of the scheduled task. Default value: `LDAP Connector Trusted User Reconciliation`
Incremental Recon Attribute	Enter the name of the target system attribute that holds the time stamp at which the last reconciliation run started. The value in this attribute is used during incremental reconciliation to determine the newest or latest record reconciled from the target system. Default value: `modifyTimestamp`
Latest Token	This attribute holds the time stamp value of the Incremental Recon Attribute. **Note:** • The reconciliation engine automatically enters a value for this attribute after execution. It is recommended that you do not change the value of this attribute. If you manually specify a value for this attribute, then only user accounts that have been modified after the time stamp specified as the value of this attribute are reconciled. If you want to perform a full reconciliation, clear the value in this field. Sample value: `<String>20120516115131Z</String>` • If you are using a connector that has been upgraded from release 9.0.4.*x* of the Sun Java System Directory connector, and you want to perform incremental reconciliation in trusted source mode, then: 1. Note down the latest timestamp value from the legacy connector. 2. Specify a value for the Latest Token attribute in the following format: `<String>yyyyMMddHHmmssZ</String>` Sample value: <String>20130517055840Z</String>

3.3.3.2 Scheduled Jobs for Reconciliation of Deleted User Records

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

- LDAP Connector User Search Delete Reconciliation, OID Connector User Search Delete Reconciliation, and eDirectory Connector User Search Reconciliation

  These scheduled jobs are used to reconcile data about deleted users in the target resource (account management) mode of the connector. During a reconciliation run, for each deleted user account on the target system, the target system resource is revoked for the corresponding OIM User.

- LDAP Connector Trusted User Delete Reconciliation, OID Connector Trusted User Delete Reconciliation, and eDirectory Connector Trusted User Reconciliation

  These scheduled jobs are 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 the attributes of these scheduled jobs.

Table 3-5 Attributes of the Scheduled Jobs for Delete User Reconciliation

Attribute	Description
IT Resource Name	Enter the name of the IT resource instance that the connector must use to reconcile data. **Note**. For Trusted Delete Reconciliation, use the Trusted Configuration Lookup in the IT Resource. The default value of this attribute in the LDAP Connector User Search Delete Reconciliation scheduled job is `DSEE Server`. OID target resource: `OID Server` eDirectory target resource: `eDirectory Server` There is no default value for this attribute in the LDAP Connector Trusted User Delete Reconciliation scheduled job.
Object Type	This attribute holds the type of object you want to reconcile. Default value: `User`

Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector User Search Delete Reconciliation:
	`LDAP User`, `OID User`, or `eDirectory User`
	• For LDAP Connector Trusted User Delete Reconciliation:
	`LDAP Trusted User`, `OID Trusted User`, or `eDirectory User Trusted`

3.3.3.3 Scheduled Jobs for Reconciliation of Groups, OUs, and Roles

The following sections describe the scheduled jobs and their attributes for ODSEE/OUD, which are similar for other target systems:

- About Scheduled Jobs for Reconciliation of Groups, OUs, and Roles

- LDAP Connector Group Search Reconciliation, LDAP Connector OU Search Reconciliation, and LDAP Connector Role Search Reconciliation Scheduled Jobs
- LDAP Connector Group Sync Reconciliation, LDAP Connector OU Sync Reconciliation, and LDAP Connector Role Sync Reconciliation Scheduled Jobs

3.3.3.3.1 About Scheduled Jobs for Reconciliation of Groups, OUs, and Roles

Depending on your target system, you must specify values for the attributes of the following scheduled jobs.

For ODSEE/OUD:

- LDAP Connector Group Search Reconciliation
- LDAP Connector Group Sync Reconciliation
- LDAP Connector OU Search Reconciliation
- LDAP Connector OU Sync Reconciliation
- LDAP Connector Role Search Reconciliation
- LDAP Connector Role Sync Reconciliation

For OID:

- OID Connector Group Search Reconciliation
- OID Connector Group Sync Reconciliation
- OID Connector OU Search Reconciliation
- OID Connector OU Sync Reconciliation

For eDirectory:

- eDirectory Connector Group Search Reconciliation
- eDirectory Connector Org Search Reconciliation
- eDirectory Connector Role Search Reconciliation

3.3.3.3.2 LDAP Connector Group Search Reconciliation, LDAP Connector OU Search Reconciliation, and LDAP Connector Role Search Reconciliation Scheduled Jobs

The LDAP Connector Group Search Reconciliation scheduled job is used to reconcile group data from the target system. Similarly, the LDAP Connector OU Search Reconciliation and LDAP Connector Role Search Reconciliation scheduled jobs are used to reconcile OU and role data from the target system. You must use these scheduled jobs if either of the following conditions is true:

- Your target system does not contain a changelog attribute.
- You want to reconcile into Oracle Identity Manager changes made to group, OU, or role memberships on the target system.

Table 3-6 describes the attributes of these scheduled jobs.

Table 3-6 Attributes of the LDAP Connector Group Search Reconciliation, LDAP Connector OU Search Reconciliation, and LDAP Connector Role Search Scheduled Jobs

Attribute	Description
Filter	Expression for filtering records that must be reconciled by the scheduled job. Sample value: `startsWith('cn','Samrole1')` Default value: None See Limited Reconciliation for the syntax of this expression.
Incremental Recon Attribute	Enter the name of the target system attribute that holds the time stamp at which the last reconciliation run started. The value in this attribute is used during incremental reconciliation to determine the newest or latest record reconciled from the target system. The default value is the same for all Search Recon Tasks: modifyTimestamp
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile group or role data. Values are: • ODSEE or OUD target resource: `DSEE Server` (default value) • OID target resource: `OID Server` • eDirectory target resource: `eDirectory Server`
Latest Token	This attribute holds the time stamp value of the Incremental Recon Attribute. **Note:** The reconciliation engine automatically enters a value for this attribute after execution. It is recommended that you do not change the value of this attribute. If you manually specify a value for this attribute, then only user accounts that have been modified after the time stamp specified as the value of this attribute are reconciled. If you want to perform a full reconciliation, clear the value in this field. Sample value: `<String>20120516115131Z</String>`

Object Type	Type of object to be reconciled.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector Group Search Reconciliation
	`Group`
	• For LDAP Connector OU Search Reconciliation
	`OU`
	• For LDAP Connector Role Search Reconciliation
	`Role`

Resource Object Name	Name of the resource object that is used for reconciliation.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector Group Search Reconciliation
	`LDAP Group`
	• For LDAP Connector OU Search Reconciliation
	`LDAP Organisation Unit`
	• For LDAP Connector Role Search Reconciliation
	`LDAP Role`

Table 3-6 (Cont.) Attributes of the LDAP Connector Group Search Reconciliation, LDAP Connector OU Search Reconciliation, and LDAP Connector Role Search Scheduled Jobs

Attribute	Description

Scheduled Task Name	Name of the scheduled task used for reconciliation.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector Group Search Reconciliation
	`LDAP Connector Group Search Reconciliation`
	• For LDAP Connector OU Search Reconciliation
	`LDAP Connector OU Search Reconciliation`
	• For LDAP Connector Role Search Reconciliation
	`LDAP Connector Role Search Reconciliation`

3.3.3.3.3 LDAP Connector Group Sync Reconciliation, LDAP Connector OU Sync Reconciliation, and LDAP Connector Role Sync Reconciliation Scheduled Jobs

The LDAP Connector Group Sync Reconciliation scheduled job is used to reconcile group data from the target system. Similarly, the LDAP Connector OU Sync Reconciliation, and LDAP Connector Role Sync Reconciliation scheduled job are used to reconcile OU and role data from the target system. You must use these scheduled jobs if your target system supports the changelog attribute.

Table 3-7 describes the attributes these scheduled jobs.

Table 3-7 Attributes of the LDAP Connector Group Sync Reconciliation, LDAP Connector OU Sync Reconciliation, and LDAP Connector Role Sync Reconciliation Scheduled Jobs

Attribute	Description
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile group or role data. The values are: • For ODSEE or OUD target resource: `DSEE Server` • OID target resource: `OID Server`

Object Type	Type of object to be reconciled.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector Group Sync Reconciliation
	`Group`
	• For LDAP Connector OU Sync Reconciliation
	`OU`
	• For LDAP Connector Role Sync Reconciliation
	`Role`

Table 3-7 (Cont.) Attributes of the LDAP Connector Group Sync Reconciliation, LDAP Connector OU Sync Reconciliation, and LDAP Connector Role Sync Reconciliation Scheduled Jobs

Attribute	Description

Resource Object Name	Name of the resource object that is used for reconciliation.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector Group Sync Reconciliation
	`LDAP Group`
	• For LDAP Connector OU Sync Reconciliation
	`LDAP Organization Unit`
	• For LDAP Connector Role Sync Reconciliation
	`LDAP Role`

Scheduled Task Name	Name of the scheduled task used for reconciliation.
	Depending on the scheduled job you are using, the default values are as follows:
	• For LDAP Connector Group Sync Reconciliation
	`LDAP Connector Group Sync Reconciliation`
	• For LDAP Connector OU Sync Reconciliation
	`LDAP Connector OU Sync Reconciliation`
	• For LDAP Connector Role Sync Reconciliation
	`LDAP Connector Role Sync Reconciliation`

Sync Token	You can manually enter the first Sync Token. To retrieve this token, query cn=changelog on rootDSE on the target system. Then, every time sync reconciliation is run, Sync Token is updated. Browse the changelog attribute of the target system to determine a value from the changelog that must be used to resume a reconciliation run. From the next reconciliation run onward, only data about records that are created or modified since the last reconciliation run ended are fetched into Oracle Identity Manager. Or, you can also leave this field blank, which causes the entire changelog to be read. This attribute stores values in one of the following formats: • If you are using a target system for which the value of the standardChangelog entry in the Configuration lookup definition is set to `true`, then this attribute stores values in the following format: <Integer>*VALUE*</Integer> Sample value: `<Integer>476</Integer>` • If you are using a target system (for example, OUD) for which the value of the standardChangelog entry in the Configuration lookup definition is set to `false,` then this attribute stores values in the following format: <String>*VALUE*</String> Sample value: `<String>dc=example,dc=com:0000013633e514427b6600000013;</String>`

3.3.3.4 Scheduled Jobs for Reconciliation of Deleted Groups, OUs, and Roles

Depending on your target system, you must specify values for the attributes of the following scheduled jobs.

For ODSEE/OUD:

- LDAP Connector Group Search Delete Reconciliation

- LDAP Connector OU Search Delete Reconciliation
- LDAP Connector Role Search Delete Reconciliation

For OID:

- OID Connector Group Search Delete Reconciliation
- OID Connector OU Search Delete Reconciliation

For eDirectory:

- eDirectory Connector Group Search Delete Reconciliation
- eDirectory Connector Org Search Delete Reconciliation
- eDirectory Connector Role Search Delete Reconciliation

Table 3-8 describes the attributes of these scheduled jobs.

Table 3-8 Attributes of the Scheduled Jobs for Deleted Groups, Organizational Units, and Roles Reconciliation

Attribute	Description
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. Default values are: • ODSEE or OUD target resource: `DSEE Server` • OID target resource: `OID Server` • eDirectory target resource: `eDirectory Server`
Object Type	This attribute holds the type of object you want to reconcile.
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed.

3.4 Configuring Scheduled Jobs

This section describes the procedure to configure scheduled jobs. You can apply this procedure to configure the scheduled jobs for lookup field synchronization and reconciliation. For a list of scheduled jobs and their attributes, see Scheduled Jobs for Lookup Field Synchronization and Reconciliation Scheduled Jobs.

This section also includes Configuring the Search Base and Search Scope in Scheduled Jobs and Tasks.

> **Note:**
>
> If the changelog attribute is configured, use the Sync Reconciliation task for incremental reconciliation and the Search for full and delete reconciliation.
>
> If changelog is not configured and the modifytimestamp attribute is used, use the Search Reconciliation task for incremental, full, and delete reconciliation.

3.4.1 Configuring a Scheduled Job

To configure a scheduled job:

1. If you are using Oracle Identity Manager release 11.1.1.*x,* then:
   1. Log in to the Administrative and User Console.
   2. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
   3. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
2. If you are using Oracle Identity Manager release 11.1.2.*x* release, then:
   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 task as follows:
   1. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   2. 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.

   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:**
>
> - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
> - 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.
> - The search base and search scope fields are not available in User, Group, Role, or Organizational Unit Lookup Reconciliation scheduled tasks. To add these fields, see Configuring the Search Base and Search Scope in Scheduled Jobs and Tasks.

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

> **Note:**
>
> You can use the Scheduler Status page in Identity System Administration to either start, stop, or reinitialize the scheduler.

3.4.2 Configuring the Search Base and Search Scope in Scheduled Jobs and Tasks

Configuring the search base and search scope in scheduled jobs and tasks involves the following steps:

- Exporting the Scheduled Job and Task
- Adding Additional Parameters to the Job and Task
- Importing the Updated XML

> **Note:**
>
> The Lookup Reconciliation scheduled jobs do not support custom task attributes, such as Search Scope and Search Base.

3.4.2.1 Exporting the Scheduled Job and Task

To configure the search base and search scope, first export the desired scheduled job and task:

1. Go to **Advanced - Export Deployment Manager File**.
2. Choose **Job** and search for the scheduled job you want to use.
3. Click **Select Children**.
4. Click **Select Dependencies**.
5. Pick the **Scheduled Task** (the root of the tree shown).
6. Click **Confirmation**.
7. Click **Add For Export**.
8. Choose **Exit Wizard and show full selection** and then click **OK**.
9. Click **Export**, and enter a description, if needed, and then click **Export** again.
10. Choose the file you want to use and click **Save**.

3.4.2.2 Adding Additional Parameters to the Job and Task

Add additional parameters to the scheduled job and task:

1. Rename the scheduled task, so that other jobs are not affected by this change:
   a. Look for the **scheduledTask** xml element, and find the xml attribute **name**. For example:

```
<scheduledTask repo-type="MDS"
name="LDAP Connector Search Incremental Reconciliation"
mds-path="/db" mds-file="LDAP Connector Search Incremental
Reconciliation.xml">
```

   b. Replace all the occurrences of the old name with a new value.

      For example, replace all occurrences of "LDAP Connector Search Incremental Reconciliation" with "LDAP Connector Search Incremental Reconciliation Extended".

2. Rename the scheduled job:

   Look for the **Job** element.

   Change the value of the **name** xml attribute. For example, change "LDAP Connector OU Search Reconciliation" to "LDAP Connector OU Search Reconciliation Extended".

3. Add additional parameters to the scheduled task:

   a. Find the `scheduledTask/completeXml/scheduledTasks/task/parameters` element.

   b. Add the following parameters:

```
<string-param required="false" encrypted="false" helpText="Search
Scope">SCOPE</string-param>
<string-param required="false" encrypted="false" helpText="Search
Base">Base Context</string-param>
```

4. Add additional parameters to the scheduled job:

   a. Find the `Job/attributes` element.

   b. Add the following parameters:

```
<object>
<key>SCOPE</key>
<value type="jobparameter">
<name type="string">SCOPE</name>
<required type="boolean">false</required>
<encrypted type="boolean">false</encrypted>
<helpText type="string">Search Scope</helpText>
<dataType type="string">String</dataType>
<paramKey type="string">30</paramKey>
<paramValue type="string"/>
</value>
</object>
<object>
<key>Base Context</key>
<value type="jobparameter">
<name type="string">Base Context</name>
<required type="boolean">false</required>
<encrypted type="boolean">false</encrypted>
<helpText type="string">Search Base</helpText>
<dataType type="string">String</dataType>
<paramKey type="string">31</paramKey>
<paramValue type="string"/>
</value>
</object>
```

3.4.2.3 Importing the Updated XML

Finally, import the updated xml back into Oracle Identity Manager:

1. Go to **Advanced - Import Deployment Manager File**.
2. Choose the updated xml file and click **Open**.
3. Click **Add File**.
4. Click **Import**.

3.5 Performing Provisioning Operations in Oracle Identity Manager Release 11.1.1.*x*

This section discusses the following topics:

- About Provisioning Operation in Oracle Identity Manager
- Direct Provisioning
- Direct Provisioning for Groups, Roles, and Organizations
- Request-Based Provisioning
- Switching Between Request-Based Provisioning and Direct Provisioning

3.5.1 About Provisioning Operation in Oracle Identity Manager

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create target system account for the user.

When you install the connector on Oracle Identity Manager, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you configure the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Switching Between Request-Based Provisioning and Direct Provisioning .

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning

> **See Also:**
>
> olink:OMUSG Manually Completing a Task in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for information about the types of provisioning.

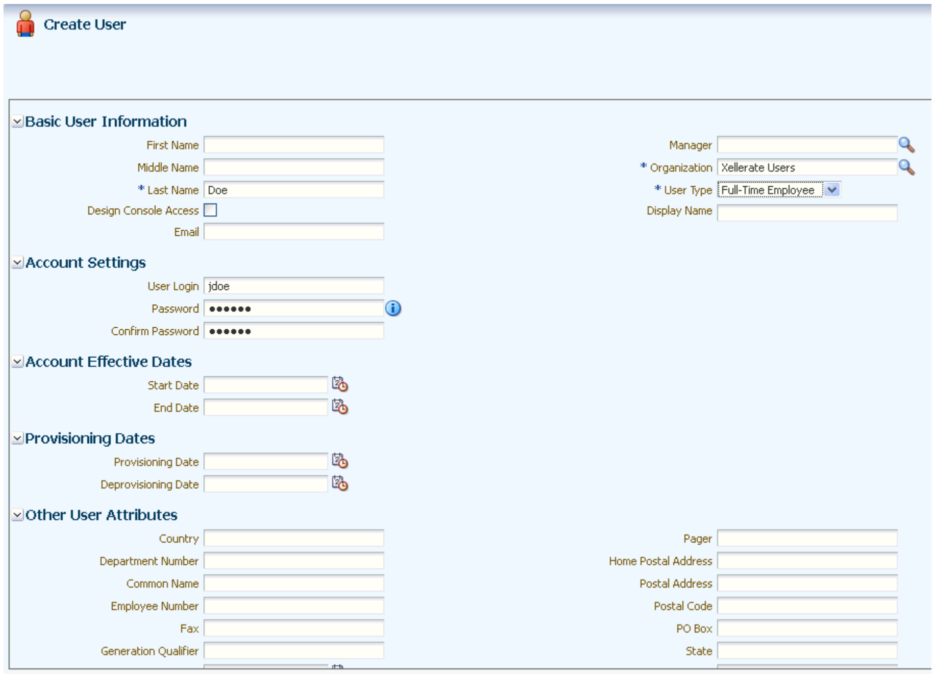
3.5.2 Direct Provisioning

> **Note:**
>
> This example is for an LDAPv3 target system. However, to provision another target system such as eDirectory or OID, the steps are similar.

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
   a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.
   b. On the user details page, enter values for the OIM User fields, and then click **Save**. Figure 3-1 shows this page.

Figure 3-1 User Details Page



Create User

Basic User Information

First Name
Middle Name
* Last Name: Doe
Design Console Access: □
Email
Manager
* Organization: Xellerate Users
* User Type: Full-Time Employee
Display Name

Account Settings

User Login: jdoe
Password: ••••••
Confirm Password: ••••••

Account Effective Dates

Start Date
End Date

Provisioning Dates

Provisioning Date
Deprovisioning Date

Other User Attributes

Country
Department Number
Common Name
Employee Number
Fax
Generation Qualifier
Pager
Home Postal Address
Postal Address
Postal Code
PO Box
State

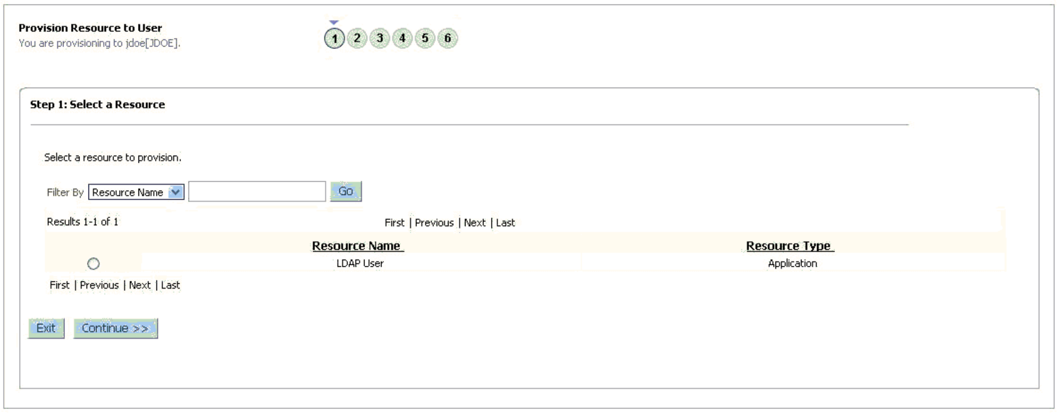
3. If you want to provision a target system account to an existing OIM User, then:
   a. On the Welcome to Identity Administration page, search for the OIM User by selecting Users from the list on the left pane.
   b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. On the user details page, click the **Resources** tab.

5. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.

6. On the Step 1: Select a Resource page, select LDAP User resources from the list and then click **Continue.**

   Figure 3-2 shows the Step 1: Select a Resource page.

Figure 3-2 Step 1: Select a Resource Page



Provision Resource to User

You are provisioning to jdoe[JDOE].

Step 1: Select a Resource

Select a resource to provision.

Filter By: Resource Name

Results 1-1 of 1

First | Previous | Next | Last

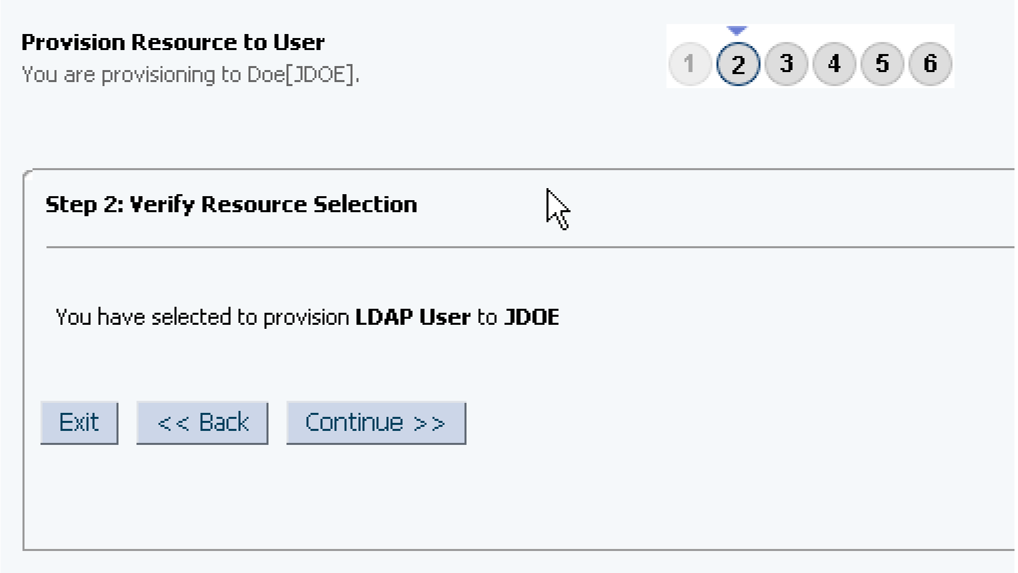
	Resource Name	Resource Type
○	LDAP User	Application

First | Previous | Next | Last

7. On the Step 2: Verify Resource Selection page, click **Continue**.

   Figure 3-3 shows the Step 2: Verify Resource Selection page.

Figure 3-3 Step 2: Verify Resource Selection Page



Provision Resource to User

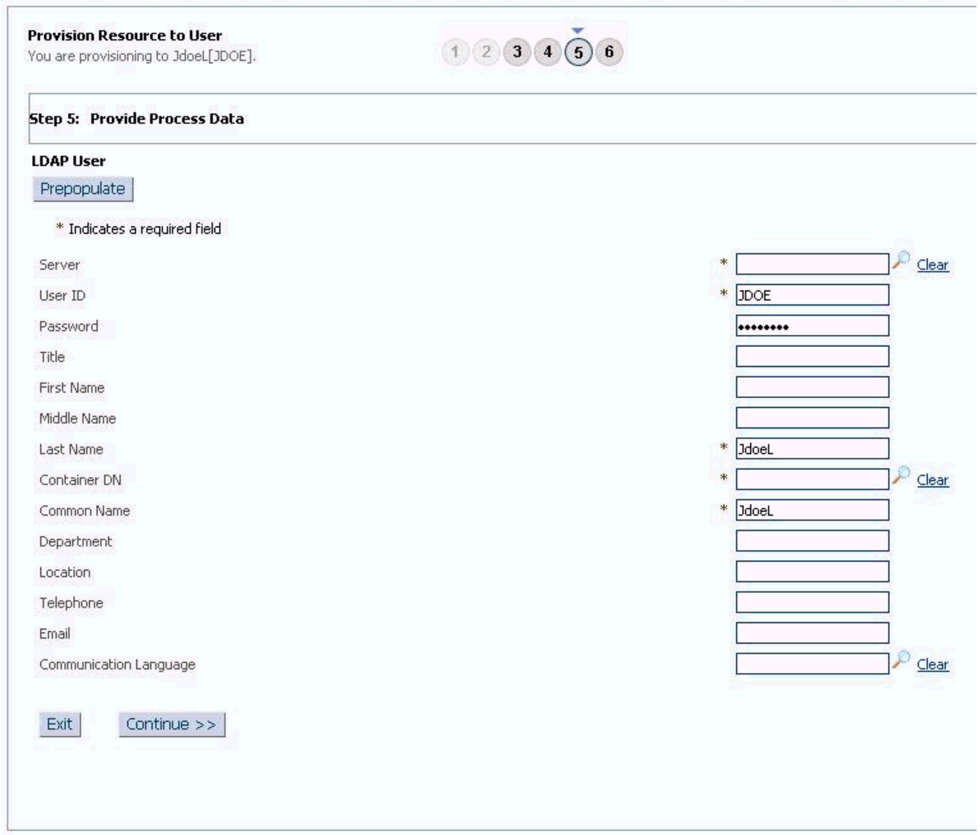
You are provisioning to Doe[JDOE].

Step 2: Verify Resource Selection

You have selected to provision **LDAP User** to **JDOE**

8. On the Step 5: Provide Process Data for LDAP User Form page, enter the details of the account that you want to create on the target system and then click **Continue.** Figure 3-4 shows the user details added.

Figure 3-4   Step 5: Provide Process Data for LDAP User Form Page



Provision Resource to User

You are provisioning to JdoeL[JDOE].

Step 5: Provide Process Data

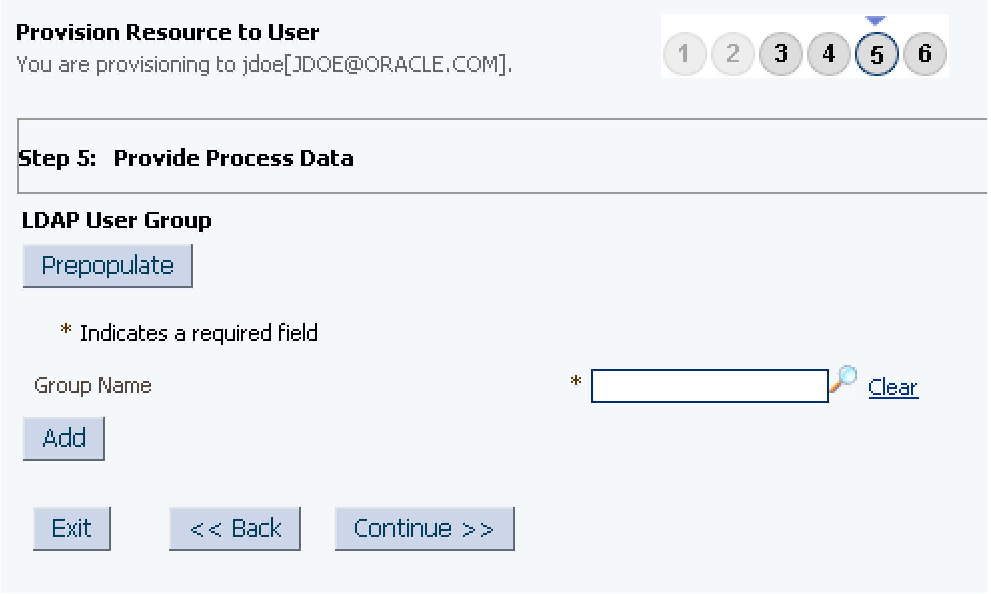
LDAP User

* Indicates a required field

Server *
User ID * JDOE
Password ••••••••
Title
First Name
Middle Name
Last Name * JdoeL
Container DN *
Common Name * JdoeL
Department
Location
Telephone
Email
Communication Language

9. If required, on the Step 5: Provide Process Data for LDAP User Group page, search for and select a group for the user on the target system and then click **Continue**. Figure 3-5 shows this page.

Figure 3-5   Step 5: Provide Process Data for LDAP User Group Page



Provision Resource to User

You are provisioning to jdoe[JDOE@ORACLE.COM].

Step 5: Provide Process Data

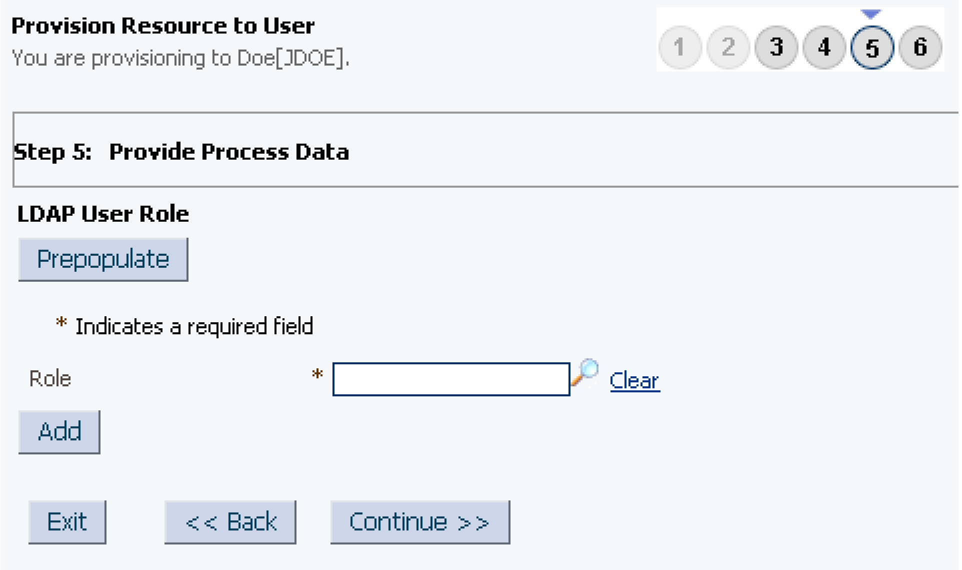
LDAP User Group

* Indicates a required field

Group Name *

10. If required, On the Step 5: Provide Process Data for LDAP User Role page, search for and select role, and then click **Continue**. Figure 3-6 shows this page.

Figure 3-6   Step 5: Provide Process Data for LDAP User Role Page



Provision Resource to User

You are provisioning to Doe[JDOE].

Step 5:   Provide Process Data

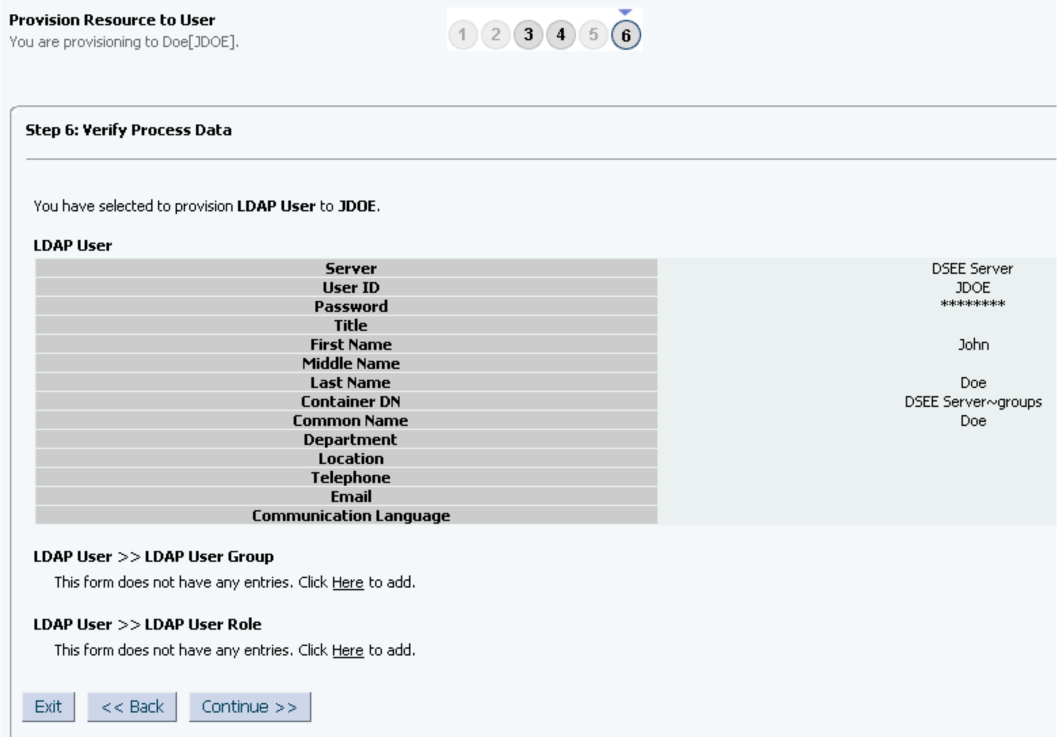
LDAP User Role

* Indicates a required field

Role *

11. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**. Figure 3-7 shows Step 6: Verify Process Data page.

Figure 3-7   Step 6: Verify Process Data Page



Provision Resource to User

You are provisioning to Doe[JDOE].

Step 6: Verify Process Data

You have selected to provision **LDAP User** to **JDOE**.

LDAP User

Server	DSEE Server
User ID	JDOE
Password	********
Title	
First Name	John
Middle Name	
Last Name	Doe
Container DN	DSEE Server~groups
Common Name	Doe
Department	
Location	
Telephone	
Email	
Communication Language	

LDAP User >> LDAP User Group

This form does not have any entries. Click Here to add.

LDAP User >> LDAP User Role

This form does not have any entries. Click Here to add.

12. Close the window displaying the "Provisioning has been initiated" message.
13. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.5.3 Direct Provisioning for Groups, Roles, and Organizations

> **Note:**
>
> This example is for an LDAPv3 target system. However, to provision another target system such as eDirectory or OID, the steps are similar.

Groups, Roles, and Organizations of directory can be provisioned to OIM organizations. To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM Organization and then provision a target system account, then:
   a. On the Welcome to Identity Administration page, in the Organizations region, click **Create Organization**.
   b. On the organization details page, enter values for the OIM Organization fields, and then click **Save**.
3. If you want to provision a target system account to an existing OIM Organization, then:
   a. On the Welcome to Identity Administration page, search for the OIM Organization by selecting Organizations from the list on the left pane.
   b. From the list of users displayed in the search results, select the OIM Organization. The user details page is displayed on the right pane.
4. On the user details page, click the **Resources** tab.
5. From the Action menu, select **Provision**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to Organization page is displayed in a new window.
6. On the Step 1: Select a Resource page, select LDAP Group resources from the list and then click **Continue.**

   > **Note:**
   >
   > If you want to provision Role or Organizational Unit, then select LDAP Role or LDAP Organization Unit respectively.

7. On the Step 2: Verify Resource Selection page, click **Continue**.
8. On the Step 5: Provide Process Data for LDAP Group Form page, enter the details of the account that you want to create on the target system and then click **Continue.**
9. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.

10. Close the window displaying the "Provisioning has been initiated" message.
11. On the Resources tab, click **Refresh** to view the newly provisioned resource.

> **Note:**
>
> OIM created Organizations do not relate to the OU objects on the Directory Resources of OID or Microsoft Active Directory. The OIM connector does not support the creation of any OU objects in OIM which can then be provisioned to OID or Microsoft Active Directory. Instead, OUs can be created directly on the Directory Services of OID or Microsoft Active Directory.
>
> Additionally, as best practice, ensure that all newly created OUs and other objects are imported through Trusted Resource Reconciliation from OID or Microsoft Active Directory into OIM.

3.5.4 Request-Based Provisioning

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

> **Note:**
>
> The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- End User's Role in Request-Based Provisioning
- Approver's Role in Request-Based Provisioning

3.5.4.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** on the top right corner of the page.
3. On the Welcome to Identity Manager Advanced Administration page, click **Requests** on the Administration tab.
4. From the Actions menu on the left pane, select **Create Request**.

   The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.

7. From the Available Users list, select the user to whom you want to provision the account.

   If you want to create a provisioning request for more than one user, then from the Available Users list, select users to whom you want to provision the account.

8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.

9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.

10. From the Available Resources list, select the following, move it to the Selected Resources list, and then click **Next:**

    For target resource configuration: **LDAP User**

11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.

12. On the Justification page, you can specify values for the following fields, and then click **Finish**.

    - Effective Date
    - Justification

    A message confirming that your request has been sent successfully is displayed along with the Request ID.

13. If you click the request ID, then the Request Details page is displayed.

14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.5.4.2 Approver's Role in Request-Based Provisioning

The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the Approvals tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task** (twice).

   A message confirming that the task was approved is displayed.

3.5.5 Switching Between Request-Based Provisioning and Direct Provisioning

Switching between request-based provisioning and direct provisioning involves the following:

- Switching From Request-Based to Direct Provisioning

- Switching From DIrect to Request-Based Provisioning

> **Note:**
>
> It is assumed that you have performed the procedure described in Configuring Oracle Identity Manager for Request-Based Provisioning.

3.5.5.1 Switching From Request-Based to Direct Provisioning

If you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **LDAP User** process definition.
   c. Deselect the Auto Save Form check box.
   d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **LDAP User** resource object.
   c. Deselect the Self Request Allowed check box.
   d. Click the Save icon.

3.5.5.2 Switching From DIrect to Request-Based Provisioning

If you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **LDAP User** process definition.
   c. Select the **Auto Save Form** check box.
   d. Click the Save icon.
3. If you want to enable end users to raise requests for themselves, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **LDAP User** resource object.
   c. Select the Self Request Allowed check box.
   d. Click the Save icon.

3.6 Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later

To perform provisioning operations in Oracle Identity Manager release 11.1.2 or later:

1. Log in to Oracle Identity Administrative and User console.
2. Create a user. See Managing Users in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance created in Step 3, and then click **Checkout.**
5. Specify value for fields in the application form and then click **Ready to Submit.**
6. Click **Submit.**
7. If you want to provision entitlements, then:
    a. On the Entitlements tab, click **Request Entitlements.**
    b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout.**
    c. Click **Submit.**

3.7 Uninstalling the Connector

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

4

Using the Connector with Oracle Directory Server Enterprise Edition

The chapter describes the following information about using the connector with Oracle Directory Server Enterprise Edition (ODSEE):

- Configuring Secure Communications
- Preconfigured Lookup Definitions for an ODSEE Target System
- Reconciling ODSEE Users Under Their Corresponding Organizations in Oracle Identity Manager
- Reconciling ODSEE Groups and Roles Under One Organization in Oracle Identity Manager

4.1 Configuring Secure Communications

To provide secure communications to the ODSEE target system, configure SSL between Oracle Identity Manager, the Connector Server, and the ODSEE target system.

For more information, see Configuring SSL for the Connector.

4.2 Preconfigured Lookup Definitions for an ODSEE Target System

This section discusses the lookup definitions that are created in Oracle Identity Manager when you deploy the connector for an ODSEE target system. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed. These lookup definitions are as follows:

- Lookup.LDAP.Configuration
- Lookup.LDAP.Configuration.Trusted
- Preconfigured Lookup Definitions for User Operations
- Preconfigured Lookup Definitions for Group Operations
- Preconfigured Lookup Definitions for Organizational Unit Operations
- Preconfigured Lookup Definitions for Role Operations

4.2.1 Lookup.LDAP.Configuration

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

Table 4-1 lists the default entries in this lookup definition.

Table 4-1   Entries in the Lookup.LDAP.Configuration Lookup Definition

Code Key	Decode	Description
accountObjectClasses	"top","person", "organizationalPerson","inetOrgPerson"	This entry holds the list of object classes required for a USER object.
accountSearchFilter	objectClass=*	This entry holds a search filter that any account needs to match in order to be returned.
accountSynchronizationFilter	objectClass=*	This entry holds a filter for all of the entries returned during the SyncOp operation that must match.
ldapGroupFilterBehavior	accept	This entry specifies the behavior for an LDAP group filter.
ldapGroupMembershipAttribute	ismemberof	This entry specifies the value for the LDAP group membership attribute.
accountUserNameAttribute	cn	This entry holds attributes that contain the name of a USER object.
attributesToSynchronize	"cn","uid"	This entry holds the list of attributes to return whenever a SyncOp is run.
blockSize	100	This entry holds the block size for simple paged results and VLV index searches.
Bundle Name	org.identityconnectors.ldap	This entry holds the name of the connector bundle package. Do *not* modify this entry.
Bundle Version	1.0.6380	This entry holds the version of the connector bundle class. Do *not* modify this entry.
changelogBaseDN	cn=changelog	This entry holds the baseDN where the connector is to find the changelog attribute value.
changeLogBlockSize	100	This entry holds the block size for simple paged results and VLV index searches when reading changelog during a SyncOp operation.
changeNumberAttribute	changeNumber	This entry holds the attribute name used for changelog.
Connector Name	org.identityconnectors.ldap.LdapConnector	This entry holds the name of the connector class. Do *not* modify this entry.
disabledRoleName	cn=nsmanageddisabledrole,dc=example,dc=com	This entry holds the name of the role that must be present in the entry when an account is disabled and that the enabledBaseOnRole is set to `TRUE`.
enabledAttribute	nsaccountlock	This entry holds the name of the attribute that is required to enable or disable accounts.
enabledValue	false	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is enabled.
disabledValue	true	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is disabled.
enabledWhenNoAttribute	true	This entry defines if the status must be enabled or disabled when the property defined in enabledAttribute is not present in the entry.

Table 4-1 (Cont.) Entries in the Lookup.LDAP.Configuration Lookup Definition

Code Key	Decode	Description
enabledBasedOnRole	false	This entry specifies whether enabling or disabling a user must be controlled by a role instead of the enabledAttribute attribute. When you set the value of this entry to `true,` it takes precedence over all the other enabled or disabled-related flags.

filterWithOrInsteadOfAnd	false	This entry specifies whether the changelog filter is built using an OR or AND filter.
		Enter `true` if the changelog filter is built using an OR filter instead of AND filter. Otherwise, enter `false.`
		An OR filter is in the following format:
		`(|(changeNumber=1) (changeNumber=2) . . . (changeNumber=xxx))`
		An AND filter is of the following format:
		`(&(changeNumber>=0) (changeNumber<=xxx))`

Group Configuration Lookup	Lookup.LDAP.Group.Configuration	This entry holds the name of the lookup definition that contains group-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of groups. Do *not* modify this entry.
groupMemberAttribute	uniqueMember	This entry holds the LDAP attribute that stores the member for non-POSIX static groups.
groupObjectClasses (optional)	"top","groupOfUniqueNames"	This entry holds the list of object classes required for a GROUP object. **Note**. This entry is not available by default. You must add it if you want to customize the lookup definition.
maintainLdapGroupMembership	true	This entry specifies whether the connector modifies group membership of renamed or deleted user entries.
maintainPosixGroupMembership	false	This entry specifies whether the connector modifies group membership of renamed or deleted user entries.
objectClassesToSynchronize	"inetOrgPerson","groupOfNames","groupOfUniqueNames","nsRoleDefinition","organizationalUnit"	This entry holds the list of object classes to be synchronized. Any synchronized entry in order to be returned must have at least one object class from this list. If this list of object classes is empty or the code key is missing, then no filtering is performed on the object classes.
OU Configuration Lookup	Lookup.LDAP.OU.Configuration	This entry holds the name of the lookup definition that contains organization-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of organizational units. Do *not* modify this entry.
passwordAttribute	userPassword	This entry holds the name of the attribute to which the predefined PASSWORD attribute is written to.
readSchema	true	This entry specifies whether the schema must be read from the server.

Table 4-1 (Cont.) Entries in the Lookup.LDAP.Configuration Lookup Definition

Code Key	Decode	Description
removeLogEntryObjectClassFromFilter	true	This entry specifies whether the changelog filter contains a condition on the changelog objectclass.
respectResourcePasswordPolicyChangeAfterReset	true	Enter `TRUE` as the decode value if the connector throws exceptions (for example, PasswordExpiredException) appropriately when binding check for the Password Expired control and Password Policy control. Otherwise, enter `FALSE.`
Role Configuration Lookup	Lookup.LDAP.Role.Configuration	This entry holds the name of the lookup definition that contains role-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of roles. Do *not* modify this entry.
roleObjectClasses (optional)	"top", "ldapsubentry","nsRoleDefinition", "nsSimpleRoleDefinition", "nsManagedRoleDefinition"	This entry holds the list of object classes required for a ROLE object. **Note**. This entry is not available by default. You must add it if you want to customize the lookup definition.
standardChangelog	true	This entry specifies how the connector accesses the changelog attribute. This entries applies mainly to an OUD target system. For other target systems, leave the value set to true.
synchronizeWithModifyTimestamps	false	This property specifies whether the connector must use the modify timestamps attribute instead of the changelog attribute during a SyncOp operation.
uidAttribute	nsuniqueid	This entry holds the LDAP attribute to which the predefined UID attribute must be mapped to.
usePagedResultControl	true	This entry specifies whether simple paged search is preferred over VLV index search when both are available.
User Configuration Lookup	Lookup.LDAP.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of users. Do *not* modify this entry.
vlvSortAttribute	uid	This entry holds the attribute used as the sort key for the VLV index.
changelogUidAttribute	targetuniqueid	This entry holds the name of the attribute that contains the uniqueId of the modified entry in the changelog.
readTimeout	120000 milliseconds	This property holds the value for the read timeout configuration property. These values can be increased or decreased if necessary. If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
connectTimeout	120000 milliseconds	This property holds the value for the connect timeout configuration property. These values can be increased or decreased if necessary.If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.

Table 4-1 (Cont.) Entries in the Lookup.LDAP.Configuration Lookup Definition

Code Key	Decode	Description
referrals	ignore, follow, or throw	This property holds the value for the read referrals configuration property. If this property is not added in the configuration lookup definition, then the value is set to ignore by default.

4.2.2 Lookup.LDAP.Configuration.Trusted

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

Table 4-2 lists the default entries in this lookup definition.

Table 4-2 Entries in the Lookup.LDAP.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
accountObjectClasses	"top","person", "organizationalPerson","inetOrgPerson"	This entry holds the list of object classes required for a USER object.
Bundle Name	org.identityconnectors.ldap	This entry holds the name of the connector bundle package. Do *not* modify this entry.
Bundle Version	1.0.6380	This entry holds the version of the connector bundle class. Do *not* modify this entry.
changeLogBlockSize	100	This entry holds the block size for simple paged results and VLV index searches when reading changelog during a SyncOp operation.
changeNumberAttribute	changeNumber	This entry holds the attribute name used for changelog.
Connector Name	org.identityconnectors.ldap.LdapConnector	This entry holds the name of the connector class. Do *not* modify this entry.
objectClassesToSynchronize	"inetOrgPerson","groupOfNames","organizationalUnit"	This entry holds the list of object classes to be synchronized. Any synchronized entry in order to be returned must have at least one object class from this list. If this list of object classes is empty or the code key is missing, then no filtering is performed on the object classes.
uidAttribute	nsuniqueid	This entry holds the LDAP attribute to which the Uid must be mapped to.
Any Incremental Recon Attribute Type	true	Indicates that any format of token is accepted during reconciliation.
disabledValue	true	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is disabled.
enabledAttribute	nsaccountlock	This entry holds the name of the attribute that is required to enable or disable accounts.
enabledValue	false	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is enabled.

Table 4-2 (Cont.) Entries in the Lookup.LDAP.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
enabledWhenNoAttribute	true	This entry defines if the status must be enabled or disabled when the property defined in enabledAttribute is not present in the entry.
usePagedResultControl	true	This entry specifies whether simple paged search is preferred over VLV index search when both are available.
readTimeout	120000 milliseconds	This property holds the value for the read timeout configuration property. These values can be increased or decreased if necessary. If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
connectTimeout	120000 milliseconds	This property holds the value for the connect timeout configuration property. These values can be increased or decreased if necessary.If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
referrals	ignore, follow, or throw	This property holds the value for the read referrals configuration property. If this property is not added in the configuration lookup definition, then the value is set to ignore by default.
User Configuration Lookup	Lookup.LDAP.UM.Configuration.Trusted	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do *not* modify this entry.

4.2.3 Preconfigured Lookup Definitions for User Operations

This section discusses the following lookup definitions for user operations:

- Lookup.LDAP.UM.Configuration
- Lookup.LDAP.UM.Configuration.Trusted
- Lookup.LDAP.UM.ProvAttrMap
- Lookup.LDAP.UM.ReconAttrMap
- Lookup.LDAP.UM.ProvValidation
- Lookup.LDAP.UM.ReconTransformation
- Lookup.LDAP.UM.ReconValidation
- Lookup.LDAP.UM.ReconAttrMap.Trusted
- Lookup.LDAP.UM.TrustedDefaults

4.2.3.1 Lookup.LDAP.UM.Configuration

The Lookup.LDAP.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 4-3 lists the default entries in this lookup definition.

Table 4-3 Entries in the Lookup.LDAP.UM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.LDAP.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.LDAP.UM.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.LDAP.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.LDAP.UM.ReconAttrMap for more information about this lookup definition.
Recon Transformation Lookup **Note:** This entry does not exist by default. You must add it if you want to enable transformation during reconciliation.	Lookup.LDAP.UM.ReconTransformation	This entry holds the name of the lookup definition that is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See Configuring Transformation of Data During Reconciliation for more information about adding entries in this lookup definition.
Recon Validation Lookup **Note:** This entry does not exist by default. You must add it if you want to enable validation during reconciliation.	Lookup.LDAP.UM.ReconValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values that are fetched from the target system during reconciliation. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.
Provisioning Validation Lookup **Note:** This entry does not exist by default. You must add it if you want to enable validation during provisioning.	Lookup.LDAP.UM.ProvValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values entered on the process form during provisioning operations. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.

4.2.3.2 Lookup.LDAP.UM.Configuration.Trusted

The Lookup.LDAP.UM.Configuration.Trusted lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during trusted source user reconciliation runs.

Table 4-4 lists the default entries in this lookup definition.

Table 4-4 Entries in the Lookup.LDAP.UM.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
Recon Attribute Defaults	Lookup.LDAP.UM.TrustedDefaults	This entry holds the name of the lookup definition that maps reconciliation fields to their default values. See Lookup.LDAP.UM.TrustedDefaults for more information.
Recon Attribute Map	Lookup.LDAP.UM.ReconAttrMap.Trusted	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.LDAP.UM.ReconAttrMap for more information about this lookup definition.

4.2.3.3 Lookup.LDAP.UM.ProvAttrMap

The Lookup.LDAP.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definitions is used during provisioning. This lookup definition is preconfigured.

For the default user fields that you can specify or modify values during provisioning operations, see User Fields for Provisioning an ODSEE Target System.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Extending the Functionality of the Connector for more information.

4.2.3.4 Lookup.LDAP.UM.ReconAttrMap

The Lookup.LDAP.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is used during reconciliation. This lookup definition is preconfigured.

For the default user fields that you can specify or modify values during reconciliation operations, see User Fields for Target Resource Reconciliation.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Connector for more information.

4.2.3.5 Lookup.LDAP.UM.ProvValidation

The Lookup.LDAP.UM.ProvValidation lookup definition is used to configure validation of attribute values entered on the process form during provisioning operations. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.

4.2.3.6 Lookup.LDAP.UM.ReconTransformation

The Lookup.LDAP.UM.ReconTransformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See Configuring Transformation of Data During Reconciliation for more information about adding entries in this lookup definition.

4.2.3.7 Lookup.LDAP.UM.ReconValidation

The Lookup.LDAP.UM.ReconValidation lookup definition is used to configure validation of attribute values that are fetched from the target system during reconciliation. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.

4.2.3.8 Lookup.LDAP.UM.ReconAttrMap.Trusted

The Lookup.LDAP.UM.ReconAttrMap.Trusted lookup definition holds mappings between resource object fields and target system attributes. This lookup definitions is used during trusted source user reconciliation runs.

This lookup definition is preconfigured. Table 1-5 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Connector for more information.

4.2.3.9 Lookup.LDAP.UM.TrustedDefaults

The Lookup.LDAP.UM.TrustedDefaults lookup definition holds mappings between reconciliation fields and their default values. This lookup definition is used when there is a mandatory field on the OIM User form, but no corresponding field in the target system from which values can be fetched during trusted source reconciliation.

You can add entries to this lookup definition by ensuring that the Code Key and Decode values are in the following format:

- **Code Key:** Name of the reconciliation field of the resource object
- **Decode:** Corresponding default value to be displayed

For example, the Employee Type field is a mandatory field on the OIM User form. However, on the target system, there is no information about the employee type for a user account. During reconciliation, as the Employee Type field cannot be left empty, you must specify a value for this field.

Therefore, the Decode value of the Employee Type Code Key has been set to Full-Time. This implies that the value of the Employee Type field on the OIM User form displays Full-Time for all user accounts reconciled from the target system.

This lookup definition is preconfigured. Table 4-5 lists the default entries.

Table 4-5 Entries in the Lookup.LDAP.UM.TrustedDefaults Lookup Definition

Code Key	Decode
Employee Type	Full-Time
Organization	Xellerate Users
User Type	End-User

4.2.4 Preconfigured Lookup Definitions for Group Operations

This section discussed the following lookup definitions for group operations:

- Lookup.LDAP.Group.Configuration
- Lookup.LDAP.Group.ProvAttrMap
- Lookup.LDAP.Group.ReconAttrMap

4.2.4.1 Lookup.LDAP.Group.Configuration

The Lookup.LDAP.Group.Configuration lookup definition holds configuration entries that are specific to the group object type. This lookup definition is used during group management operations when your target system is configured as a target resource.

Table 4-6 lists the default entries in this lookup definition.

Table 4-6 Entries in the Lookup.LDAP.Group.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.LDAP.Group.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.LDAP.Group.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.LDAP.Group.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.LDAP.Role.ProvAttrMap for more information about this lookup definition.

4.2.4.2 Lookup.LDAP.Group.ProvAttrMap

The Lookup.LDAP.Group.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during group provisioning operations.

This lookup definition is preconfigured. Table 1-25 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Adding Custom Fields for Provisioning for more information.

4.2.4.3 Lookup.LDAP.Group.ReconAttrMap

The Lookup.LDAP.Group.ReconAttrMap lookup definition holds mappings between resource object fields for groups and target system attributes. This lookup definition is used during reconciliation.

This lookup definition is preconfigured. Table 1-8 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation.

4.2.5 Preconfigured Lookup Definitions for Organizational Unit Operations

This section discusses the following lookup definitions for organizational unit operations:

- Lookup.LDAP.OU.Configuration
- Lookup.LDAP.OU.ProvAttrMap
- Lookup.LDAP.OU.ReconAttrMap

4.2.5.1 Lookup.LDAP.OU.Configuration

The Lookup.LDAP.OU.Configuration lookup definition holds configuration entries that are specific to the organizational unit object type. This lookup definition is used during organizational unit management operations when your target system is configured as a target resource.

Table 4-7 lists the default entry in this lookup definition.

Table 4-7 Entries in the Lookup.LDAP.OU.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.LDAP.OU.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.LDAP.OU.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.LDAP.OU.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.LDAP.OU.ReconAttrMap for more information about this lookup definition.

4.2.5.2 Lookup.LDAP.OU.ProvAttrMap

The Lookup.LDAP.OU.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during provisioning.

This lookup definition is preconfigured. Table 1-30 lists the default entries.

You can add entries in this lookup definition if you want to map new target system attributes for provisioning. See Extending the Functionality of the Connector for more information.

4.2.5.3 Lookup.LDAP.OU.ReconAttrMap

The Lookup.LDAP.OU.ReconAttrMap lookup definition holds mappings between resource object fields for organizational units (OUs) and target system attributes. This lookup definitions is used during reconciliation.

This lookup definition is preconfigured. Table 1-13 lists the default entries.

You can add entries in this lookup definition if you want to map new target system attributes for provisioning. See Extending the Functionality of the Connector for more information.

4.2.6 Preconfigured Lookup Definitions for Role Operations

This section discusses the following lookup definitions for role operations:

- Lookup.LDAP.Role.Configuration
- Lookup.LDAP.Role.ProvAttrMap
- Lookup.LDAP.Role.ReconAttrMap

4.2.6.1 Lookup.LDAP.Role.Configuration

The Lookup.LDAP.Role.Configuration lookup definition holds configuration entries that are specific to the role object type. This lookup definition is used during role management operations when your target system is configured as a target resource.

Table 4-8 Entries in the Lookup.LDAP.Role.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.LDAP.Role.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.LDAP.Role.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.LDAP.Role.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.LDAP.Role.ReconAttrMap for more information about this lookup definition.

4.2.6.2 Lookup.LDAP.Role.ProvAttrMap

The Lookup.LDAP.Role.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during role provisioning operations. This lookup definition is preconfigured.

Table 1-28 lists the default entries in this lookup definition.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Adding Custom Fields for Provisioning for more information.

4.2.6.3 Lookup.LDAP.Role.ReconAttrMap

The Lookup.LDAP.Role.ReconAttrMap lookup definition holds mappings between resource object fields for roles and target system attributes. This lookup definitions is used during reconciliation.

This lookup definition is preconfigured.Table 1-11 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Adding New Fields for Trusted Source Reconciliation for more information.

4.3 Reconciling ODSEE Users Under Their Corresponding Organizations in Oracle Identity Manager

> **Note:**
>
> Before you perform the following optional task, make sure you have created the corresponding organizations with the same names from the target system in Oracle Identity Manager.

To reconcile users from an ODSEE target system under their corresponding organizations in Oracle Identity Manager:

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

2. Find the **Lookup.LDAP.UM.ReconAttrMap.Trusted** lookup.
3. Add the following entry:
   - **code**: Organization
   - **decode**: __PARENTRDNVALUE__

4.4 Reconciling ODSEE Groups and Roles Under One Organization in Oracle Identity Manager

This section describes the following optional procedures:

- Reconciling ODSEE Groups Under One Organization
- Reconciling ODSEE Roles Under One Organization

4.4.1 Reconciling ODSEE Groups Under One Organization

To configure ODSEE groups to be reconciled under one organization:

1. Log in to the Oracle Identity Manager Design Console.
2. Find the **Lookup.LDAP.Group.Configuration** lookup.
3. Add a new entry such as the following:
   - **code**: Recon Attribute Defaults
   - **decode**: Lookup.LDAP.Group.Defaults

   Note that the decode value is an example, and you can set your own lookup name.
4. Create the new **Lookup.LDAP.Group.Defaults** lookup (specified in the previous step).
5. Add a new entry:
   - **code**: Org Name
   - **decode**: Group1

   The decode value is the name of the Oracle Identity Manager organization under which all groups will be reconciled.
6. Find the **Lookup.LDAP.Group.ReconAttrMap** lookup.
7. Delete the row with the code **Org Name**.
8. Find the Recon Rule **LDAP Group Recon**.
9. Change the current rule **Organization Name Equals Group Name** to **Organization Name Equals Org Name** by double clicking the rule element and changing the **Group Name** attribute to **Org Name**.
10. Save the rule.
11. Open the **LDAP Group** resource object and click **Create Reconciliation Profile**.

4.4.2 Reconciling ODSEE Roles Under One Organization

To configure ODSEE roles to be reconciled under one organization:

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

2. Find the **Lookup.LDAP.Role.Configuration** lookup.
3. Add a new entry such as the following:
   - **code**: Recon Attribute Defaults
   - **decode**: Lookup.LDAP.Role.Defaults

   Note that the decode value is an example, and you can set your own lookup name.
4. Create the new **Lookup.LDAP.Role.Defaults** lookup (specified in the previous step).
5. Add a new entry:
   - **code**: Org Name
   - **decode**: Role1

   The decode value is the name of the Oracle Identity Manager organization under which all roles will be reconciled.
6. Find **Lookup.LDAP.Role.ReconAttrMap**.
7. Delete the row with code **Org Name**.
8. Find the Recon Rule **LDAP Role Recon**.
9. Change the current rule **Organization Name Equals Role Name** to **Organization Name Equals Org Name** by double clicking the rule element and changing attribute **Role Name** to **Org Name**.
10. Save the rule.
11. Open the **LDAP Role** resource object and click **Create Reconciliation Profile**.

5 Using the Connector with Oracle Unified Directory

The chapter describes the following information about using the connector with Oracle Unified Directory (OUD):

- Configuring Secure Communications
- Preconfigured Lookup Definitions for an OUD Target System
- Reconciling OUD Users Under Their Corresponding Organizations in Oracle Identity Manager
- Reconciling OUD Groups Under One Organization in Oracle Identity Manager
- Reconciling Newly Created Objects for an OUD Target System
- Guidelines on Using the Connector for Dynamic and Virtual Static Groups

5.1 Configuring Secure Communications

To provide secure communications to the OUD target system, configure SSL between Oracle Identity Manager, the Connector Server, and the OUD target system.

For more information, see Configuring SSL for the Connector.

5.2 Preconfigured Lookup Definitions for an OUD Target System

This section discusses the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector for the OUD target system. 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.LDAP.OUD.Configuration
- Lookup.LDAP.OUD.Configuration.Trusted
- Preconfigured Lookup Definitions for User Operations
- Preconfigured Lookup Definitions for Group Operations
- Preconfigured Lookup Definitions for Organizational Unit Operations

5.2.1 Lookup.LDAP.OUD.Configuration

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

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

Table 5-1 Entries in the Lookup.LDAP.OUD.Configuration Lookup Definition

Code Key	Decode	Description
accountObjectClasses	"top","person", "organizationalPerson","inetOrgPerson"	This entry holds the list of object classes required for a USER object.
accountSearchFilter	objectClass=*	This entry holds a search filter that any account needs to match in order to be returned.
accountSynchronizationFilter	objectClass=*	This entry holds a filter for all of the entries returned during the SyncOp operation that must match.
accountUserNameAttribute	cn	This entry holds attributes that contain the name of a USER object.
Any Incremental Recon Attribute Type	true	This entry indicates that any format of token is accepted during reconciliation.
attributesToSynchronize	"cn","uid"	This entry holds the list of attributes to return whenever a SyncOp is run.
blockSize	100	This entry holds the block size for simple paged results and VLV index searches.
Bundle Name	org.identityconnectors.ldap	This entry holds the name of the connector bundle package. Do *not* modify this entry.
Bundle Version	1.0.6380	This entry holds the version of the connector bundle class. Do *not* modify this entry.
changelogBaseDN	cn=changelog	This entry holds the baseDN where the connector is to find the changelog attribute value.
changeLogBlockSize	100	This entry holds the block size for simple paged results and VLV index searches when reading changelog during a SyncOp operation.
changelogUidAttribute	targetEntryUUID	This entry holds the name of the attribute that contains the uniqueId of the modified entry in the changelog.
changeNumberAttribute	changelogcookie	This entry holds the attribute name used for changelog.
Connector Name	org.identityconnectors.ldap.LdapConnector	This entry holds the name of the connector class. Do *not* modify this entry.
disabledRoleName	cn=nsmanageddisabledrole,dc=example,dc=com	This entry holds the name of the role that must be present in the entry when an account is disabled and that the enabledBaseOnRole is set to `TRUE`.
enabledAttribute	ds-pwp-account-disabled	This entry holds the name of the attribute that is required to enable or disable accounts.
enabledValue	FALSE	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is enabled.
disabledValue	true	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is disabled.
enabledWhenNoAttribute	true	This entry defines if the status must be enabled or disabled when the property defined in enabledAttribute is not present in the entry.

Table 5-1 (Cont.) Entries in the Lookup.LDAP.OUD.Configuration Lookup Definition

Code Key	Decode	Description
enabledBasedOnRole	false	This entry specifies whether enabling or disabling a user must be controlled by a role instead of the enabledAttribute attribute. When you set the value of this entry to `true,` it takes precedence over all the other enabled or disabled-related flags.

filterWithOrInsteadOfAnd	false	This entry specifies whether the changelog filter is built using an OR or AND filter.
		Enter `true` if the changelog filter is built using an OR filter instead of AND filter. Otherwise, enter `false.`
		An OR filter is in the following the following format:
		`(|(changeNumber=1) (changeNumber=2) . . . (changeNumber=xxx))`
		An AND filter is of the following format:
		`(&(changeNumber>=0) (changeNumber<=xxx))`

Group Configuration Lookup	Lookup.LDAP.Group.Configuration	This entry holds the name of the lookup definition that contains group-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of groups. Do *not* modify this entry.
groupMemberAttribute	uniqueMember	This entry holds the LDAP attribute that stores the member for non-POSIX static groups.
groupObjectClasses (optional)	"top","groupOfUniqueNames"	This entry holds the list of object classes required for a GROUP object. **Note:** By default, the connector uses groupOfUniqueNames as the object class for groups. If you want to use other object classes for groups, then modify the decode value by replacing "groupOfUniqueNames" with the name of the other object class. For example, if you want to use the groupOfNames object class, then change the decode value to `"top","groupOfNames"`.
ldapGroupFilterBehavior	accept	This entry specifies the behavior for an LDAP group filter.
ldapGroupMembershipAttribute	ismemberof	This entry specifies the value for the LDAP group membership attribute.
maintainLdapGroupMembership	true	This entry specifies whether the connector modifies group membership of renamed or deleted user entries.
maintainPosixGroupMembership	false	This entry specifies whether the connector modifies POSIX group membership of renamed or deleted user entries.
objectClassesToSynchronize	"inetOrgPerson","groupOfNames","groupOfUniqueNames","organizationalUnit"	This entry holds the list of object classes to be synchronized. Any synchronized entry in order to be returned must have at least one object class from this list. If this list of object classes is empty or the code key is missing, then no filtering is performed on the object classes.

Table 5-1 (Cont.) Entries in the Lookup.LDAP.OUD.Configuration Lookup Definition

Code Key	Decode	Description
OU Configuration Lookup	Lookup.LDAP.OU.Configuration	This entry holds the name of the lookup definition that contains organization-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of organizational units. Do *not* modify this entry.
passwordAttribute	userPassword	This entry holds the name of the attribute to which the predefined PASSWORD attribute is written to.
readSchema	true	This entry specifies whether the schema must be read from the server.
removeLogEntryObjectClassFromFilter	true	This entry specifies whether the changelog filter contains a condition on the changelog objectclass.
respectResourcePasswordPolicyChangeAfterReset	true	Enter `TRUE` as the decode value if the connector throws exceptions (for example, PasswordExpiredException) appropriately when binding check for the Password Expired control and Password Policy control. Otherwise, enter `FALSE.`
Role Configuration Lookup	Lookup.LDAP.Role.Configuration	This entry holds the name of the lookup definition that contains role-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of roles. Do *not* modify this entry.
standardChangelog	false	This entry specifies how the connector accesses the changelog attribute: • `true`: The connector retrieves changes using the changelog mechanism described in the draft RFC (`http://tools.ietf.org/html/draft-good-ldap-changelog-04`). • `false`: The connector uses optimized (or non-standard) access based on LDAP control and a cookie. **Note**. Set this entry to `false` only for an OUD target system. For other target systems, this value must be set the `true`.
synchronizeWithModifyTimestamps	false	This property specifies whether the connector must use the modify timestamps attribute instead of the changelog attribute during a SyncOp operation.
uidAttribute	entryUUID	This entry holds the LDAP attribute to which the predefined UID attribute must be mapped to.
usePagedResultControl	true	This entry specifies whether simple paged search is preferred over VLV index search when both are available.
User Configuration Lookup	Lookup.LDAP.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of users. Do *not* modify this entry.
vlvSortAttribute	uid	This entry holds the attribute used as the sort key for the VLV index.

Table 5-1 (Cont.) Entries in the Lookup.LDAP.OUD.Configuration Lookup Definition

Code Key	Decode	Description
readTimeout	120000 milliseconds	This property holds the value for the read timeout configuration property. These values can be increased or decreased if necessary. If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
connectTimeout	120000 milliseconds	This property holds the value for the connect timeout configuration property. These values can be increased or decreased if necessary.If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
referrals	ignore, follow, or throw	This property holds the value for the read referrals configuration property. If this property is not added in the configuration lookup definition, then the value is set to ignore by default.

5.2.2 Lookup.LDAP.OUD.Configuration.Trusted

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

Table 5-2 lists the default entries in this lookup definition.

Table 5-2 Entries in the Lookup.LDAP.OUD.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
accountObjectClasses	"top","person", "organizationalPerson","inetOrgPerson"	This entry holds the list of object classes required for a USER object.
Bundle Name	org.identityconnectors.ldap	This entry holds the name of the connector bundle package. Do *not* modify this entry.
Bundle Version	1.0.6380	This entry holds the version of the connector bundle class. Do *not* modify this entry.
Any Incremental Recon Attribute Type	true	This entry indicates that any format of token is accepted during reconciliation.
changeLogBlockSize	100	This entry holds the block size for simple paged results and VLV index searches when reading changelog during a SyncOp operation.
changeNumberAttribute	changelogcookie	This entry holds the attribute name used for changelog.
Connector Name	org.identityconnectors.ldap.LdapConnector	This entry holds the name of the connector class. Do *not* modify this entry.
disabledValue	true	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is disabled.
enabledAttribute	ds-pwp-account-disabled	This entry holds the name of the attribute that is required to enable or disable accounts.
enabledValue	false	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is enabled.

Table 5-2 (Cont.) Entries in the Lookup.LDAP.OUD.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
enabledWhenNoAttribute	true	This entry defines if the status must be enabled or disabled when the property defined in enabledAttribute is not present in the entry.
objectClassesToSynchronize	"inetOrgPerson","groupOfNames","groupOfUniqueNames","organizationalUnit"	This entry holds the list of object classes to be synchronized. Any synchronized entry in order to be returned must have at least one object class from this list. If this list of object classes is empty or the code key is missing, then no filtering is performed on the object classes.
uidAttribute	entryUUID	This entry holds the LDAP attribute to which the UID must be mapped to.
usePagedResultControl	true	This entry specifies whether simple paged search is preferred over VLV index search when both are available.
User Configuration Lookup	Lookup.LDAP.UM.Configuration.Trusted	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do *not* modify this entry.
readTimeout	120000 milliseconds	This property holds the value for the read timeout configuration property. These values can be increased or decreased if necessary. If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
connectTimeout	120000 milliseconds	This property holds the value for the connect timeout configuration property. These values can be increased or decreased if necessary.If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
referrals	ignore, follow, or throw	This property holds the value for the read referrals configuration property. If this property is not added in the configuration lookup definition, then the value is set to ignore by default.

5.2.3 Preconfigured Lookup Definitions for User Operations

This section discusses the following lookup definitions for user operations:

- Lookup.LDAP.UM.Configuration
- Lookup.LDAP.UM.Configuration.Trusted
- Lookup.LDAP.UM.ProvAttrMap
- Lookup.LDAP.UM.ReconAttrMap
- Lookup.LDAP.UM.ProvValidation
- Lookup.LDAP.UM.ReconTransformation
- Lookup.LDAP.UM.ReconValidation
- Lookup.LDAP.UM.ReconAttrMap.Trusted
- Lookup.LDAP.UM.TrustedDefaults

5.2.3.1 Lookup.LDAP.UM.Configuration

The Lookup.LDAP.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 5-3 lists the default entries in this lookup definition.

Table 5-3 Entries in the Lookup.LDAP.UM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.LDAP.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.LDAP.UM.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.LDAP.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.LDAP.UM.ReconAttrMap for more information about this lookup definition.
Recon Transformation Lookup **Note:** This entry does not exist by default. You must add it if you want to enable transformation during reconciliation.	Lookup.LDAP.UM.ReconTransformation	This entry holds the name of the lookup definition that is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See Configuring Transformation of Data During Reconciliation for more information about adding entries in this lookup definition.
Recon Validation Lookup **Note:** This entry does not exist by default. You must add it if you want to enable validation during reconciliation.	Lookup.LDAP.UM.ReconValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values that are fetched from the target system during reconciliation. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.
Provisioning Validation Lookup **Note:** This entry does not exist by default. You must add it if you want to enable validation during provisioning.	Lookup.LDAP.UM.ProvValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values entered on the process form during provisioning operations. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.

5.2.3.2 Lookup.LDAP.UM.Configuration.Trusted

The Lookup.LDAP.UM.Configuration.Trusted lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during trusted source user reconciliation runs.

Table 5-4 lists the default entry in this lookup definition.

Table 5-4 Entries in the Lookup.LDAP.UM.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
Recon Attribute Defaults	Lookup.LDAP.UM.TrustedDefaults	This entry holds the name of the lookup definition that maps reconciliation fields to their default values. See Lookup.LDAP.UM.TrustedDefaults for more information.
Recon Attribute Map	Lookup.LDAP.UM.ReconAttrMap.Trusted	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.LDAP.UM.ReconAttrMap for more information about this lookup definition.

5.2.3.3 Lookup.LDAP.UM.ProvAttrMap

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

For the default user fields that you can specify or modify values during provisioning operations, see User Fields for Provisioning an OUD Target System.

You can also add entries in this lookup definition if you want to map new target system attributes for provisioning. See Extending the Functionality of the Connector for more information.

5.2.3.4 Lookup.LDAP.UM.ReconAttrMap

The Lookup.LDAP.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is used during reconciliation.

For the default user fields that you can specify or modify values during reconciliation operations, see User Fields for Target Resource Reconciliation.

You can also add entries in this lookup definition if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Connector for more information.

5.2.3.5 Lookup.LDAP.UM.ProvValidation

The Lookup.LDAP.UM.ProvValidation lookup definition is used to configure validation of attribute values entered on the process form during provisioning operations. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.

5.2.3.6 Lookup.LDAP.UM.ReconTransformation

The Lookup.LDAP.UM.ReconTransformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See Configuring Transformation of Data During Reconciliation for more information about adding entries in this lookup definition.

5.2.3.7 Lookup.LDAP.UM.ReconValidation

The Lookup.LDAP.UM.ReconValidation lookup definition is used to configure validation of attribute values that are fetched from the target system during reconciliation. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.

5.2.3.8 Lookup.LDAP.UM.ReconAttrMap.Trusted

The Lookup.LDAP.UM.ReconAttrMap.Trusted lookup definition holds mappings between resource object fields and target system attributes. This lookup definitions is used during trusted source user reconciliation runs. This lookup definition is preconfigured.Table 1-33 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Connector for more information.

5.2.3.9 Lookup.LDAP.UM.TrustedDefaults

The Lookup.LDAP.UM.TrustedDefaults lookup definition holds mappings between reconciliation fields and their default values. This lookup definition is used when there is a mandatory field on the OIM User form, but no corresponding field in the target system from which values can be fetched during trusted source reconciliation.

You can add entries to this lookup definition by ensuring that the Code Key and Decode values are in the following format:

- **Code Key:** Name of the reconciliation field of the resource object
- **Decode:** Corresponding default value to be displayed

For example, the Employee Type field is a mandatory field on the OIM User form. However, on the target system, there is no information about the employee type for a user account. During reconciliation, as the Employee Type field cannot be left empty, you must specify a value for this field. Therefore, the Decode value of the Employee Type Code Key has been set to Full-Time. This implies that the value of the Employee Type field on the OIM User form displays Full-Time for all user accounts reconciled from the target system.

This lookup definition is preconfigured. Table 5-5 lists the default entries.

Table 5-5 Entries in the Lookup.LDAP.UM.TrustedDefaults Lookup Definition

Code Key	Decode
Employee Type	Full-Time
Organization	Xellerate Users
User Type	End-User

5.2.4 Preconfigured Lookup Definitions for Group Operations

This section discussed the following lookup definitions for group operations:

- Lookup.LDAP.Group.Configuration
- Lookup.LDAP.Group.ProvAttrMap

- Lookup.LDAP.Group.ReconAttrMap

5.2.4.1 Lookup.LDAP.Group.Configuration

The Lookup.LDAP.Group.Configuration lookup definition holds configuration entries that are specific to the group object type. This lookup definition is used during group management operations when your target system is configured as a target resource.

Table 5-6 lists the default entries in this lookup definition.

Table 5-6 Entries in the Lookup.LDAP.Group.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.LDAP.Group.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.LDAP.Group.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.LDAP.Group.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.LDAP.Group.ReconAttrMap for more information about this lookup definition.

5.2.4.2 Lookup.LDAP.Group.ProvAttrMap

The Lookup.LDAP.Group.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during group provisioning operations.

This lookup definition is preconfigured. Table 1-25 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Adding Custom Fields for Provisioning for more information.

5.2.4.3 Lookup.LDAP.Group.ReconAttrMap

The Lookup.LDAP.Group.ReconAttrMap lookup definition holds mappings between resource object fields for groups and target system attributes. This lookup definition is used during reconciliation.

This lookup definition is preconfigured. Table 1-8 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Adding Custom Fields for Target Resource Reconciliation for more information.

5.2.5 Preconfigured Lookup Definitions for Organizational Unit Operations

This section discusses the following lookup definitions for organizational unit operations:

- Lookup.LDAP.OU.Configuration

- Lookup.LDAP.OU.ProvAttrMap
- Lookup.LDAP.OU.ReconAttrMap

5.2.5.1 Lookup.LDAP.OU.Configuration

The Lookup.LDAP.OU.Configuration lookup definition holds configuration entries that are specific to the organizational unit object type. This lookup definition is used during organizational unit management operations when your target system is configured as a target resource.

Table 5-7 lists the default entry in this lookup definition.

Table 5-7 Entries in the Lookup.LDAP.OU.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.LDAP.OU.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.LDAP.OU.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.LDAP.OU.ReconAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.LDAP.OU.ReconAttrMap for more information about this lookup definition.

5.2.5.2 Lookup.LDAP.OU.ProvAttrMap

The Lookup.LDAP.OU.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during provisioning.

This lookup definition is preconfigured. Table 1-30 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Extending the Functionality of the Connector for more information.

5.2.5.3 Lookup.LDAP.OU.ReconAttrMap

The Lookup.LDAP.OU.ReconAttrMap lookup definition maps process form fields and target system attributes. This lookup definition is used during reconciliation.

This lookup definition is preconfigured. Table 1-13 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Extending the Functionality of the Connector for more information.

5.3 Reconciling OUD Users Under Their Corresponding Organizations in Oracle Identity Manager

> **Note:**
>
> Before you perform the following optional task, make sure you have created the corresponding organizations with the same names from the target system in Oracle Identity Manager.

To reconcile users from an OUD target system under their corresponding organizations in Oracle Identity Manager:

1. Log in to Oracle Identity Manager Design Console.
2. Find the **Lookup.LDAP.UM.ReconAttrMap.Trusted** lookup.
3. Add the following entry:
   - **code**: Organization
   - **decode**: __PARENTRDNVALUE__

5.4 Reconciling OUD Groups Under One Organization in Oracle Identity Manager

To configure OUD groups to be reconciled under one organization:

1. Log in to Oracle Identity Manager Design Console.
2. Find the **Lookup.LDAP.Group.Configuration** lookup.
3. Add a new entry such as the following:
   - **code**: Recon Attribute Defaults
   - **decode**: Lookup.LDAP.Group.Defaults

   Note that the decode value is an example, and you can set your own lookup name.
4. Create the new **Lookup.LDAP.Group.Defaults** lookup (specified in the previous step).
5. Add a new entry:
   - **code**: Org Name
   - **decode**: Group1

   The decode value is the name of the Oracle Identity Manager organization under which all groups will be reconciled.
6. Find the **Lookup.LDAP.Group.ReconAttrMap** lookup.
7. Delete the row with the code **Org Name**.
8. Find the reconciliation rule **LDAP Group Recon**.

9. Change the current rule **Organization Name Equals Group Name** to **Organization Name Equals Org Name** by double clicking the rule element and changing the **Group Name** attribute to **Org Name**.
10. Save the rule.
11. Open the **LDAP Group** resource object and click **Create Reconciliation Profile**.

5.5 Reconciling Newly Created Objects for an OUD Target System

An OUD target system has a specific behavior with respect to the modifyTimestamp attribute. When a new object such as a user, OU, or group is created on the OUD target, only createTimestamp is updated and not modifyTimestamp.

Consequently, when you run a search reconciliation with modifyTimestamp in Incremental Recon Attribute, the reconciliation events are not created for new objects. In this case, you must run reconciliation with createTimestamp in Incremental Recon Attribute.

Create a new scheduled job to reconcile newly created objects separately, as follows:

1. Go to **Advanced** / **Search Scheduled Jobs**.
2. Create new scheduled job.
3. Set the job name depending on the object type you want to reconcile (User, OU, or Group). For example, "OUD New Users Search Reconciliation".
4. Set the **Task** to **LDAP Connector Search Incremental Reconciliation**.
5. Set the **Retries** and **Schedule Type** as required by your deployment.
6. Set the **Incremental Recon Attribute** to **createTimestamp**.
7. Set the **IT Resource** Name to the IT resource name you are using.
8. Set **Object Type** to User, OU or Group, depending on the object type you want to reconcile.
9. Set **Resource Object Name** to **LDAP User**, **LDAP Organisation Unit**, or **LDAP Group**, depending on the object type you want to reconcile.
10. Set the **Scheduled Task Name** to the same value you specified in Step 3.
11. Click **Apply** to save the job.

5.6 Guidelines on Using the Connector for Dynamic and Virtual Static Groups

This connector does not support dynamic and virtual static groups in LDAP, by default. If you want to use the connector for dynamic or virtual static groups, then you must apply the following guidelines:

- Ensure referential integrity in OUD is enabled.
- Set the value of the maintainLdapGroupMembership entry in the Lookup.LDAP.OUD.Configuration lookup definition to `false`.

6

Using the Connector with Oracle Internet Directory

This chapter describes the following information about using the connector with Oracle Internet Directory (OID):

- Configuring Secure Communication
- Preconfigured Lookup Definitions for an OID Target System
- Reconciling OID Users Under Their Corresponding Organizations in Oracle Identity Manager
- Reconciling OID Groups Under One Organization in Oracle Identity Manager

6.1 Configuring Secure Communication

To provide secure communications to the OID target system, configure SSL between Oracle Identity Manager, the Connector Server, and the OID target system.

For more information, see Configuring SSL for the Connector.

6.2 Preconfigured Lookup Definitions for an OID Target System

This section discusses the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector for the OID target system. 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.OID.Configuration
- Lookup.OID.Configuration.Trusted
- Preconfigured Lookup Definitions for User Operations
- Preconfigured Lookup Definitions for Group Operations
- Preconfigured Lookup Definitions for Organizational Unit Operations

> **Note:**
>
> Roles are not supported for an OID target system.

6.2.1 Lookup.OID.Configuration

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

Table 6-1 lists the default entries in this lookup definition.

Table 6-1 Entries in the Lookup.OID.Configuration Lookup Definition

Code Key	Decode	Description
accountObjectClasses	"top","person","organizationalPerson","inetOrgPerson","orclUserV2"	This entry holds the list of object classes required for a USER object.
accountSearchFilter	objectClass=*	This entry holds a search filter that any account needs to match in order to be returned.
accountSynchronizationFilter	objectClass=*	This entry holds a filter for all of the entries returned during the SyncOp operation that must match.
accountUserNameAttribute	cn	This entry holds attributes that contain the name of a USER object.
attributesToSynchronize	"cn","uid"	This entry holds the list of attributes to return whenever a SyncOp is run.
blockSize	100	This entry holds the block size for simple paged results and VLV index searches.
Bundle Name	org.identityconnectors.ldap	This entry holds the name of the connector bundle package. Do *not* modify this entry.
Bundle Version	1.0.6380	This entry holds the version of the connector bundle class. Do *not* modify this entry.
changelogBaseDN	cn=changelog	This entry holds the baseDN where the connector is to find the changelog attribute value.
changeLogBlockSize	100	This entry holds the block size for simple paged results and VLV index searches when reading changelog during a SyncOp operation.
changelogUidAttribute	orclguid	This entry holds the name of the attribute that contains the uniqueId of the modified entry in the changelog.
changeNumberAttribute	changeNumber	This entry holds the attribute name used for changelog.
Connector Name	org.identityconnectors.ldap.LdapConnector	This entry holds the name of the connector class. Do *not* modify this entry.
disabledValue	DISABLED	This entry specifies the value to be used for the attribute defined by the enabledAttribute entry whenever an account is disabled.
enabledAttribute	orclIsEnabled	This entry holds the name of the attribute that is required to enable or disable accounts.
enabledWhenNoAttribute	true	This entry defines if the status must be enabled or disabled when the property defined in enabledAttribute is not present in the entry.
enabledValue	ENABLED	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is enabled.

Table 6-1 (Cont.) Entries in the Lookup.OID.Configuration Lookup Definition

Code Key	Decode	Description

filterWithOrInsteadOfAnd	false	This entry specifies whether the changelog filter is built using an OR or AND filter.
		Enter `true` if the changelog filter is built using an OR filter instead of AND filter. Otherwise, enter `false.`
		An OR filter is in the following the following format:
		`(|(changeNumber=1) (changeNumber=2) . . . (changeNumber=xxx))`
		An AND filter is of the following format:
		`(&(changeNumber>=0) (changeNumber<=xxx))`

Group Configuration Lookup	Lookup.OID.Group.Configuration	This entry holds the name of the lookup definition that contains group-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of groups. Do *not* modify this entry.
groupMemberAttribute	uniqueMember	This entry holds the LDAP attribute that stores the member for non-POSIX static groups.
ldapGroupFilterBehavior	reject	This entry specifies the behavior for an LDAP group filter.
ldapGroupMembershipAttribute	ismemberof	This entry specifies the value for the LDAP group membership attribute.
maintainLdapGroupMembership	true	This entry specifies whether the connector modifies group membership of renamed or deleted user entries.
maintainPosixGroupMembership	false	This entry specifies whether the connector modifies POSIX group membership of renamed or deleted user entries.
objectClassesToSynchronize	"inetOrgPerson","groupOfNames","groupOfUniqueNames","organizationalUnit"	This entry holds the list of object classes to be synchronized. Any synchronized entry in order to be returned must have at least one object class from this list. If this list of object classes is empty or the code key is missing, then no filtering is performed on the object classes.
OU Configuration Lookup	Lookup.OID.OU.Configuration	This entry holds the name of the lookup definition that contains organization-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of organizational units. Do *not* modify this entry.
passwordAttribute	userPassword	This entry holds the name of the attribute to which the predefined PASSWORD attribute is written to.

Table 6-1   (Cont.) Entries in the Lookup.OID.Configuration Lookup Definition

Code Key	Decode	Description
readSchema	true	This entry specifies whether the schema must be read from the server.
removeLogEntryObjectClassFromFilter	true	This entry specifies whether the changelog filter contains a condition on the changelog objectclass.
respectResourcePasswordPolicyChangeAfterReset	true	Enter `TRUE` as the decode value if the connector throws exceptions (for example, PasswordExpiredException) appropriately when binding check for the Password Expired control and Password Policy control. Otherwise, enter `FALSE.`
standardChangelog	true	This entry specifies how the connector accesses the changelog attribute.
synchronizeWithModifyTimestamps	false	This property specifies whether the connector must use the modify timestamps attribute instead of the changelog attribute during a SyncOp operation.
uidAttribute	orclguid	This entry holds the LDAP attribute to which the predefined UID attribute must be mapped to.
usePagedResultControl	true	This entry specifies whether simple paged search is preferred over VLV index search when both are available.
User Configuration Lookup	Lookup.OID.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of users. Do *not* modify this entry.
vlvSortAttribute	uid	This entry holds the attribute used as the sort key for the VLV index.
readTimeout	120000 milliseconds	This property holds the value for the read timeout configuration property. These values can be increased or decreased if necessary. If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
connectTimeout	120000 milliseconds	This property holds the value for the connect timeout configuration property. These values can be increased or decreased if necessary.If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
referrals	ignore, follow, or throw	This property holds the value for the read referrals configuration property. If this property is not added in the configuration lookup definition, then the value is set to ignore by default.

6.2.2 Lookup.OID.Configuration.Trusted

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

Table 6-2 lists the default entries in this lookup definition.

Table 6-2 Entries in the Lookup.OID.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
accountObjectClasses	"top","person","organizationalPerson","inetOrgPerson","orclUserV2"	This entry holds the name of the account object classes.
Any Incremental Recon Attribute Type	true	This entry indicates that any format of token is accepted during reconciliation.
Bundle Name	org.identityconnectors.ldap	This entry holds the name of the connector bundle package. Do *not* modify this entry.
Bundle Version	1.0.6380	This entry holds the version of the connector bundle class. Do *not* modify this entry.
changeLogBlockSize	100	This entry holds the block size for simple paged results and VLV index searches when reading changelog during a SyncOp operation.
changeNumberAttribute	changeNumber	This entry holds the attribute name used for changelog.
Connector Name	org.identityconnectors.ldap.LdapConnector	This entry holds the name of the connector class. Do *not* modify this entry.
disabledValue	DISABLED	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is disabled.
enabledAttribute	orclIsEnabled	This entry holds the name of the attribute that is required to enable or disable accounts.
enabledValue	ENABLED	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is enabled.
enabledWhenNoAttrbribute	true	This entry defines if the status must be enabled or disabled when the property defined in enabledAttribute is not present in the entry.
objectClassesToSynchronize	"inetOrgPerson","groupOfNames","groupOfUniqueNames", "OrganizationalUnit"	This entry holds the list of object classes to be synchronized. Any synchronized entry in order to be returned must have at least one object class from this list. If this list of object classes is empty or the code key is missing, then no filtering is performed on the object classes.
uidAttribute	orclguid	This entry holds the LDAP attribute to which the Uid must be mapped to.
UsePagedResultControl	true	This entry specifies whether simple paged search is preferred over VLV index search when both are available.

Table 6-2 (Cont.) Entries in the Lookup.OID.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
User Configuration Lookup	Lookup.OID.UM.Configuration.Trusted	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do *not* modify this entry.
readTimeout	120000 milliseconds	This property holds the value for the read timeout configuration property. These values can be increased or decreased if necessary. If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
connectTimeout	120000 milliseconds	This property holds the value for the connect timeout configuration property. These values can be increased or decreased if necessary.If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
referrals	ignore, follow, or throw	This property holds the value for the read referrals configuration property. If this property is not added in the configuration lookup definition, then the value is set to ignore by default.

6.2.3 Preconfigured Lookup Definitions for User Operations

This section describes the following lookup definitions for user operations:

- Lookup.OID.UM.Configuration
- Lookup.OID.UM.Configuration.Trusted
- Lookup.OID.UM.ProvAttrMap
- Lookup.OID.UM.ReconAttrMap
- Lookup.OID.UM.ReconAttrMap.Trusted
- Lookup.OID.UM.TrustedDefaults

6.2.3.1 Lookup.OID.UM.Configuration

The Lookup.OID.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 6-3 lists the default entries in this lookup definition.

Table 6-3 Entries in the Lookup.OID.UM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.OID.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes.

Table 6-3 (Cont.) Entries in the Lookup.OID.UM.Configuration Lookup Definition

Code Key	Decode	Description
Recon Attribute Map	Lookup.OID.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes.

6.2.3.2 Lookup.OID.UM.Configuration.Trusted

The Lookup.OID.UM.Configuration.Trusted lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during trusted source user reconciliation runs.

Table 6-4 lists the default entries in this lookup definition.

Table 6-4 Entries in the Lookup.OID.UM.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
Recon Attribute Defaults	Lookup.OID.UM.TrustedDefaults	This entry holds the name of the lookup definition that maps reconciliation fields to their default values.
Recon Attribute Map	Lookup.OID.UM.ReconAttrMap.Trusted	This entry holds the name of the lookup definition that maps resource object fields and target system attributes.

6.2.3.3 Lookup.OID.UM.ProvAttrMap

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

Table 6-5 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 6-5 Entries in the Lookup.OID.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Common Name	cn
Container DN[IGNORE,LOOKUP]	ContainerDN
Department	departmentnumber
Email ID	mail
EndDate	orclActiveEndDate=End_Date!=null&&!End_Date.startsWith("1969-12-31")?Date.parse('yyyy-MM-dd', End_Date).format('yyyyMMddHHmmss') + 'Z':null
End Date[IGNORE]	enddate
First Name	givenname
Last Name	sn
Location	l
Login Disabled	__ENABLED__

Table 6-5 (Cont.) Entries in the Lookup.OID.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
manager	manager
Middle Name	initials
Name	__NAME__="uid=${User_ID},${Container_DN}"
orclGuid	__UID__
Password	__PASSWORD__
Preferred Language	preferredlanguage
StartDate	orclActiveStartDate=Start_Date!=null&&! Start_Date.startsWith("1969-12-31")?Date.parse('yyyy-MM-dd', Start_Date).format('yyyyMMddHHmmss') + 'Z':null
Start Date[IGNORE]	startdate
Telephone	telephonenumber
Time Zone	orclTimeZone
Title	title
UD_OID_GRP	ldapGroups
User ID	uid

6.2.3.4 Lookup.OID.UM.ReconAttrMap

The Lookup.OID.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 6-6 lists the default entries in this lookup definition.

Table 6-6 Entries in the Lookup.OID.UM.ReconAttrMap Lookup Definition

Code Key	Decode
Common Name	cn
Container DN[LOOKUP]	__parentDN__
Department	departmentnumber
Email	mail
End Date[Date]	orclActiveEndDate=binding.variables.containsKey("orclActiveEndDate")&&orclActiveEndDate!=null? Date.parse('yyyyMMddHHmmss',orclActiveEndDate).getTime():null
First Name	givenname
Last Name	sn

Table 6-6 (Cont.) Entries in the Lookup.OID.UM.ReconAttrMap Lookup Definition

Code Key	Decode
Location	l
manager	manager
Middle Name	initials
orclGuid	__UID__
Preferred Language	preferredlanguage
Start Date[Date]	orclActiveStartDate=binding.variables.containsKey("orclActiveStartDate")&&orclActiveStartDate!=null? Date.parse('yyyyMMddHHmmss',orclActiveStartDate).getTime():null
Status	__ENABLE__
Telephone	telephonenumber
TimeZone	orclTimeZone
Title	title
UserGroup~GroupName[LOOKUP]	ldapGroups
User ID	uid

6.2.3.5 Lookup.OID.UM.ReconAttrMap.Trusted

The Lookup.OID.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.

Table 6-7 lists the default entries in this lookup definition.

Table 6-7 Entries in the Lookup.OID.UM.ReconAttrMap.Trusted Lookup Definition

OIM User Form Field	Target System Field
Email	mail
First Name	givenname
Last Name	sn
Manager	manager=matcher=java.util.regex.Pattern.compile("uid=(\\w*).*").matcher(manager==null?"":manager);matcher.matches()?matcher[0][1]:null
Middle Name	initials
OrclGuid	__UID__
Status[TRUSTED]	__ENABLE__
User Login	uid

6.2.3.6 Lookup.OID.UM.TrustedDefaults

The Lookup.OID.UM.TrustedDefaults lookup definition holds mappings between reconciliation fields and their default values. This lookup definition is used when thereis a mandatory field on the OIM User form, but no corresponding field in the target system from which values can be fetched during trusted source reconciliation.

You can add entries to this lookup definition by ensuring that the Code Key and Decode values are in the following format:

- **Code Key**: Name of the reconciliation field of the resource object
- **Decode**: Corresponding default value to be displayed

Table 6-8 lists the default entries in this lookup definition.

Table 6-8 Entries in the Lookup.OID.UM.TrustedDefaults Lookup Definition

Key Code	Decode
Employee Type	Full-Time
Organization	Xellerate Users
User Type	End-User

6.2.4 Preconfigured Lookup Definitions for Group Operations

This section describes the following lookup definitions for group operations:

- Lookup.OID.Group.Configuration
- Lookup.OID.Group.ProvAttrMap
- Lookup.OID.Group.ReconAttrMap

6.2.4.1 Lookup.OID.Group.Configuration

The Lookup.OID.Group.Configuration lookup definition holds configuration entries that are specific to the group object type. This lookup definition is used during group management operations when your target system is configured as a target resource.

Table 6-9 lists the default entries in this lookup definition.

Table 6-9 Entries in the Lookup.OID.Group.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.OID.Group.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes.
Recon Attribute Map	Lookup.OID.Group.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes.

6.2.4.2 Lookup.OID.Group.ProvAttrMap

The Lookup.OID.Group.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during group provisioning operations. This lookup definition is preconfigured.

Table 6-10 lists the default entries. You can add entries in this lookup definitions if you want to map new target system attributes for provisioning.

Table 6-10 Entries in the Lookup.OID.Group.ProvAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Target System Field
Container DN[IGNORE,LOOKUP]	container
Group Name	cn
Name	__NAME__="cn=${Group_Name},${Container_DN}"
OrclGuid	__UID__

6.2.4.3 Lookup.OID.Group.ReconAttrMap

The Lookup.OID.Group.ReconAttrMap lookup definition holds mappings between resource object fields for groups and target system attributes. This lookup definition isused during reconciliation. This lookup definition is preconfigured.

Table 6-11 lists the default entries. You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation.

Table 6-11 Entries in the Lookup.OID.Group.ReconAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Target System Field
Container DN[LOOKUP]	__parentDN__
Group Name	cn
OrclGuid	__UID__
Org Name	__PARENTRDNVALUE__

6.2.5 Preconfigured Lookup Definitions for Organizational Unit Operations

This section describes the following lookup definitions for organizational unit operations:

- Lookup.OID.OU.Configuration
- Lookup.OID.OU.ProvAttrMap
- Lookup.OID.OU.ReconAttrMap

6.2.5.1 Lookup.OID.OU.Configuration

The Lookup.OID.OU.Configuration lookup definition holds configuration entries that are specific to the organizational unit object type. This lookup definition is used during organizational unit management operations when your target system is configured as a target resource.

Table 6-12 lists the default entries in this lookup definition.

Table 6-12 Entries in the Lookup.OID.OU.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.OID.OU.ProvAttrMap	Lookup used during provisioning.
Recon Attribute Map	Lookup.OID.OU.ReconAttrMap	Lookup used during reconciliation.

6.2.5.2 Lookup.OID.OU.ProvAttrMap

The Lookup.OID.OU.ProvAttrMap lookup definition maps process form fields for organizations and target system attributes. This lookup definition is used for performing organizational unit provisioning operations.

Table 6-13 lists the organizational unit fields of the target system for which you can specify or modify values during provisioning operations.

Table 6-13 Entries in the Lookup.OID.OU.ProvAttrMap Lookup Definition

Organization Field on Oracle Identity Manager	Target System Field
Container DN[IGNORE,LOOKUP]	Not used.
Name	__NAME__="ou=${Organisation_Unit_Name},${Container_DN}"
OrclGuid	__UID__
Organisation Unit Name	ou

6.2.5.3 Lookup.OID.OU.ReconAttrMap

This lookup definition is used during reconciliation. Table 6-14 lists the entries in this lookup definition.

Table 6-14 Entries in the Lookup.OID.OU.ReconAttrMap Lookup Definition

Code Key	Decode
Container DN[LOOKUP]	__parentDN__
OrclGuid	__UID__
Organization Unit Name	ou
Org Name	__PARENTRDNVALUE__

6.3 Reconciling OID Users Under Their Corresponding Organizations in Oracle Identity Manager

> **Note:**
>
> Before you perform the following optional task, make sure you have created the corresponding organizations with the same names from the target system in Oracle Identity Manager.

To reconcile users from an OID target system under their corresponding organizations in Oracle Identity Manager:

1. Log in to Oracle Identity Manager Design Console.
2. Find the **Lookup.OID.UM.ReconAttrMap.Trusted** lookup.
3. Add the following entry:
   - **code**: Organization
   - **decode**: __PARENTRDNVALUE__

6.4 Reconciling OID Groups Under One Organization in Oracle Identity Manager

To configure an OID group to be reconciled under one organization:

1. Log in to Oracle Identity Manager Design Console.
2. Find the **Lookup.OID.Group.Configuration** lookup.
3. Add a new entry such as the following:
   - **code**: Recon Attribute Defaults
   - **decode**: Lookup.OID.Group.Defaults

   Note that the decode value is an example, and you can set your own lookup name.
4. Create the new **Lookup.OID.Group.Defaults** lookup (specified in the previous step).
5. Add a new entry:
   - **code**: Org Name
   - **decode**: Group1

   The decode value is the name of the Oracle Identity Manager organization under which all groups will be reconciled.
6. Find **Lookup.OID.Group.ReconAttrMap**.
7. Delete the row with code **Org Name**.
8. Find the reconciliation rule **OID Group Recon.**

9. Change the current rule **Organization Name Equals Group Name** to **Organization Name Equals Org Name** by double clicking the rule element and changing attribute **Group Name** to **Org Name**

10. Save the rule.

11. Open the **OID Group** resource object and click **Create Reconciliation Profile**.

7

Using the Connector with Novell eDirectory

The chapter describes the following information about using the connector with Novell eDirectory:

- Configuring Secure Communications
- Provisioning an eDirectory Target System
- Performing Reconciliation for an eDirectory Target System
- Preconfigured Lookup Definitions for an eDirectory Target System

7.1 Configuring Secure Communications

To provide secure communications to the eDirectory target system, configure SSL between Oracle Identity Manager, the Connector Server, and the eDirectory target system.

For more information, see Configuring SSL for the Connector

7.2 Provisioning an eDirectory Target System

This section describes the following information about provisioning an eDirectory target system:

- User Fields for Provisioning an eDirectory Target System
- Group Fields for Provisioning an eDirectory Target System
- Role Fields for Provisioning an eDirectory Target System
- Organizational Unit (OU) Fields for Provisioning an eDirectory Target System

7.2.1 User Fields for Provisioning an eDirectory Target System

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

Table 7-1 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 7-1 Entries in the Lookup.EDIR.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Password	__PASSWORD__
UD_EDIR_ROL~Role Name[LOOKUP]	rbsAssignedRoles~rbsRole~__NAME__
UD_EDIR_ROL~Inheritable	rbsAssignedRoles~rbsRole~inheritable
Logon Script	loginScript

Table 7-1 (Cont.) Entries in the Lookup.EDIR.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Timezone	timezone
Title	title
Department	departmentNumber
UD_EDIR_ROL~Scope[LOOKUP]	rbsAssignedRoles~rbsRole~domainScope
First Name	givenName
Communication Language	preferredLanguage
Profile[LOOKUP] profile	profile
Last Name	sn
Guid	__NAME__="cn=${User_ID},${Container_DN}"
User ID	cn
Container DN[IGNORE,LOOKUP]	ContainerDN
Email	mail
Location	l
Telephone	telephoneNumber
Reference ID	__UID__
UD_EDIR_GRP~Group Name[LOOKUP]	ldapGroups
Middle Name	initials

7.2.2 Group Fields for Provisioning an eDirectory Target System

The Lookup.EDIR.Group.ProvAttrMap lookup definition maps process form fields with eDirectory attributes. This lookup definition is used for performing group provisioning operations.

Table 7-2 lists the group identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 7-2 Entries in the Lookup.EDIR.Group.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Reference ID	__UID__
Container DN[IGNORE,LOOKUP]	ContainerDN
Group Name	cn
Guid	__NAME__="cn=${Group_Name},${Container_DN}"

7.2.3 Role Fields for Provisioning an eDirectory Target System

The Lookup.EDIR.Role.ProvAttrMap lookup definition maps process form fields with eDirectory attributes. This lookup definition is used for performing role provisioning operations.

Note:

The scope attribute in the Role child form is pre-populated from the Lookup.EDIR.DefaultScope lookup definition. You must enter a default value manually in this lookup before you perform a provisioning or reconciliation operation. Only one value is required.

Table 7-3 lists the role identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 7-3 Entries in the Lookup.EDIR.Role.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Role Container[IGNORE,LOOKUP]	ContainerDN
Reference ID	__UID__
Guid	__NAME__="cn=${Role_Name},${Role_Container}"
Role Name	cn

7.2.4 Organizational Unit (OU) Fields for Provisioning an eDirectory Target System

The Lookup.EDIR.OU.ProvAttrMap lookup definition maps process form fields with eDirectory attributes. This lookup definition is used for performing organizational unit provisioning operations.

Table 7-4 lists the organizational unit fields of the target system for which you can specify or modify values during provisioning operations.

Table 7-4 Entries in the Lookup.EDIR.OU.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
Organisation Name	ou
Reference ID	__UID__
Guid	__NAME__="ou=${Organisation_Name},${Container_DN}"
Container DN[LOOKUP,IGNORE]	ContainerDN

7.3 Performing Reconciliation for an eDirectory Target System

This section describes the following information about reconciliation:

- Trusted Reconciliation Fields for an eDirectory Target System
- Reconciliation Rules for Target Resource Reconciliation
- Reconciling eDirectory Users Under Their Corresponding Organizations in Oracle Identity Manager

- Reconciling eDirectory Groups and Roles Under One Organization in Oracle Identity Manager

7.3.1 Trusted Reconciliation Fields for an eDirectory Target System

The Lookup.EDIR.UM.ReconAttrMap.Trusted lookup definition maps Oracle Identity Manager fields with eDirectory fields. This lookup definition is used for performing trusted reconciliation operations.

Table 7-4 lists the corresponding fields in the Lookup.EDIR.UM.ReconAttrMap.Trusted lookup definition.

Table 7-5 Entries in the Lookup.EDIR.UM.ReconAttrMap.Trusted Lookup Definition

OIM Field	Target System Field
Fax	facsimileTelephoneNumber
Pager	pager
Status[TRUSTED]	__ENABLE__
First Name	givenName
Title	title
location	l
Email	mail
Street	street
Telephone	telephoneNumber
Department Number	departmentNumber
Postal Address	postalAddress
entryDN[IGNORE]	entryDN
User ID	cn from entryDN
Postal Code	postalCode
parentDN[IGNORE]	__PARENTDN__
Last Name	sn

7.3.2 Reconciliation Rules for Target Resource Reconciliation

This section contains the following topics:

- About Rules for Target Resource Reconciliation
- Viewing the Reconciliation Rule for Target Resource Reconciliation

7.3.2.1 About Rules for Target Resource Reconciliation

The following is the process matching rule:

Rule name: eDirectory User Trusted

Rule element: (GUID Equals guid) OR (User Login Equals User ID)

In the first rule component:

- GUID on the left of Equals is the unique ID of the user.
- guid on the right of Equals is the user ID field of the user on the target system.

In the second rule component:

- User Login is the User Login field on the OIM User form.
- User ID is the user ID field of the target system.

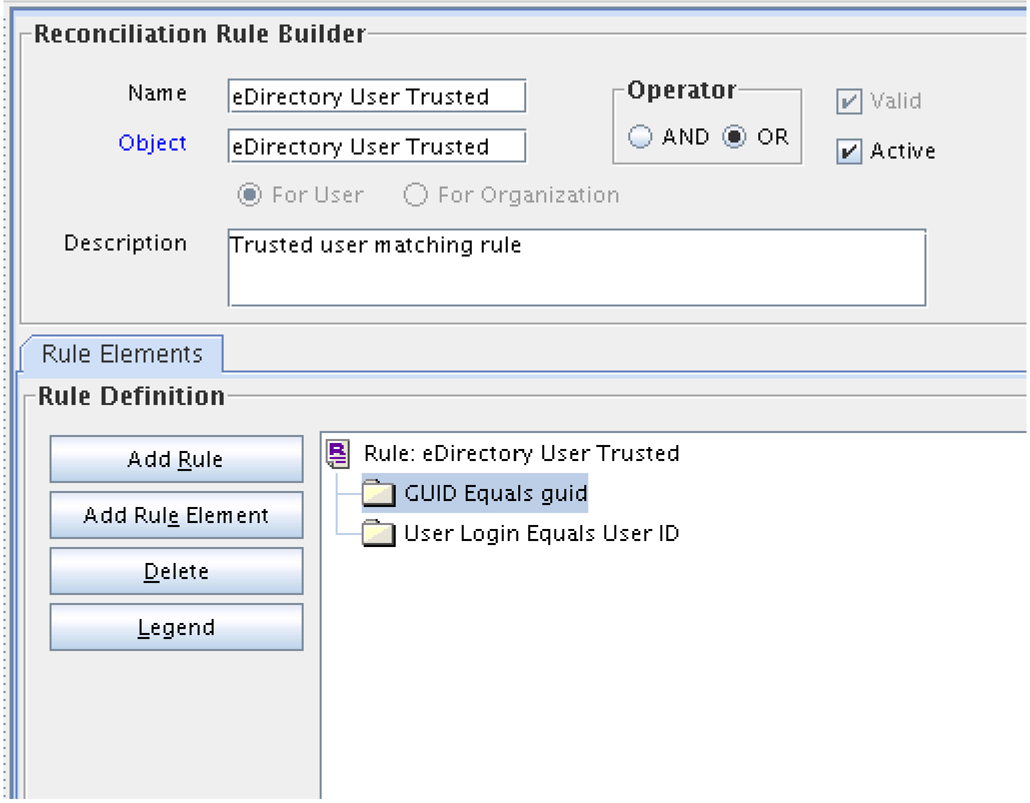
7.3.2.2 Viewing the Reconciliation Rule for Target Resource Reconciliation

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

1. Log in to Oracle Identity Manager Design Console.
2. Expand Development Tools.
3. Double-click Reconciliation Rules.
4. Search for eDirectory User Trusted. Figure 7-1 shows the reconciliation rule for Target Resource Reconciliation.

   Note. The Reconciliation Action Rule is the same as this rule.

Figure 7-1 Reconciliation Rule Builder Screen for Target Resource Reconciliation



Reconciliation Rule Builder

Name: eDirectory User Trusted
Object: eDirectory User Trusted
Operator: ○ AND ● OR
☑ Valid
☑ Active
● For User ○ For Organization
Description: Trusted user matching rule

Rule Elements

Rule Definition

Rule: eDirectory User Trusted
- GUID Equals guid
- User Login Equals User ID

7.3.3 Reconciling eDirectory Users Under Their Corresponding Organizations in Oracle Identity Manager

> **Note:**
>
> Before you perform the following optional task, make sure you have created the corresponding organizations with the same names from the target system in Oracle Identity Manager.

To reconcile users from an eDirectory target system under their corresponding organizations in Oracle Identity Manager:

1. Log in to Oracle Identity Manager Design Console.
2. Find the **Lookup.EDIR.UM.ReconAttrMap.Trusted** lookup.
3. Add the following entry:
   - code: Organization
   - decode: __PARENTRDNVALUE__

7.3.4 Reconciling eDirectory Groups and Roles Under One Organization in Oracle Identity Manager

This section describes the following optional procedures:

- Reconciling eDirectory Groups Under One Organization
- Reconciling eDirectory Roles Under One Organization

7.3.4.1 Reconciling eDirectory Groups Under One Organization

To configure eDirectory groups to be reconciled under one organization:

1. Log in to Oracle Identity Manager Design Console.
2. Find the **Lookup.EDIR.Group.Configuration** lookup.
3. Add a new entry such as the following:
   - code: Recon Attribute Defaults
   - decode: Lookup.EDIR.Group.Defaults

   Note. The decode value is an example, and you can set your own lookup name.
4. Create the new Lookup.EDIR.Group.Defaults lookup (specified in the previous step).
5. Add a new entry:
   - code: Org Name
   - decode: Group1

The decode value is the name of the Oracle Identity Manager organization under which all groups will be reconciled.

6. Find the **Lookup.EDIR.Group.ReconAttrMap** lookup.
7. Delete the row with code Org Name.
8. Find the rule eDirectory Group Recon.
9. Change the current rule Organization Name Equals Group Name to Organization Name Equals Org Name by double clicking the rule element and changing attribute Group Name to Org Name.
10. Save the rule.
11. Open the eDirectory Group resource object and click **Create Reconciliation Profile**.

7.3.4.2 Reconciling eDirectory Roles Under One Organization

To configure eDirectory roles to be reconciled under one organization:

1. Log in to Oracle Identity Manager Design Console.
2. Find the **Lookup.EDIR.Role.Configuration** lookup.
3. Add a new entry such as the following:
   - code: Recon Attribute Defaults
   - decode: Lookup.EDIR.Role.Defaults

   Note. The decode value is an example, and you can set your own lookup name.
4. Create the new Lookup.EDIR.Role.Defaults lookup (specified in the previous step).
5. Add a new entry:
   - code: Org Name
   - decode: Role1

   The decode value is the name of the Oracle Identity Manager organization under which all roles will be reconciled.
6. Find **Lookup.EDIR.Role.ReconAttrMap**.
7. Delete the row with code Org Name.
8. Find the rule eDirectory Role Recon.
9. Change the current rule Organization Name Equals Role Name to Organization Name Equals Role Name by double clicking the rule element and changing attribute Role Name to Org Name.
10. Save the rule.
11. Open the eDirectory Role resource object and click Create Reconciliation Profile.

7.4 Preconfigured Lookup Definitions for an eDirectory Target System

This section describes the following preconfigured lookup definitions for an eDirectory target system:

- Lookup.EDIR.Configuration

- Lookup.EDIR.CommLang
- Preconfigured Lookup Definitions for User Operations
- Preconfigured Lookup Definitions for Group Operations
- Preconfigured Lookup Definitions for Role Operations
- Preconfigured Lookup Definitions for Organizational Unit Operations
- Preconfigured Lookup Definitions for Trusted Configuration Operations

7.4.1 Lookup.EDIR.Configuration

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

Table 7-6 lists the default entries in this lookup definition.

Table 7-6 Entries in the Lookup.EDIR.Configuration Lookup Definition

Code	Decode	Description
OU Configuration Lookup	Lookup.EDIR.OU.Configuration	This entry holds the name of the lookup definition that contains organization-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of organizational units. Do not modify this entry
Connector Name	org.identityconnectors.ldap.LdapConnector	This entry holds the name of the connector class. Do not modify this entry.
User Configuration Lookup	Lookup.EDIR.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of users. Do not modify this entry.
uidInBinary	TRUE	This attribute symbolizes that the UID field type is binary. Binary values are stored in hexadecimal format in OIM.
Bundle Name	org.identityconnectors.ldap	This entry holds the name of the connector bundle package. Do not modify this entry.
enabledAttribute	loginDisabled	This entry holds the name of the attribute that is required to enable or disable accounts.
activateMembershipAttributesAtUser	TRUE	Activates group membership attribute at user entry. For every group membership, user entry is modified with group membership attribute.
accountObjectClasses	"ndsLoginProperties","top","person","organizationalPerson","inetOrgPerson"	This entry holds the list of object classes required for a USER object.

Table 7-6 (Cont.) Entries in the Lookup.EDIR.Configuration Lookup Definition

Code	Decode	Description
uidAttribute	guid	This entry holds the LDAP attribute to which the predefined UID attribute must be mapped to.
rBSRole Configuration Lookup	Lookup.EDIR.Role.Configuration	This entry holds the name of the lookup definition that contains role-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of roles. Do not modify this entry
Bundle Version	1.0.6380	This entry holds the version of the connector bundle class. Do not modify this entry.
groupMemberAttribute	member	This entry holds the list of object classes required for a GROUP object.
Any Incremental Recon Attribute Type	TRUE	Indicates that any format of token is accepted during reconciliation. For Novell eDirectory, token type is String.
enabledValue	FALSE	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is enabled.
ldapGroupMembershipAttribute	groupMembership	This field gets updated with the group reference in the user entry. Its updated only if activateGroupMembershipAttribute configuration is set to true.
Group Configuration Lookup	Lookup.EDIR.Group.Configuration	This entry holds the name of the lookup definition that contains group-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of groups. Do not modify this entry.
disabledValue	TRUE	This entry specifies the value to use for the attribute defined by the enabledAttribute property whenever an account is disabled.
secondaryGroupMemberAttributes	equivalentToMe	Other attributes in the group entry that have to be updated with user reference along with the primary membership attribute.

Table 7-6 (Cont.) Entries in the Lookup.EDIR.Configuration Lookup Definition

Code	Decode	Description
readTimeout	120000 milliseconds	This property holds the value for the read timeout configuration property. These values can be increased or decreased if necessary. If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
connectTimeout	120000 milliseconds	This property holds the value for the connect timeout configuration property. These values can be increased or decreased if necessary.If this property is not added in the configuration lookup definition, then the value is set to 60000 milliseconds by default.
referrals	ignore, follow, or throw	This property holds the value for the read referrals configuration property. If this property is not added in the configuration lookup definition, then the value is set to ignore by default.

7.4.2 Lookup.EDIR.CommLang

The Lookup.EDIR.CommLang lookup definition contains the supported user languages. Do not modify the entries in this lookup definition. Table 7-7 lists the default entries.

Table 7-7 Entries in the Lookup.EDIR.CommLang Lookup Definition

Code Key	Decode
TRADITIONAL CHINESE	TRADITIONAL CHINESE
GERMAN	GERMAN
BRAZILIAN PORTUGUESE	BRAZILIAN PORTUGUESE
JAPANESE	JAPANESE
ITALIAN	ITALIAN
KOREAN	KOREAN
SIMPLIFIED CHINESE	SIMPLIFIED CHINESE
ENGLISH	ENGLISH
FRENCH	FRENCH
SPANISH	SPANISH

7.4.3 Preconfigured Lookup Definitions for User Operations

This section describes the following lookup definitions for user operations:

- Lookup.EDIR.UM.Configuration
- Lookup.EDIR.UM.ProvAttrMap
- Lookup.EDIR.UM.ReconAttrMap
- Other Lookup Definitions

7.4.3.1 Lookup.EDIR.UM.Configuration

The Lookup.EDIR.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 7-8 lists the default entries in this lookup definition.

Table 7-8 Entries in the Lookup.EDIR.UM.Configuration Lookup Definition

Code	Decode
Provisioning Attribute Map	Lookup.EDIR.UM.ProvAttrMap
Provisioning Exclusion List	Lookup.EDIR.UM.ProvExclusions
Provisioning Validation Lookup	Lookup.EDIR.UM.ProvValidations
Recon Attribute Defaults	Lookup.EDIR.UM.ReconDefaults
Recon Attribute Map	Lookup.EDIR.UM.ReconAttrMap
Recon Exclusion List	Lookup.EDIR.UM.ReconExclusions
Recon Transformation Lookup	Lookup.EDIR.UM.ReconTramsformations
Recon Validation Lookup	Lookup.EDIR.UM.ReconValidations

7.4.3.2 Lookup.EDIR.UM.ProvAttrMap

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

See Table 7-1 for the entries in this lookup definition.

7.4.3.3 Lookup.EDIR.UM.ReconAttrMap

The Lookup.EDIR.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.

Table 7-9 lists the entries in this lookup definition.

Table 7-9 Entries in the Lookup.EDIR.UM.ReconAttrMap Lookup Definition

Code	Decode
Communication Language	preferredLanguage
Container DN[LOOKUP]	__PARENTDN__
Department	departmentNumber
Email	mail

Table 7-9 (Cont.) Entries in the Lookup.EDIR.UM.ReconAttrMap Lookup Definition

Code	Decode
entryDN[IGNORE]	entryDN
First Name	givenName
Guid __UID__	
Last Name	sn
Location	l
Logon Script	loginScript
Middle Initial	initials
parentDN[IGNORE]	__PARENTDN__
Profile	profile
refid	__UID__
Role~Inheritance	rbsAssignedRoles~rbsRole~inheritable
Role~Role Name[LOOKUP]	rbsAssignedRoles~rbsRole~__NAME__
Role~Scope[LOOKUP]	rbsAssignedRoles~rbsRole~domainScope
Security Group~Group Name[LOOKUP]	ldapGroups
Status	__ENABLE__
Telephone	telephoneNumber
TimeZone	timezone
Title	title
User ID	entryDN **Note:** The decode value for the "User ID" code key must always be mapped to a target system attribute which contains a unique value.

7.4.3.4 Other Lookup Definitions

Other lookup definitions used for an eDirectory target system include:

- The Lookup.EDIR.UM.ProvValidation lookup allows you to have custom validations on any of provisioning attribute values.

  The Lookup.EDIR.UM.ReconValidation lookup allows you to have validations on any of the reconciled values.

  See Configuring Validation of Data During Reconciliation and Provisioning.
- The Lookup.EDIR.UM.ProvExclusions lookup allows you to specify account properties that should not be managed by the connector during provisioning. This lookup can also contain rules for determining excluded accounts.

  The Lookup.EDIR.UM.ReconExclusions lookup allows you to specify account properties that should not be managed by the connector during reconciliation. This lookup can also contain rules for determining the excluded accounts.
- The Lookup.EDIR.UM.ReconDefaults lookup allows you to specify default values for any reconciliation field.

- Lookup.EDIR.UM.ReconTransformation lookup allows you to specify custom transformations during reconciliation. See Configuring Transformation of Data During Reconciliation.

7.4.4 Preconfigured Lookup Definitions for Group Operations

This section discusses the following lookup definitions for group operations:

- Lookup.EDIR.Group.Configuration
- Lookup.EDIR.Group.ReconAttrMap
- Lookup.EDIR.Group.ProvAttrMap

7.4.4.1 Lookup.EDIR.Group.Configuration

The Lookup.EDIR.Group.Configuration lookup definition holds configuration entries that are specific to the group object type. This lookup definition is used during group management operations when your target system is configured as a target resource.

Table 7-10 Entries in the Lookup.EDIR.Group.Configuration Lookup Definition

Code	Decode	Description
Provisioning Attribute Map	Lookup.EDIR.Group.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.EDIR.Group.ProvAttrMap.
Recon Attribute Map	Lookup.EDIR.Group.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.EDIR.Group.ReconAttrMap.

7.4.4.2 Lookup.EDIR.Group.ProvAttrMap

The Lookup.EDIR.Group.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during group provisioning operations.

See Table 7-2 for the entries in this lookup definition.

7.4.4.3 Lookup.EDIR.Group.ReconAttrMap

The Lookup.EDIR.Group.ReconAttrMaplookup definition holds mappings between resource object fields for groups and target system attributes. This lookup definition is used during reconciliation.

See Table 7-11 for the entries in this lookup definition.

Table 7-11 Entries in the Lookup.EDIR.Group.ReconAttrMap Lookup Definition

Code	Decode
GroupName	cn
Guid	__UID__

Table 7-11 (Cont.) Entries in the Lookup.EDIR.Group.ReconAttrMap Lookup Definition

Code	Decode
Organization[LOOKUP]	__PARENTDN__

7.4.5 Preconfigured Lookup Definitions for Role Operations

This section describes the following lookup definitions for role operations:

- Lookup.EDIR.Role.Configuration
- Lookup.EDIR.Role.ReconAttrMap
- Lookup.EDIR.Role.ProvAttrMap

> **Note:**
>
> For eDirectory, the supported objectclass for roles is `rBSRole`.

7.4.5.1 Lookup.EDIR.Role.Configuration

The Lookup.EDIR.Role.Configuration lookup definition holds configuration entries that are specific to the role object type. This lookup definition is used during role management operations when your target system is configured as a target resource.

Table 7-12 Entries in the Lookup.EDIR.Role.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.EDIR.Role.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.EDIR.Role.ProvAttrMap.
Recon Attribute Map	Lookup.EDIR.Role.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.EDIR.Role.ReconAttrMap.

7.4.5.2 Lookup.EDIR.Role.ProvAttrMap

The Lookup.EDIR.Role.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during role provisioning operations.

See Table 7-3 for the entries in this lookup definition.

7.4.5.3 Lookup.EDIR.Role.ReconAttrMap

The Lookup.EDIR.Role.ReconAttrMap lookup definition holds mappings between resource object fields for roles and target system attributes. This lookup definitions is used during reconciliation.

Table 7-13 lists the entries in this lookup definition.

Table 7-13 Entries in the Lookup.EDIR.Role.ReconAttrMap Lookup Definition

Code	Decode
Guid	__UID__
Organization[LOOKUP]	__PARENTDN__
RoleName	cn

7.4.6 Preconfigured Lookup Definitions for Organizational Unit Operations

This section describes the following lookup definitions for organizational unit operations:

- Lookup.EDIR.OU.Configuration
- Lookup.EDIR.OU.ProvAttrMap
- Lookup.EDIR.OU.ReconAttrMap

7.4.6.1 Lookup.EDIR.OU.Configuration

The Lookup.EDIR.OU.Configuration lookup definition holds configuration entries that are specific to the organizational unit object type. This lookup definition is used during organizational unit management operations when your target system is configured as a target resource.

Table 7-14 lists the default entries in this lookup definition.

Table 7-14 Entries in the Lookup.EDIR.OU.Configuration Lookup Definition

Code	Decode	Description
Provisioning Attribute Map	Lookup.EDIR.OU.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.EDIR.OU.ProvAttrMap.
Recon Attribute Map	Lookup.EDIR.OU.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.EDIR.OU.ReconAttrMap.

7.4.6.2 Lookup.EDIR.OU.ProvAttrMap

The Lookup.EDIR.OU.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is used during provisioning.

See Table 7-4 for the entries in this lookup definition.

7.4.6.3 Lookup.EDIR.OU.ReconAttrMap

The Lookup.EDIR.Role.ReconAttrMap lookup definition holds mappings between resource object fields for roles and target system attributes. This lookup definitions is used during reconciliation.

Table 7-13 lists the entries in this lookup definition.

Table 7-15 Entries in the Lookup.EDIR.OU.ReconAttrMap Lookup Definition

Code	Decode
Container	__PARENTDN__
Guid	__UID__
OrgName	ou

7.4.7 Preconfigured Lookup Definitions for Trusted Configuration Operations

The connector uses the following lookup definitions for trusted configuration operations:

- Lookup.EDIR.Configuration.Trusted
- Lookup.EDIR.UM.Configuration.Trusted
- Lookup.EDIR.UM.ExclusionList.Trusted
- Lookup.EDIR.UM.ReconAttrMap.Trusted
- Lookup.EDIR.UM.ReconTransformations.Trusted
- Lookup.EDIR.UM.ReconDefaults.Trusted

7.4.7.1 Lookup.EDIR.Configuration.Trusted

Table 7-16 lists the entries in this lookup definition.

Table 7-16 Entries in the Lookup.EDIR.Configuration.Trusted Lookup Definition

Code	Decode
accountObjectClasses	"top","person","organizationalPerson","inetOrgPerson"
Any Incremental Recon Attribute Type	true
Bundle Name	org.identityconnectors.ldap
Bundle Version	1.0.6380
Connector Name	org.identityconnectors.ldap.LdapConnector
disabledValue	true
enabledAttribute	loginDisabled
enabledValue	false

Table 7-16 (Cont.) Entries in the Lookup.EDIR.Configuration.Trusted Lookup Definition

Code	Decode
objectClassesToSynchronize	"inetOrgPerson","groupOfNames","groupOfUniqueNames"
uidAttribute	GUID
uidInBinary	true
User Configuration Lookup	Lookup.EDIR.UM.Configuration.Trusted

7.4.7.2 Lookup.EDIR.UM.Configuration.Trusted

Table 7-17 lists the entries in this lookup definition.

Table 7-17 Entries in the Lookup.EDIR.UM.Configuration.Trusted Lookup Definition

Code	Decode
Recon Attribute Defaults	Lookup.EDIR.UM.ReconDefaults.Trusted
Recon Attribute Map	Lookup.EDIR.UM.ReconAttrMap.Trusted
Recon Exclusion List	Lookup.EDIR.UM.ExclusionList.Trusted
Recon Transformation Lookup	Lookup.EDIR.UM.ReconTransformations.Trusted
Recon Validation Lookup	Lookup.EDIR.UM.ReconValidations.Trusted

7.4.7.3 Lookup.EDIR.UM.ExclusionList.Trusted

Table 7-18 lists the entry in this lookup definition.

Table 7-18 Entry in the Lookup.EDIR.UM.ExclusionList.Trusted Lookup Definition

Code	Decode
User ID	root

7.4.7.4 Lookup.EDIR.UM.ReconAttrMap.Trusted

Table 7-19 lists the entries in this lookup definition.

Table 7-19 Entries in the Lookup.EDIR.UM.ReconAttrMap.Trusted Lookup Definition

Code Key	Decode
Department Number	departmentNumber
Mail	email
entryDN[IGNORE]	entryDN
Fax	facsimileTelephoneNumber
First Name	givenName

Table 7-19 (Cont.) Entries in the Lookup.EDIR.UM.ReconAttrMap.Trusted Lookup Definition

Code Key	Decode
GUID	__UID__
Last Name	sn
location	l
Pager	pager
parentDN[IGNORE]	__PARENTDN__
Postal Address	postalAddress
Postal Code	postalCode
Status[TRUSTED]	__ENABLE__
Street	street
Telephone	telephoneNumber
Title	title
User ID	entryDN **Note:** The decode value for the "User ID" code key must always be mapped to a target system attribute which contains a unique value.

7.4.7.5 Lookup.EDIR.UM.ReconTransformations.Trusted

Table 7-20 lists the entry in this lookup definition.

Table 7-20 Entry in the Lookup.EDIR.UM.ReconTransformations.Trusted Lookup Definition

Code	Decode
User ID	oracle.iam.connectors.edirectory.transformations.EdirectoryUserIdTransformation

7.4.7.6 Lookup.EDIR.UM.ReconDefaults.Trusted

Table 7-21 lists the entries in this lookup definition.

Table 7-21 Entries in the Lookup.EDIR.UM.ReconDefaults.Trusted Lookup Definition

Code	Decode
Empl Type	Full-Time
Organization Name	Xellerate Users
Status	Active
User Type	End-User

8 Using the Connector with an LDAPv3 Compliant Directory

This chapter describes the following information about using the connector with an LDAPv3 compliant directory server:

- Configuring Secure Communication
- Creating a New IT Resource Instance
- Configuring the Connector for OpenLDAP Server

> **Note:**
>
> In this chapter, OpenLDAP server is used as an example of an LDAPv3 compliant target system. You will need to adapt the examples in this chapter to the LDAPv3 compliant directory server you are using.

8.1 Configuring Secure Communication

To provide secure communications to the LDAPv3 target system, configure SSL between Oracle Identity Manager, the Connector Server, and the LDAPv3 target system.

For more information, see Configuring SSL for the Connector.

8.2 Creating a New IT Resource Instance

> **Note:**
>
> As a prerequisite, OpenLDAP server (or the LDAPv3 compliant directory server you are using) must be installed and configured. The examples in this chapter use the baseDN as `dc=example,dc=com` and the administrator account as `cn=admin,dc=example,dc=com`.

When you install the connector, create a new IT Resource instance named **OpenLDAP** with the parameters described in Table 8-1.

Table 8-1 Parameters of the IT Resource for the OpenLDAP Server Target System

Parameter	Description
host	OpenLDAP server hostname or IP address.

Table 8-1 (Cont.) Parameters of the IT Resource for the OpenLDAP Server Target System

Parameter	Description
port	OpenLDAP server port.
ssl	Specifies whether communication with the target system must be secured using SSL. Specify true or false, depending on how the OpenLDAP server is configured.
Configuration Lookup	Name of the lookup definition that stores configuration information used during reconciliation and provisioning. Specify Lookup.LDAP.Configuration.
baseContexts	Base contexts for operations on the target system. Sample value: "dc=example,dc=com"
credentials	Password you used during the OpenLDAP server setup.
principal	Bind DN for performing operations on the OpenLDAP server target system. Sample value: cn=admin,dc=example,dc=com

8.3 Configuring the Connector for OpenLDAP Server

This section describes these topics:

- Main Configuration Lookup
- User Provisioning
- Group Provisioning
- Organizational Unit (OU) Provisioning
- User Search Reconciliation

8.3.1 Main Configuration Lookup

The main configuration lookup **Lookup.LDAP.Configuration** contains the configuration parameters you need to change for an OpenLDAP server.

First, set `entryUUID` to `uidAttribute` in the **Lookup.LDAP.Configuration** lookup, because OpenLDAP uses `entryUUID`.

> **Note:**
>
> The Lookup.LDAP.Configuration contains many configuration properties that can change the behavior of the connector. See Lookup.LDAP.Configuration for more details on the configuration options. However, the most important configuration property is uidAttribute, which is explicitly mentioned in this section.

In order to make the provisioning work with the connector, configure the following lookup reconciliations, because these values are used in the provisioning forms:

- Organizational Unit (OU) Lookup Reconciliation
- Group Lookup Reconciliation

8.3.1.1 Organizational Unit (OU) Lookup Reconciliation

This Job finds all existing organizational units on target resource and reconciles them into the lookup configured in the **Lookup Name** job parameter (by default **Lookup.LDAP.Organization**).

The **Code Key Attribute** job parameter specifies which LDAP attribute will be used as the value in the lookup's **Code Key**. The default value `dn` doesn't need to be changed for OpenLDAP. Similarly, do not change the **Decode Attribute** job parameter, because the default value `ou` is sufficient.

Note that the **Object Type** job parameter is set to `OU` by default. The connector bundle translates this value to the `organizationalUnit` object class, so the organization units defined in OpenLDAP must have the `organizationUnit` object class assigned.

Therefore, you only need to set the **IT Resource Name** job parameter to **OpenLDAP**.

By running the task, the connector bundle will search using an LDAP filter like `(&(objectClass=top)(objectClass=organizationalUnit))`, and the attributes `dn` and `ou` will be used respectively as the **Code Key** and **Decode** values in the **Lookup.LDAP.Configuration** lookup.

8.3.1.2 Group Lookup Reconciliation

As in case of the previous lookup reconciliation job, the default parameters for this job should work sufficiently. Set the **IT Resource Name** parameter to **OpenLDAP**.

The `(&(objectClass=top)(objectClass=groupOfUniqueNames))` LDAP filter will be used to find out all groups available on the OpenLDAP server.

8.3.2 User Provisioning

This section contains the following topics:

- About User Provisioning With OpenLDAP
- Using the Enable/Disable Feature with OpenLDAP

8.3.2.1 About User Provisioning With OpenLDAP

The out-of-the-box configuration works sufficiently with OpenLDAP, and there is no need to change anything to make provisioning work.

When creating a new **LDAP User** resource object, Oracle Identity Manager uses the **LDAP User** process and triggers the **Create User** process task, which uses the `adpLDAPCREATEOBJECT` adapter.

The adapter calls the `ICProvisioningManager#createObject`method, which is a common implementation for all ICF based connectors. The `ICProvisioningManager` finds and configures the ICF connector bundle, maps the form fields to ICF attributes based on the

Lookup.LDAP.UM.ProvAttrMap lookup, and invokes the `CreateApiOp#create` ICF method. The connector bundle code takes care of actually creating the object in OpenLDAP.

Note that Lookup.LDAP.UM.ProvAttrMap contains the following entry:

`NsuniqueID:__UID__`

Because you configured `entryUUID` to be used as the `UID` attribute, the `Nsunique` form field attribute (configured as not visible) will be updated with the `entryUUID` value by object creation. Similar mapping is present for all groups and organizational units, and this field is used in reconciliation matching rules.

Updating the resource object functions in a similar way. Note that `LDAP User` process has the `UD_LDAP_USR Updated` process task, which is triggered by making changes to multiple fields. Thus, all the changes are handled in one `CreateApiOp#create` operation invocation.

LDAP User provisioning has out-of-the-box support for two multivalued attributes Group and Role, which means the following two child tables are defined in the `UD_LDAP_USR` table:

- `UD_LDAP_GRP` for groups
- `UD_LDAP_ROL` for roles

> **Note:**
>
> The connector supports the notion of Role and Group, only if the target directory implements these features in the following standard way:
>
> - For role: A multivalued attribute is added in the User Object that represents the user's role.
> - For group: A multivalued attribute is added in the Group Object that represents the members of the group.

Because OpenLDAP doesn't support roles, only groups can be used.

If you need to add an LDAP attribute that is not supported out-of-the-box, follow the steps described in Extending the Functionality of the Connector.

8.3.2.2 Using the Enable/Disable Feature with OpenLDAP

To use the enable/disable feature with OpenLDAP, perform the following steps in OpenLDAP:

1. Ensure you have the following entries in /etc/openldap/slapd.conf:

   ```
   include         /etc/openldap/schema/ppolicy.schema
   modulepath /usr/lib64/openldap
   moduleload ppolicy.la
   overlay ppolicy
   ppolicy_default "cn=default,ou=Password
   Policies,dc=example,dc=com"
   ppolicy_use_lockout
   ```

2. Restart OpenLDAP.

/etc/rc.d/init.d/ldap restart

3. Create new file named /tmp/policy.ldif with the following content and modify it as needed:

   ```
   # add default policy to DIT
   # attributes preceded with # indicate the defaults and
   # can be omitted
   # passwords must be reset every 30 days,
   # have a minimum length of 6 and users will
   # get a expiry warning starting 1 hour before
   # expiry, when the consecutive fail attempts exceed 5
   # the count will be locked and can only be reset by an
   # administrator, users do not need to supply the old
   # password when changing
   dn: cn=default,ou=Password Policies,dc=example,dc=com
   objectclass: top
   objectclass: person
   objectClass: pwdPolicy
   cn: default
   pwdMaxAge: 2592000
   #pwdExpireWarning: 3600
   #pwdInHistory: 0
   #pwdCheckQuality: 0
   pwdMaxFailure: 5
   pwdLockout: TRUE
   #pwdLockoutDuration: 0
   #pwdGraceAuthNLimit: 0
   #pwdFailureCountInterval: 0
   pwdMustChange: TRUE
   pwdMinLength: 6
   #pwdAllowUserChange: TRUE
   pwdSafeModify: FALSE
   pwdAttribute: userPassword
   sn: default
   ```

4. Import the policy to OpenLDAP. For example:

   ```
   ldapmodify -D cn=admin,dc=example,dc=com -W -a -f /tmp/policy.ldif
   ```

5. Set the following values in **Lookup.LDAP.Configuration**:

   ```
   enabledAttribute=pwdAccountLockedTime
   enabledValue=dummy
   disabledValue=000001010000Z
   enabledWhenNoAttribute=true
   allowOtherValuesForEnabledAttribute=true
   enabledWhenOtherValue=false
   ```

   > **Note:**
   >
   > Enabling or Disabling a user might be server specific. If you are using another LDAPv3 server, check how this feature is implemented for that server.
   >
   > The connector behavior can be configured using the configuration options enabledAttribute, enabledValue, disabledValue, enabledWhenNoAttribute, allowOtherValuesForEnabledAttribute, and enabledWhenOtherValue, which are mentioned in Step 5.

8.3.3 Group Provisioning

Group provisioning is done in Oracle Identity Manager by provisioning the `LDAP Group` resource object to the Oracle Identity Manager organization.

The connector uses `groupOfUniqueNames` as the object class for groups. OpenLDAP requires the `uniqueMember` attribute to be filled. Because the connector provides four attributes: `container`, `cn`, `__NAME__`, and `__UID__` as configured in Lookup.LDAP.Group.ProvAttrMap, the group provisioning ends up with an exception stating:

```
object class 'groupOfUniqueNames' requires attribute 'uniqueMember'
```

To resolve this issue, do one of the following:

- Update the `groupOfUniqueNames` object class schema in OpenLDAP so the `uniqueAttribute` is not required. However, this is not recommended by OpenLDAP.
- Configure Oracle Identity Manager to provide the `uniqueMember` attribute value every time the group is created or updated by adding the following entry to Lookup.LDAP.Group.ProvAttrMap:

  ```
  uniqueMember: uniqueMember='cn=admin,dc=example,dc=com'
  ```

  This entry ensures that the admin user is member of every group provisioned by Oracle Identity Manager. Note that this might not be desirable for some deployments.

If you need to add an LDAP attribute that is not supported out-of-the-box, follow the steps described in Extending the Functionality of the Connector.

8.3.4 Organizational Unit (OU) Provisioning

Organizational unit provisioning is done in Oracle Identity Manager by provisioning the `LDAP Organisation Unit` resource object to the Oracle Identity Manager organization.

As already mentioned in Organizational Unit (OU) Lookup Reconciliation,, the connector uses the `organizationalUnit` object class for organizational unit provisioning. There is no need to change any configuration to make OpenLDAP OU provisioning work.

If you need to add an LDAP attribute that is not supported out-of-the-box, follow the steps described in Extending the Functionality of the Connector.

8.3.5 User Search Reconciliation

This section contains the following topics:

- About User Search Reconciliation
- User Search Delete Reconciliation
- Trusted User Reconciliation
- Trusted User Delete Reconciliation
- Group Search Reconciliation

- Group Search Delete Reconciliation
- OU Search Reconciliation
- OU Search Delete Reconciliation
- Unused Reconciliation Jobs

8.3.5.1 About User Search Reconciliation

The out-of-the-box configuration works sufficiently with OpenLDAP, so just set **OpenLDAP** as the **IT Resource Name**. By default the `modifyTimestamp` attribute is configured as `Incremental Recon Attribute`, which works with OpenLDAP.

Note that Lookup.LDAP.UM.ReconAttrMap contains the following entry:

```
NsuniqueID: __UID__
```

Because `entryUUID` is configured as `uidAttribute`, the `entryUUID` value will be stored in the `NsuniqueID` field. This field is also used in the reconciliation matching rule.

> **Note:**
>
> Check if your LDAPv3 server supports modifyTimestamp. If modifyTimestamp is not supported, delete Incremental Recon Attribute, and the schedule job will always run full reconciliation.

If you need to add a custom attribute for reconciliation, see Adding Custom Fields for Target Resource Reconciliation.

8.3.5.2 User Search Delete Reconciliation

This jobs works out-of-the-box too. The only thing that needs to be done is to set **IT Resource Name** to **OpenLDAP**.

8.3.5.3 Trusted User Reconciliation

For trusted reconciliations, you must create a separate IT Resource, as follows:

1. Create an **OpenLDAP Trusted** IT Resource of type **LDAP**.
2. Set the same connection parameters as used in the OpenLDAP IT Resource.
3. Set **Lookup.LDAP.Configuration.Trusted** as the **Configuration Lookup** parameter value.
4. Set the **IT Resource Name** job parameter to **OpenLDAP Trusted** to make this job work with OpenLDAP.

8.3.5.4 Trusted User Delete Reconciliation

Setting the **IT Resource Name** job parameter to **OpenLDAP Trusted** is sufficient to make this job work with OpenLDAP.

8.3.5.5 Group Search Reconciliation

Setting the **IT Resource Name** job parameter to **OpenLDAP** is sufficient to make this job work with OpenLDAP.

8.3.5.6 Group Search Delete Reconciliation

Setting the **IT Resource Name** job parameter to **OpenLDAP** is sufficient to make this job work with OpenLDAP.

8.3.5.7 OU Search Reconciliation

Setting the **IT Resource Name** job parameter to **OpenLDAP** is sufficient to make this job work with OpenLDAP.

8.3.5.8 OU Search Delete Reconciliation

Setting the **IT Resource Name** job parameter to **OpenLDAP** is sufficient to make this job work with OpenLDAP.

8.3.5.9 Unused Reconciliation Jobs

You cannot use the following reconciliation jobs with OpenLDAP, because OpenLDAP doesn't support changelog and roles:

- Group Sync Reconciliation
- Organizational Unit (OU) Sync Reconciliation
- Role Lookup Reconciliation
- Role Search Delete Reconciliation
- Role Search Reconciliation
- Role Sync Reconciliation
- User Sync Reconciliation

9 Extending the Functionality of the Connector

This chapter describes procedures that you can perform to extend the functionality of the connector for addressing your specific business requirements.

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

This chapter discusses the following sections:

- Adding Custom Fields for Target Resource Reconciliation
- Adding New Multivalued Fields for Target Resource Reconciliation
- Adding Custom Fields for Provisioning
- Adding New Multivalued Fields for Provisioning
- Adding New Fields for Trusted Source Reconciliation
- Configuring Transformation of Data During Reconciliation
- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring the Connector for User-Defined Object Classes
- Configuring the Connector to Use Custom Object Classes
- Configuring the Connector for Multiple Trusted Source Reconciliation
- Configuring the Connector to Support POSIX Groups and Accounts
- Configuring the Connector to Support Provisioning of Custom Object Classes while Provisioning Organizational Unit

9.1 Adding Custom Fields for Target Resource Reconciliation

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to add custom fields for target resource reconciliation.

By default, the fields listed in Table 1-5 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional fields for user reconciliation.

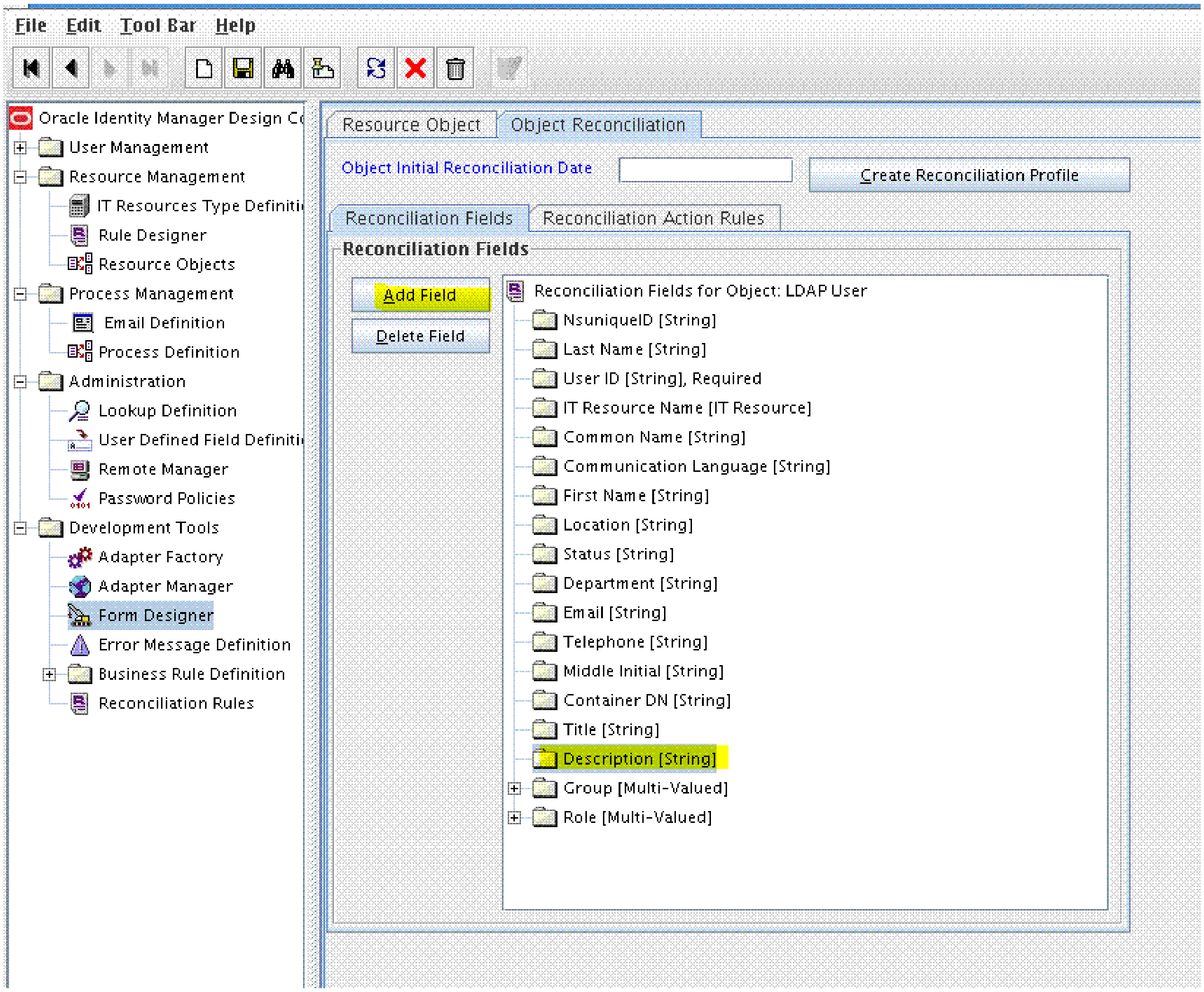
To add a custom field for target resource reconciliation, perform the following procedures:

- Adding the Custom Field to Resource Object Reconciliation Fields
- Creating an Entry for the Custom Field in the Lookup Definition for Reconciliation
- Adding the Custom Field on the Process Form
- Associating a New Form With the Application Instance
- Creating a Reconciliation Field Mapping for the Custom Field in the Provisioning Process
- Creating the Reconciliation Profile

9.1.1 Adding the Custom Field to Resource Object Reconciliation Fields

To add the custom field to the list of reconciliation fields in the resource object:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Resource Management** and then double-click **Resource Objects**.
3. Search for and open the **LDAP User**, **OID User**, or **eDirectory User** resource object.
4. On the Object Reconciliation tab, click **Add Field**. For example:

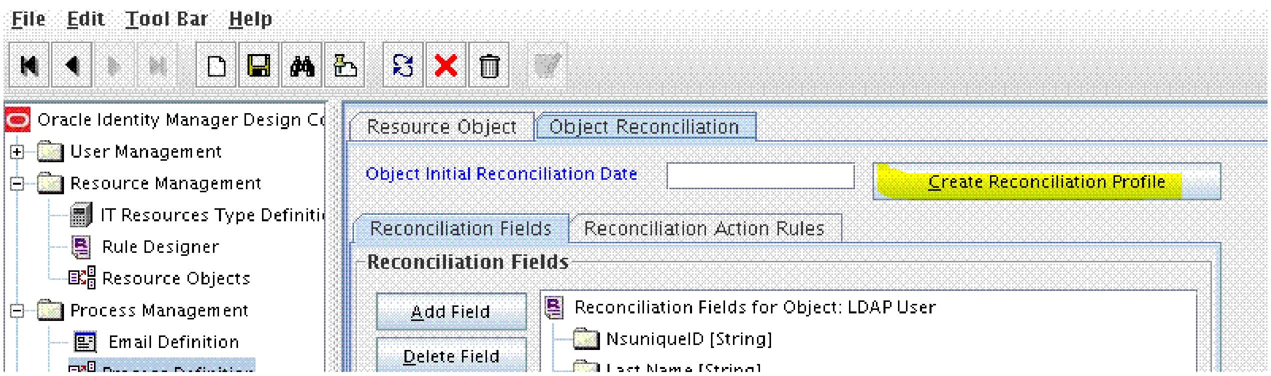


5. In the Add Reconciliation Field dialog box, enter the details of the field.

   For example, enter `Description` in the Field Name field and select **String** from the Field Type list.

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

7. Click **Create Reconciliation Profile**. This copies changes made to the resource object into Oracle Identity Manager Meta Data Store (MDS). For example:



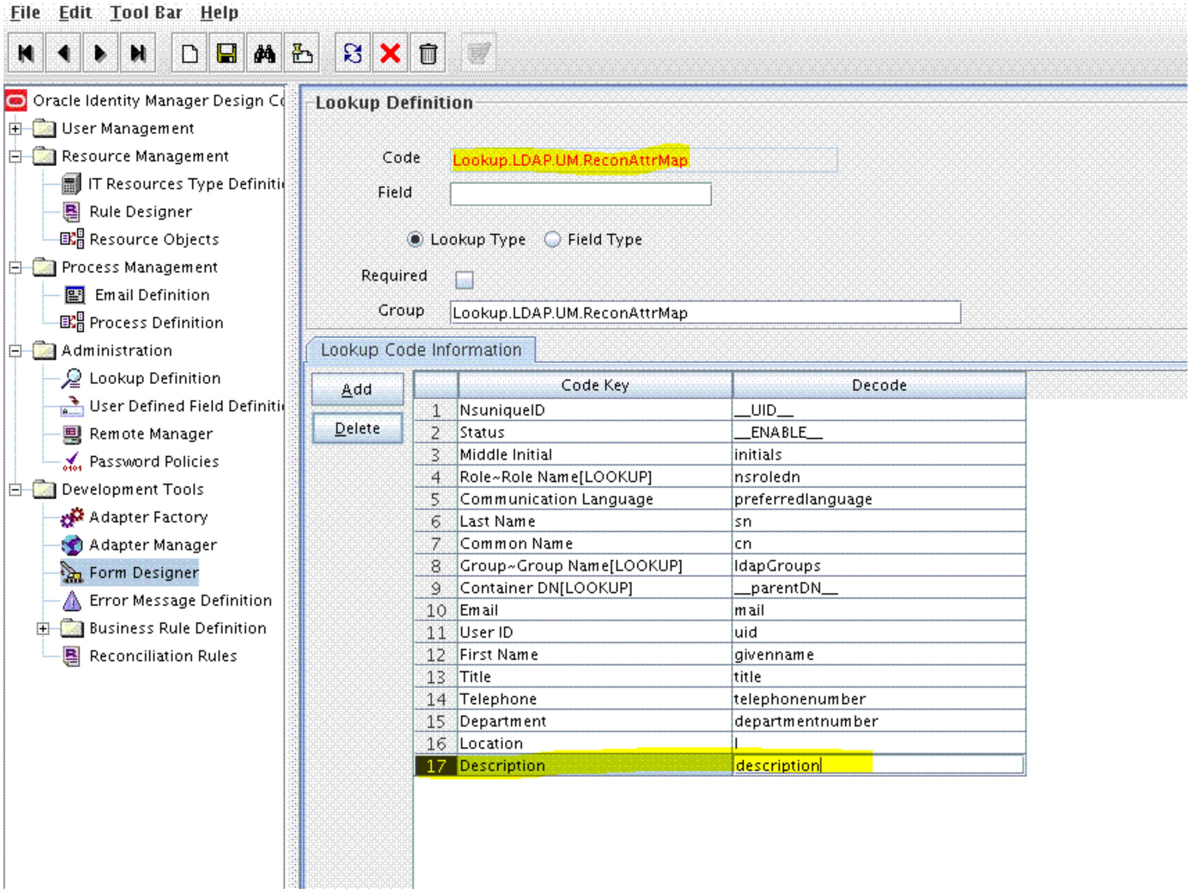
8. Click **Save.**

9.1.2 Creating an Entry for the Custom Field in the Lookup Definition for Reconciliation

To create an entry for the field in the lookup definition for reconciliation:

1. Expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.LDAP.UM.ReconAttrMap**, **Lookup.OID.UM.ReconAttrMap**, or **Lookup.EDIR.UM.ReconAttrMap** lookup definition.
3. Click **Add** and enter the Code Key and Decode values for the field. The Code Key value is the name of the field that you provide for the reconciliation field. The Decode value is the name of the target system field.

   For example, enter `Description` in the Code Key field and then enter `description` in the Decode field.



Code: Lookup.LDAP.UM.ReconAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: Lookup.LDAP.UM.ReconAttrMap

	Code Key	Decode
1	NsuniqueID	__UID__
2	Status	__ENABLE__
3	Middle Initial	initials
4	Role~Role Name[LOOKUP]	nsroledn
5	Communication Language	preferredlanguage
6	Last Name	sn
7	Common Name	cn
8	Group~Group Name[LOOKUP]	ldapGroups
9	Container DN[LOOKUP]	__parentDN__
10	Email	mail
11	User ID	uid
12	First Name	givenname
13	Title	title
14	Telephone	telephonenumber
15	Department	departmentnumber
16	Location	l
17	Description	description

4. Click **Save**.

9.1.3 Adding the Custom Field on the Process Form

To add the custom field on the process form:

1. Expand **Development Tools** and then double-click **Form Designer**.
2. Search for and open the **UD_LDAP_USR**, **UD_OID_USR**, or **UD_EDIR_USR** process form.
3. Click **Create New Version** and then click **Add Field**.
4. Enter the details of the field.

   For example, if you are adding the Description field, enter **UD_LDAP_USR_DESCRIPTION** or **UD_OID_USR_DESCRIPTION** in the Name field, and then enter the rest of the details of this field.

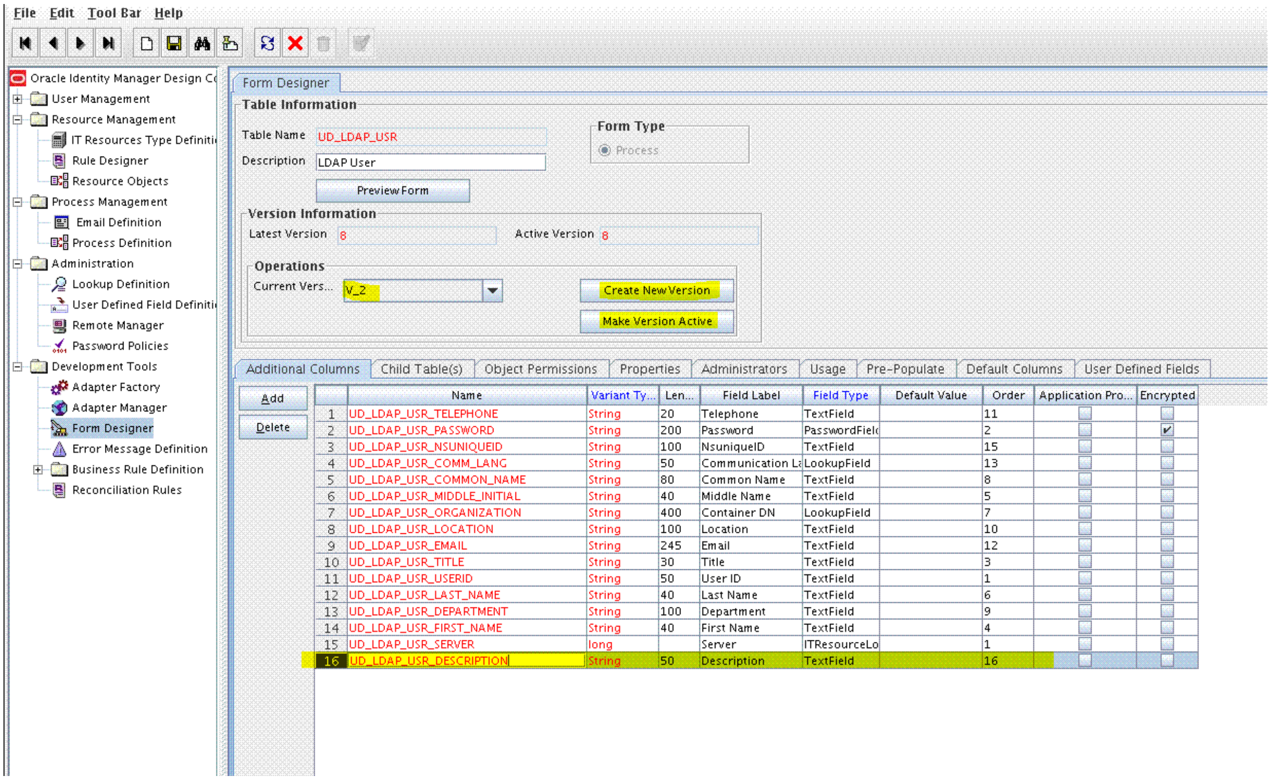


Table Information

Table Name UD_LDAP_USR

Description LDAP User

Form Type

● Process

Version Information

Latest Version 8

Active Version 8

Operations

Current Vers... V_2

	Name	Variant Ty...	Len...	Field Label	Field Type	Default Value	Order	Application Pro...	Encrypted
1	UD_LDAP_USR_TELEPHONE	String	20	Telephone	TextField		11	☐	☐
2	UD_LDAP_USR_PASSWORD	String	200	Password	PasswordFiel(		2	☐	☑
3	UD_LDAP_USR_NSUNIQUEID	String	100	NsuniqueID	TextField		15	☐	☐
4	UD_LDAP_USR_COMM_LANG	String	50	Communication La	LookupField		13	☐	☐
5	UD_LDAP_USR_COMMON_NAME	String	80	Common Name	TextField		8	☐	☐
6	UD_LDAP_USR_MIDDLE_INITIAL	String	40	Middle Name	TextField		5	☐	☐
7	UD_LDAP_USR_ORGANIZATION	String	400	Container DN	LookupField		7	☐	☐
8	UD_LDAP_USR_LOCATION	String	100	Location	TextField		10	☐	☐
9	UD_LDAP_USR_EMAIL	String	245	Email	TextField		12	☐	☐
10	UD_LDAP_USR_TITLE	String	30	Title	TextField		3	☐	☐
11	UD_LDAP_USR_USERID	String	50	User ID	TextField		1	☐	☐
12	UD_LDAP_USR_LAST_NAME	String	40	Last Name	TextField		6	☐	☐
13	UD_LDAP_USR_DEPARTMENT	String	100	Department	TextField		9	☐	☐
14	UD_LDAP_USR_FIRST_NAME	String	40	First Name	TextField		4	☐	☐
15	UD_LDAP_USR_SERVER	long		Server	ITResourceLo		1	☐	☐
16	UD_LDAP_USR_DESCRIPTION	String	50	Description	TextField		16	☐	☐

5. Click **Save** and then click **Make Version Active**.

9.1.4 Associating a New Form With the Application Instance

If you are using Oracle Identity Manager release 11.1.2.*x* or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:

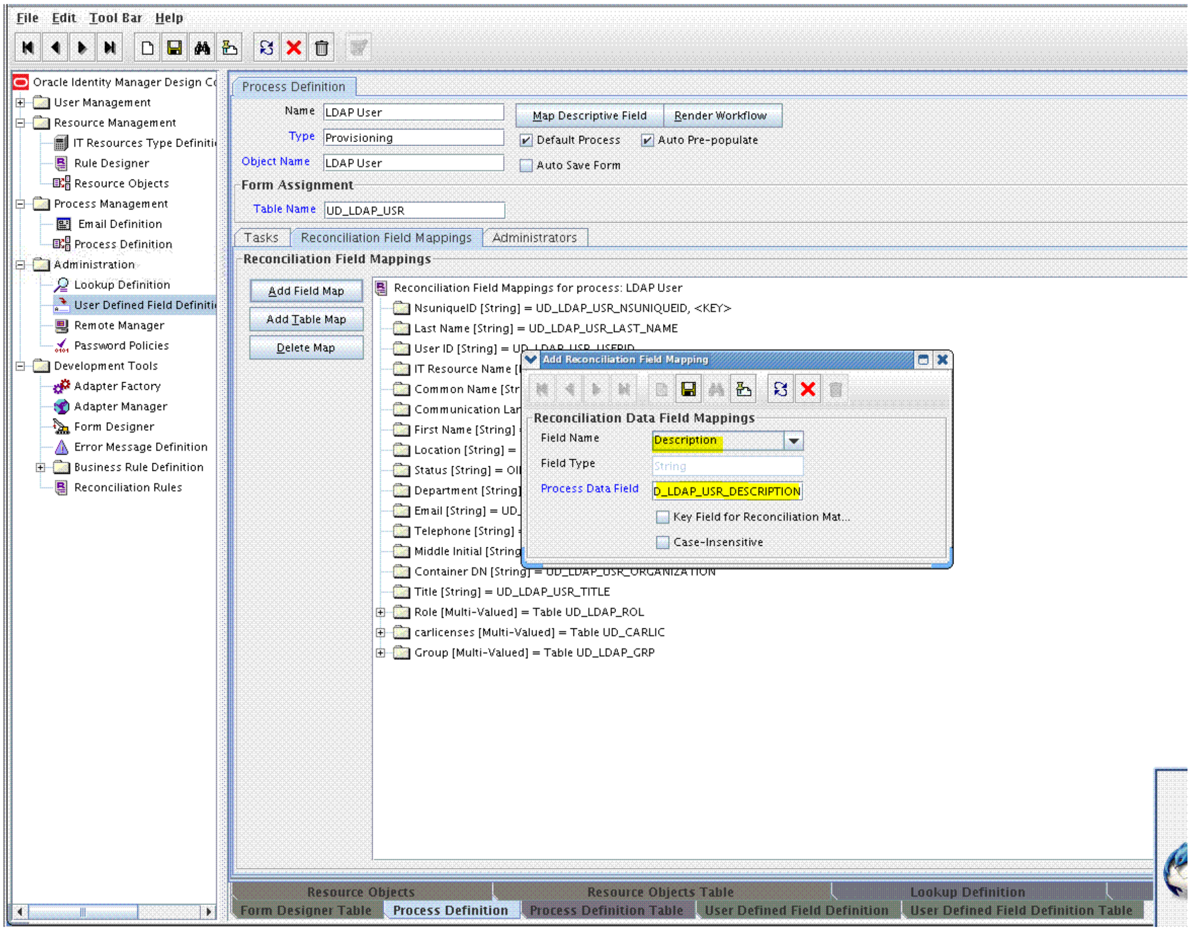
1. Log in to Oracle Identity System Administration.
2. Create and active a sandbox. See Creating and Activating a Sandbox for more information.
3. Create a new UI form to view the newly added field along with the rest of the fields. See Creating a New UI Form for more information about creating a UI form.
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 (created in Step 5.c), and then save the application instance.
5. Publish the sandbox. See Publishing a Sandbox for more information.

9.1.5 Creating a Reconciliation Field Mapping for the Custom Field in the Provisioning Process

Create a reconciliation field mapping for the custom field in the provisioning process as follows:

1. Expand **Process Management** and then double-click **Process Definition**.
2. Search for and open the **LDAP User**, **OID User**, or **eDirectory User** provisioning process.
3. On the Reconciliation Field Mappings tab of the provisioning process, click **Add Field Map**.
4. In the Add Reconciliation Field Mapping dialog box, from the Field Name field, select the value for the field that you want to add.

   For example, from the Field Name field, select **Description**.
5. Double-click the Process Data field, and then select **UD_LDAP_USR_DESCRIPTION** or **UD_OID_USR_DESCRIPTION**. For example:



Name: LDAP User
Type: Provisioning
Object Name: LDAP User
☑ Default Process
☑ Auto Pre-populate
☐ Auto Save Form

Form Assignment
Table Name: UD_LDAP_USR

Reconciliation Field Mappings

Reconciliation Field Mappings for process: LDAP User
- NsuniqueID [String] = UD_LDAP_USR_NSUNIQUEID, <KEY>
- Last Name [String] = UD_LDAP_USR_LAST_NAME
- User ID [String] = UD_LDAP_USR_USERID
- IT Resource Name [
- Common Name [Str
- Communication Lar
- First Name [String]
- Location [String] =
- Status [String] = OII
- Department [String]
- Email [String] = UD_
- Telephone [String]
- Middle Initial [String
- Container DN [String] = UD_LDAP_USR_ORGANIZATION
- Title [String] = UD_LDAP_USR_TITLE
- Role [Multi-Valued] = Table UD_LDAP_ROL
- carlicenses [Multi-Valued] = Table UD_CARLIC
- Group [Multi-Valued] = Table UD_LDAP_GRP

Reconciliation Data Field Mappings
Field Name: Description
Field Type: String
Process Data Field: D_LDAP_USR_DESCRIPTION
☐ Key Field for Reconciliation Mat...
☐ Case-Insensitive

6. Click **Save** and close the dialog box.
7. Click **Save**.

9.1.6 Creating the Reconciliation Profile

Create the Reconciliation Profile:

1. Expand **Resource Management** and then double-click **Resource Objects**.
2. Search for and open the **LDAP User**, **OID User**, or **eDirectory User** resource object.
3. Click **Create Reconciliation Profile**. This copies changes made to the resource object into Oracle Identity Manager Meta Data Store (MDS).

9.2 Adding New Multivalued Fields for Target Resource Reconciliation

By default, the multivalued fields listed in the respective lookup definitions are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new multivalued fields for target resource reconciliation.

> **Note:**
>
> - This section describes an optional procedure. Perform this procedure only if you want to add multivalued fields for target resource reconciliation.
> - You can apply this procedure to add either user, group, organizational unit, or role fields.
> - You must ensure that new fields you add for reconciliation contain only string-format data. Binary fields must not be brought into Oracle Identity Manager natively.

To add a new multivalued field for target resource reconciliation, perform the following procedures:

- Creating a Form for the Multivalued Field
- Adding the Form as a Child Form of the Process Form
- Associating a New Form With the Application Instance
- Adding the New Multivalued Field to the Resource Object Reconciliation Fields
- Creating an Entry for the Field in the Lookup Definition for Reconciliation
- Creating a Reconciliation Field Mapping for the New Field

9.2.1 Creating a Form for the Multivalued Field

To create a form for the multivalued field:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools** and double-click **Form Designer**.
3. Create a form by specifying a table name and description, and then click **Save**.

4. Click **Add** and enter the details of the field.
5. Click **Save** and then click **Make Version Active**. For example:

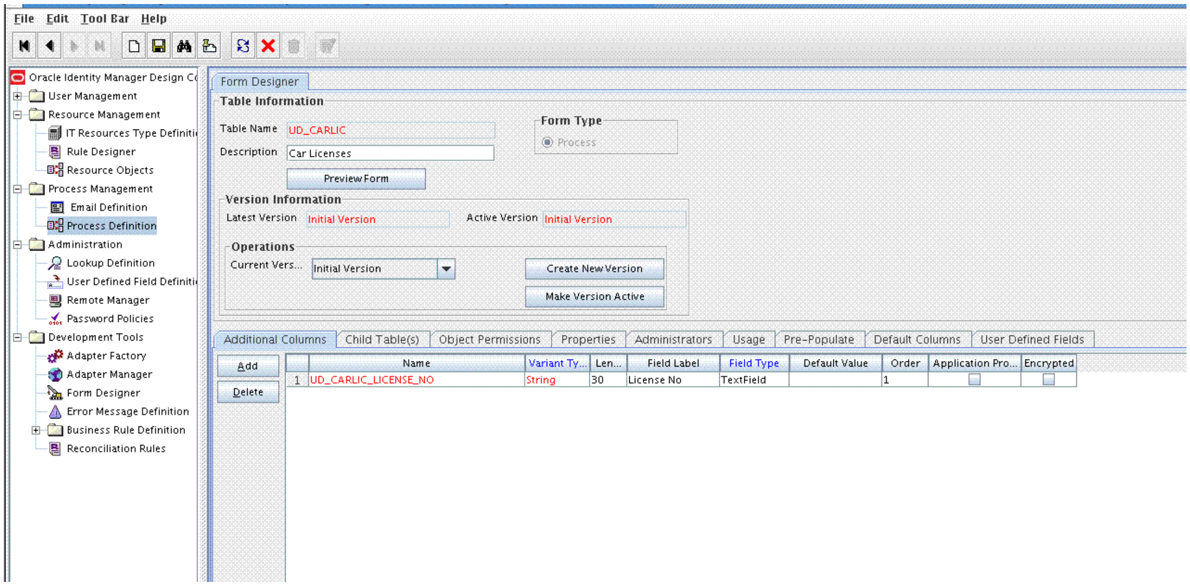


Table Name: UD_CARLIC
Description: Car Licenses
Form Type: ○ Process
Latest Version: Initial Version
Active Version: Initial Version
Current Vers...: Initial Version

	Name	Variant Ty...	Len...	Field Label	Field Type	Default Value	Order	Application Pro...	Encrypted
1	UD_CARLIC_LICENSE_NO	String	30	License No	TextField		1	☐	☐

9.2.2 Adding the Form as a Child Form of the Process Form

Add the form created for the multivalued field as a child form of the process form as follows:

1. Search for and open one of the following process forms:

   For users: **UD_LDAP_USR**, **UD_OID_USR**, or **UD_EDIR_USR**

   For groups: **UD_LDAP_GR**, **UD_OID_GR**, or **UD_EDIR_GR**

   For organizational units: **UD_LDAP_OU**, **UD_OID_OU**, or **UD_EDIR_OU**

   For roles: **UD_LDAP_RL** or **UD_EDIR_RL**
2. Click **Create New Version.**
3. Click the **Child Table(s)** tab.
4. Click **Assign.**
5. In the Assign Child Tables dialog box, select the newly created child form, click the right arrow, and then click **OK.**
6. Click **Save** and then click **Make Version Active**. For example:

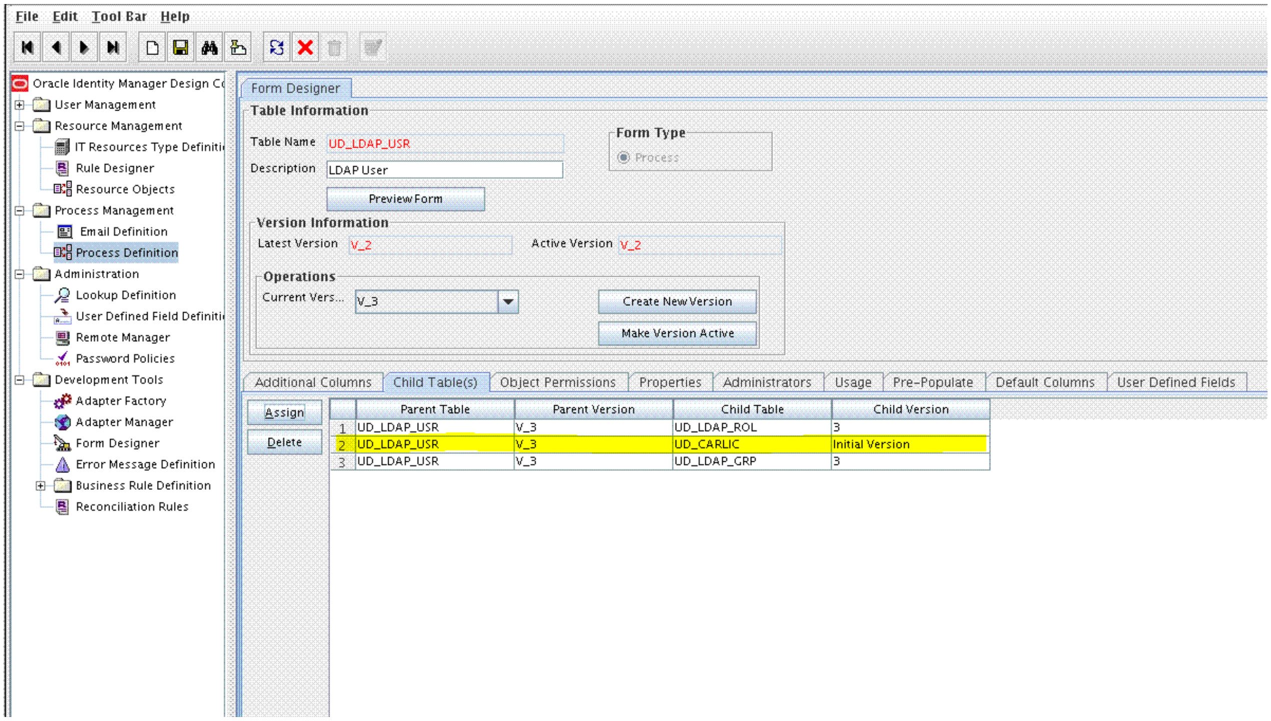


Table Information

Table Name UD_LDAP_USR

Description LDAP User

Form Type

○ Process

Version Information

Latest Version V_2

Active Version V_2

Operations

Current Vers... V_3

	Parent Table	Parent Version	Child Table	Child Version
1	UD_LDAP_USR	V_3	UD_LDAP_ROL	3
2	UD_LDAP_USR	V_3	UD_CARLIC	Initial Version
3	UD_LDAP_USR	V_3	UD_LDAP_GRP	3

9.2.3 Associating a New Form With the Application Instance

If you are using Oracle Identity Manager release 11.1.2.*x* or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:

1. Log in to Oracle Identity System Administration.
2. Create and active a sandbox. See Creating and Activating a Sandbox for more information.
3. Create a new UI form to view the newly added field along with the rest of the fields. See Creating a New UI Form for more information about creating a UI form.
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 (created in Step 4.c), and then save the application instance.
5. Publish the sandbox. See Publishing a Sandbox for more information.

9.2.4 Adding the New Multivalued Field to the Resource Object Reconciliation Fields

Add the new multivalued field to the list of reconciliation fields in the resource object as follows:

1. Expand **Resource Management** and then double-click **Resource Objects**.
2. Search for and open one of the following resource objects:

   For users: **LDAP User**, **OID User**, or **eDirectory User**

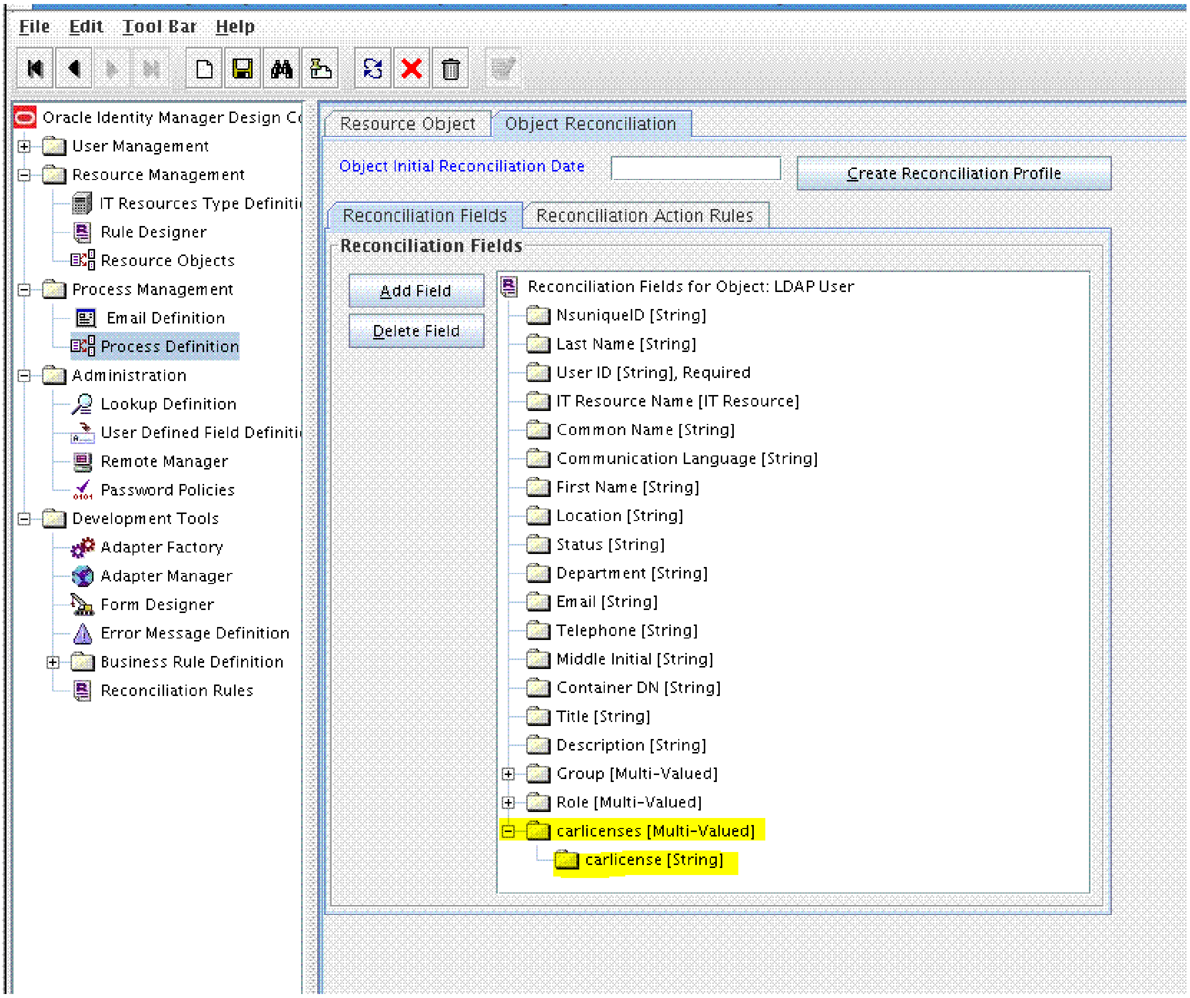
   For groups: **LDAP Group**, **OID Group**, or **eDirectory Group**

For organizational units: **LDAP Organizational Unit**, **OID Organizational Unit**, or **eDir Organisation Unit**

For roles: **LDAP Role** or **eDirectory Role**

3. On the Object Reconciliation tab, click **Add Field**.
4. In the Add Reconciliation Fields dialog box, enter the details of the field.

   For example, enter `carlicenses` in the **Field Name** field and select **Multi-Valued Attribute** from the Field Type list.



Reconciliation Fields for Object: LDAP User
- NsuniqueID [String]
- Last Name [String]
- User ID [String], Required
- IT Resource Name [IT Resource]
- Common Name [String]
- Communication Language [String]
- First Name [String]
- Location [String]
- Status [String]
- Department [String]
- Email [String]
- Telephone [String]
- Middle Initial [String]
- Container DN [String]
- Title [String]
- Description [String]
- Group [Multi-Valued]
- Role [Multi-Valued]
- carlicenses [Multi-Valued]
  - carlicense [String]

5. Click **Save** and then close the dialog box.
6. Right-click the newly created field and select **Define Property Fields**.
7. In the Add Reconciliation Fields dialog box, enter the details of the newly created field.

   For example, enter `carlicense` in the Field Name field and select **String** from the Field Type list.
8. Click **Save**, and then close the dialog box.
9. Click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.

9.2.5 Creating an Entry for the Field in the Lookup Definition for Reconciliation

Create an entry for the field in the lookup definition for reconciliation as follows:

1. Expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open one of the following lookup definitions:

   For users: **Lookup.LDAP.UM.ReconAttrMap**, **Lookup.OID.UM.ReconAttrMap**, or **Lookup.EDIR.UM.ReconAttrMap**

   For groups: **Lookup.LDAP.Group.ReconAttrMap**, **Lookup.OID.Group.ReconAttrMap**, or **Lookup.EDIR.Group.ReconAttrMap**

   For organizational units: **Lookup.LDAP.OU.ReconAttrMap**, **Lookup.OID.OU.ReconAttrMap**, or **Lookup.EDIR.OU.ReconAttrMap**

   For roles: **Lookup.LDAP.Role.ReconAttrMap** or **Lookup.EDIR.Role.ReconAttrMap**

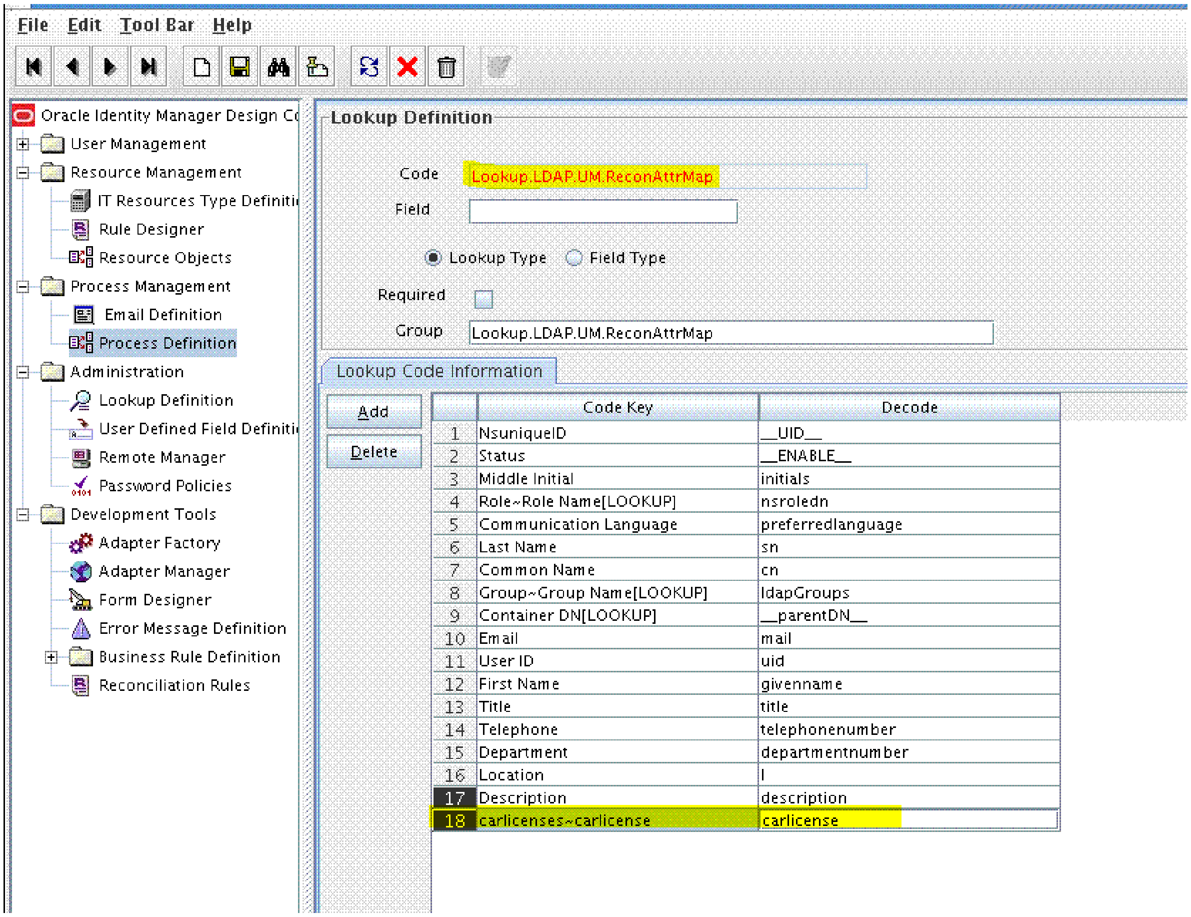
   > **Note:**
   >
   > For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the field names are case-sensitive.

3. Click **Add** and enter the Code Key and Decode values for the field, and then Click **Save**. The Code Key and Decode values must be in the following format:

   Code Key: *MULTIVALUED_FIELD_NAME~CHILD_RESOURCE_OBJECT_FIELD_NAME*

   Decode: Corresponding target system attribute.

   For example, enter `carlicenses~carlicense` in the Code Key field and then enter `carlicense` in the Decode field.



Code: Lookup.LDAP.UM.ReconAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: Lookup.LDAP.UM.ReconAttrMap

	Code Key	Decode
1	NsuniqueID	__UID__
2	Status	__ENABLE__
3	Middle Initial	initials
4	Role~Role Name[LOOKUP]	nsroledn
5	Communication Language	preferredlanguage
6	Last Name	sn
7	Common Name	cn
8	Group~Group Name[LOOKUP]	ldapGroups
9	Container DN[LOOKUP]	__parentDN__
10	Email	mail
11	User ID	uid
12	First Name	givenname
13	Title	title
14	Telephone	telephonenumber
15	Department	departmentnumber
16	Location	l
17	Description	description
18	carlicenses~carlicense	carlicense

9.2.6 Creating a Reconciliation Field Mapping for the New Field

Create a reconciliation field mapping for the new field as follows:

1. Expand **Process Management** and double-click **Process Definition**.
2. Search for and open one of the following process definitions:

   For users: **LDAP User**, **OID User**, or **eDirectory User**

   For groups: **LDAP Group**, **OID Group**, or **eDirectory Group**

   For organizational units: **LDAP Organizational Unit**, **OID Organizational Unit**, or **eDir Organisation Unit**

   For roles: **LDAP Role** or **eDirectory Role**
3. On the Reconciliation Field Mappings tab of one of the following process definitions, click **Add Table Map**:

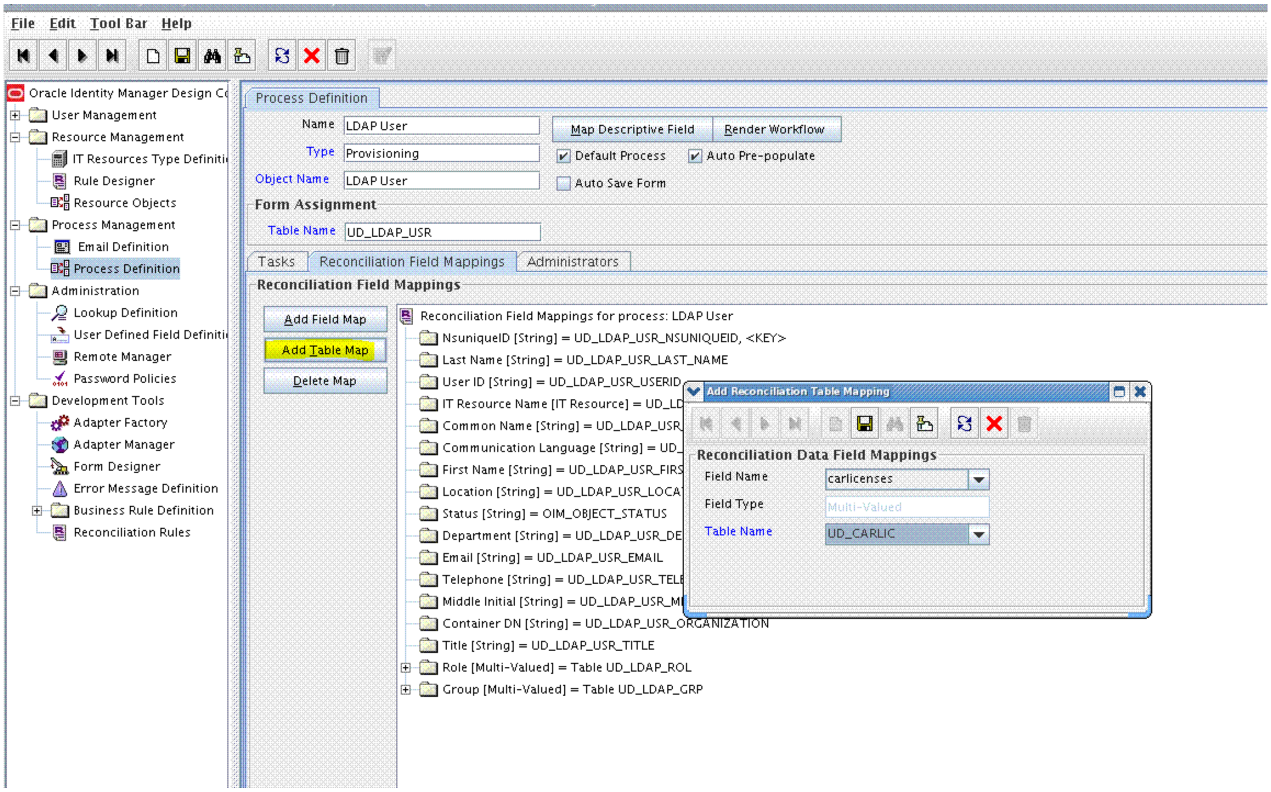
   For users: **LDAP User**, **OID User**, or **eDirectory User**

   For groups: **LDAP Group**, **OID Group**, or **eDirectory Group**

   For organizational units: **LDAP Organizational Unit**, **OID Organizational Unit**, or **eDir Organisation Unit**

   For roles: **LDAP Role** or **eDirectory Role**

   For example:



Name: LDAP User

Type: Provisioning

Object Name: LDAP User

☑ Default Process ☑ Auto Pre-populate

□ Auto Save Form

Form Assignment

Table Name: UD_LDAP_USR

Reconciliation Field Mappings

Reconciliation Field Mappings for process: LDAP User
- NsuniqueID [String] = UD_LDAP_USR_NSUNIQUEID, <KEY>
- Last Name [String] = UD_LDAP_USR_LAST_NAME
- User ID [String] = UD_LDAP_USR_USERID
- IT Resource Name [IT Resource] = UD_LD
- Common Name [String] = UD_LDAP_USR_
- Communication Language [String] = UD_
- First Name [String] = UD_LDAP_USR_FIRS
- Location [String] = UD_LDAP_USR_LOCA
- Status [String] = OIM_OBJECT_STATUS
- Department [String] = UD_LDAP_USR_DE
- Email [String] = UD_LDAP_USR_EMAIL
- Telephone [String] = UD_LDAP_USR_TELE
- Middle Initial [String] = UD_LDAP_USR_MI
- Container DN [String] = UD_LDAP_USR_ORGANIZATION
- Title [String] = UD_LDAP_USR_TITLE
- Role [Multi-Valued] = Table UD_LDAP_ROL
- Group [Multi-Valued] = Table UD_LDAP_GRP

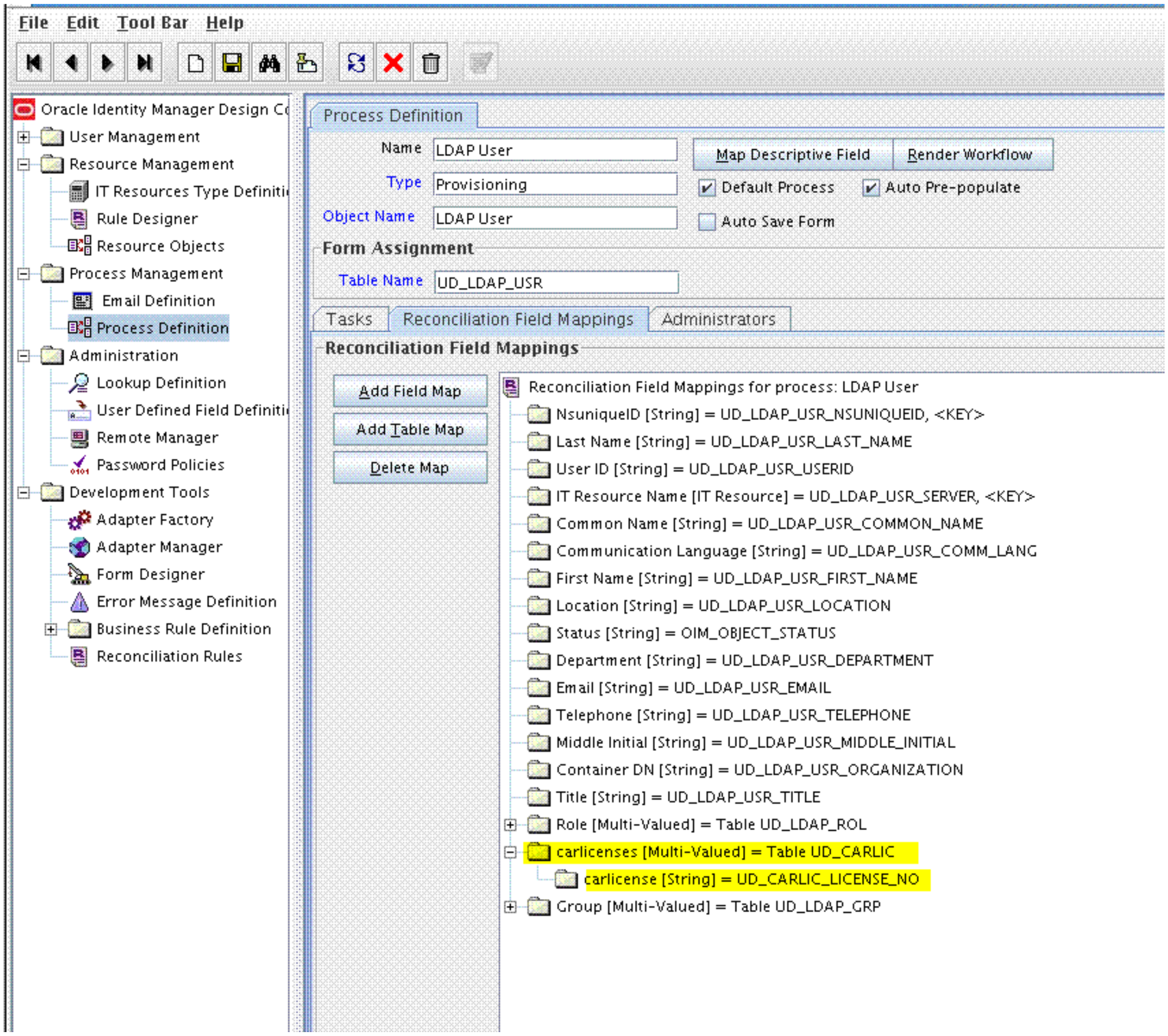
Reconciliation Data Field Mappings

Field Name: carlicenses

Field Type: Multi-Valued

Table Name: UD_CARLIC

4. In the Add Reconciliation Table Mapping dialog box, select the field name and table name from the list, click **Save**, and then close the dialog box. For example:



Name: LDAP User
Type: Provisioning
Object Name: LDAP User
☑ Default Process
☑ Auto Pre-populate
□ Auto Save Form
Table Name: UD_LDAP_USR

Reconciliation Field Mappings

Reconciliation Field Mappings for process: LDAP User
- NsuniqueID [String] = UD_LDAP_USR_NSUNIQUEID, <KEY>
- Last Name [String] = UD_LDAP_USR_LAST_NAME
- User ID [String] = UD_LDAP_USR_USERID
- IT Resource Name [IT Resource] = UD_LDAP_USR_SERVER, <KEY>
- Common Name [String] = UD_LDAP_USR_COMMON_NAME
- Communication Language [String] = UD_LDAP_USR_COMM_LANG
- First Name [String] = UD_LDAP_USR_FIRST_NAME
- Location [String] = UD_LDAP_USR_LOCATION
- Status [String] = OIM_OBJECT_STATUS
- Department [String] = UD_LDAP_USR_DEPARTMENT
- Email [String] = UD_LDAP_USR_EMAIL
- Telephone [String] = UD_LDAP_USR_TELEPHONE
- Middle Initial [String] = UD_LDAP_USR_MIDDLE_INITIAL
- Container DN [String] = UD_LDAP_USR_ORGANIZATION
- Title [String] = UD_LDAP_USR_TITLE
- Role [Multi-Valued] = Table UD_LDAP_ROL
- carlicenses [Multi-Valued] = Table UD_CARLIC
  - carlicense [String] = UD_CARLIC_LICENSE_NO
- Group [Multi-Valued] = Table UD_LDAP_GRP

5. Right-click the newly created field, and select **Define Property Field Map**.
6. In the Field Name field, select the value for the field that you want to add.
7. Double-click the **Process Data Field** field, and then select **UD_CARLICEN**.
8. Select **Key Field for Reconciliation Field Matching** and click **Save**.

9.3 Adding Custom Fields for Provisioning

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to add custom fields for provisioning.

By default, the attributes listed in User Fields for Provisioning are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

To add a custom field for provisioning, perform the following procedures:

- Adding the new Field to the Process Form
- Associating a New Form With the Application Instance
- Creating an Entry for the Field in the Lookup Definition for Provisioning
- Enabling Update Provisioning Operations on the Custom Field
- Updating the Request Dataset
- Running the PurgeCache Utility and Importing the Request Dataset Definition to MDS

9.3.1 Adding the new Field to the Process Form

To add the new field to the process form:

1. Log in to Oracle Identity Manager Design Console.
2. Add the new field to the process form.

   If you have added the field on the process form by performing the procedure described in Adding the Custom Field on the Process Form, then you need not add the field again. If you have not added the field, then:

   a. Expand **Development Tools** and then double-click **Form Designer**.
   b. Search for and open the **UD_LDAP_USR**, **UD_OID_USR**, or **UD_EDIR_USR** process form.
   c. Click **Create New Version** and then click **Add**.
   d. Enter the details of the field.

      For example, if you are adding the Description field, enter **UD_LDAP_USR_DESCRIPTION** or **UD_OID_USR_DESCRIPTION** in the Name field, and then enter the rest of the details of this field.
   e. Click **Save** and then click **Make Version Active**. For example:

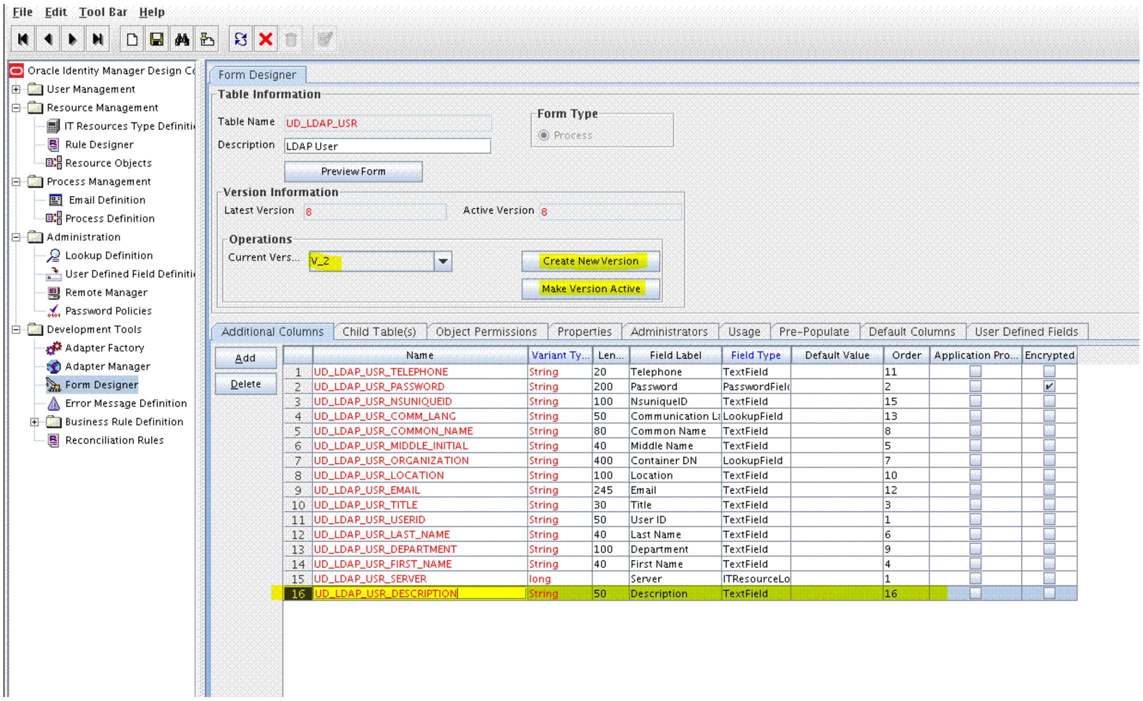


Table Information

Table Name UD_LDAP_USR

Description LDAP User

Form Type ● Process

Version Information

Latest Version 8

Active Version 8

Operations

Current Vers... V_2

	Name	Variant Ty...	Len...	Field Label	Field Type	Default Value	Order	Application Pro...	Encrypted
1	UD_LDAP_USR_TELEPHONE	String	20	Telephone	TextField		11	□	□
2	UD_LDAP_USR_PASSWORD	String	200	Password	PasswordFiel(		2	□	☑
3	UD_LDAP_USR_NSUNIQUEID	String	100	NsuniqueID	TextField		15	□	□
4	UD_LDAP_USR_COMM_LANG	String	50	Communication La	LookupField		13	□	□
5	UD_LDAP_USR_COMMON_NAME	String	80	Common Name	TextField		8	□	□
6	UD_LDAP_USR_MIDDLE_INITIAL	String	40	Middle Name	TextField		5	□	□
7	UD_LDAP_USR_ORGANIZATION	String	400	Container DN	LookupField		7	□	□
8	UD_LDAP_USR_LOCATION	String	100	Location	TextField		10	□	□
9	UD_LDAP_USR_EMAIL	String	245	Email	TextField		12	□	□
10	UD_LDAP_USR_TITLE	String	30	Title	TextField		3	□	□
11	UD_LDAP_USR_USERID	String	50	User ID	TextField		1	□	□
12	UD_LDAP_USR_LAST_NAME	String	40	Last Name	TextField		6	□	□
13	UD_LDAP_USR_DEPARTMENT	String	100	Department	TextField		9	□	□
14	UD_LDAP_USR_FIRST_NAME	String	40	First Name	TextField		4	□	□
15	UD_LDAP_USR_SERVER	long		Server	ITResourceLo		1	□	□
16	UD_LDAP_USR_DESCRIPTION	String	50	Description	TextField		16	□	□

9.3.2 Associating a New Form With the Application Instance

If you are using Oracle Identity Manager release 11.1.2.*x* or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:

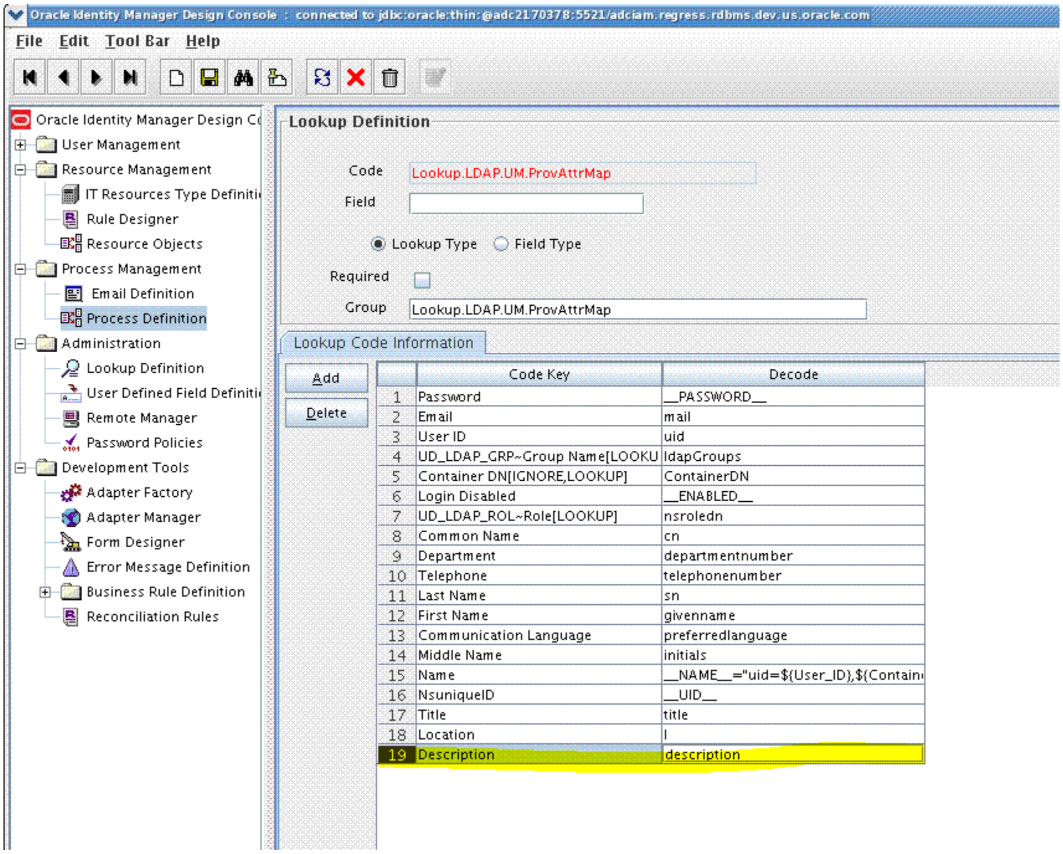
1. Log in to Oracle Identity System Administration.
2. Create and active a sandbox. See Creating and Activating a Sandbox for more information.
3. Create a new UI form to view the newly added field along with the rest of the fields. See Creating a New UI Form for more information about creating a UI form.
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 (created in Step 3.c), and then save the application instance.
5. Publish the sandbox. See Publishing a Sandbox for more information.

9.3.3 Creating an Entry for the Field in the Lookup Definition for Provisioning

Create an entry for the field in the lookup definition for provisioning as follows:

1. Expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.LDAP.UM.ProvAttrMap**, **Lookup.OID.UM.ProvAttrMap**, or **Lookup.EDIR.UM.ProvAttrMap** lookup definition.
3. Click **Add** and then enter the Code Key and Decode values for the field. The Decode value must be the name of the field on the target system.

For example, enter `Description` (name of the field added to the process form in Adding the new Field to the Process Form) in the Code Key field and then enter `description` in the Decode field. For example:



Code: Lookup.LDAP.UM.ProvAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: Lookup.LDAP.UM.ProvAttrMap

	Code Key	Decode
1	Password	__PASSWORD__
2	Email	mail
3	User ID	uid
4	UD_LDAP_GRP~Group Name[LOOKU	ldapGroups
5	Container DN[IGNORE,LOOKUP]	ContainerDN
6	Login Disabled	__ENABLED__
7	UD_LDAP_ROL~Role[LOOKUP]	nsroledn
8	Common Name	cn
9	Department	departmentnumber
10	Telephone	telephonenumber
11	Last Name	sn
12	First Name	givenname
13	Communication Language	preferredlanguage
14	Middle Name	initials
15	Name	__NAME__="uid=${User_ID},${Contain
16	NsuniqueID	__UID__
17	Title	title
18	Location	l
19	Description	description

4. Click **Save.**

9.3.4 Enabling Update Provisioning Operations on the Custom Field

Enable update provisioning operations on the custom field as follows:

1. In the provisioning process, add a new task for updating the field as follows:

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

   b. Search for and open the **LDAP User**, **OID User**, or **eDirectory User** provisioning process.

   c. Click **Add** and enter the task name and task description. The following are sample values:

      Task Name: `Description Updated`

      Task Description: `Process Task for handling update of the description field.`

   d. In the Task Properties section, select the following fields:

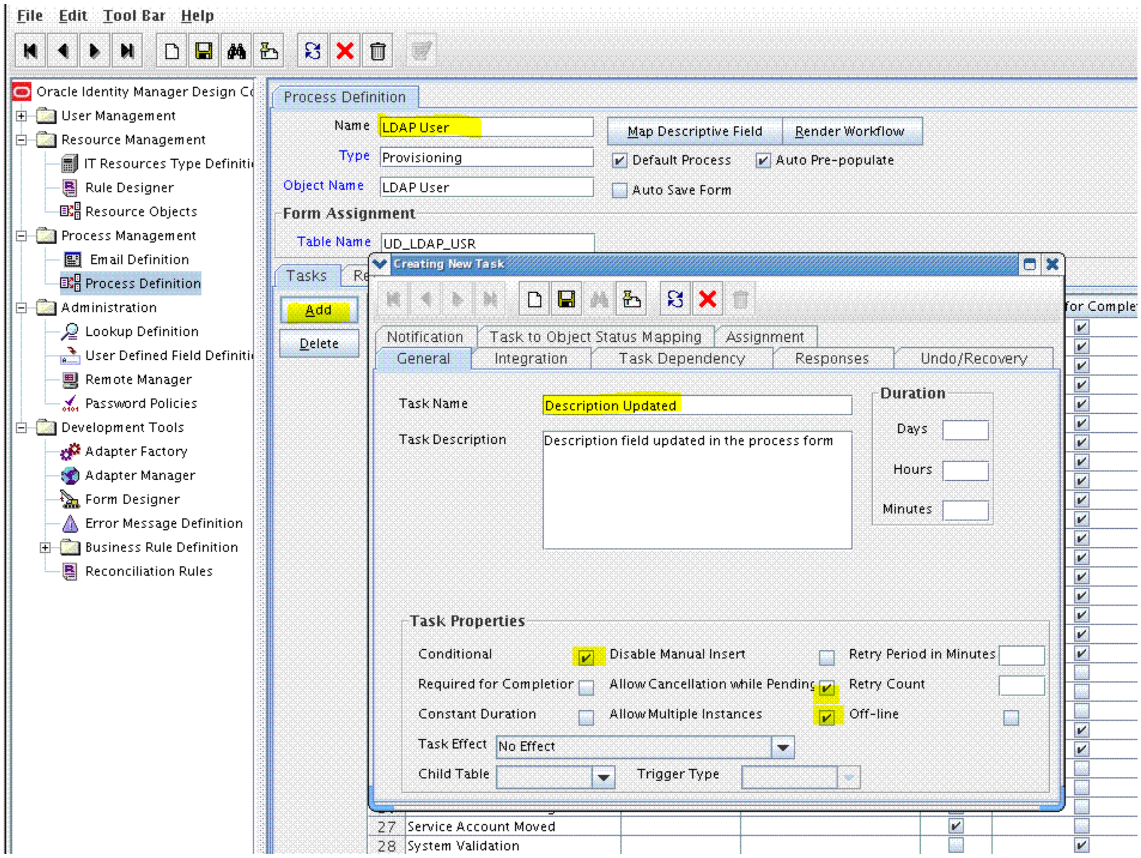
      - Conditional

      - Allow Cancellation while Pending

      - Allow Multiple Instances

e. Insert to add the data from the Trigger Type list.

f. Click **Save**. For example:



Name: LDAP User
Type: Provisioning
Object Name: LDAP User
☑ Default Process
☑ Auto Pre-populate
□ Auto Save Form

Form Assignment
Table Name: UD_LDAP_USR

Task Name: Description Updated
Task Description: Description field updated in the process form

Duration
Days:
Hours:
Minutes:

Task Properties
Conditional ☑
Disable Manual Insert □
Retry Period in Minutes:
Required for Completion □
Allow Cancellation while Pending ☑
Retry Count:
Constant Duration □
Allow Multiple Instances ☑
Off-line □
Task Effect: No Effect
Child Table:
Trigger Type:

27 Service Account Moved
28 System Validation

2. In the provisioning process, select the adapter name in the Handler Type section as follows:

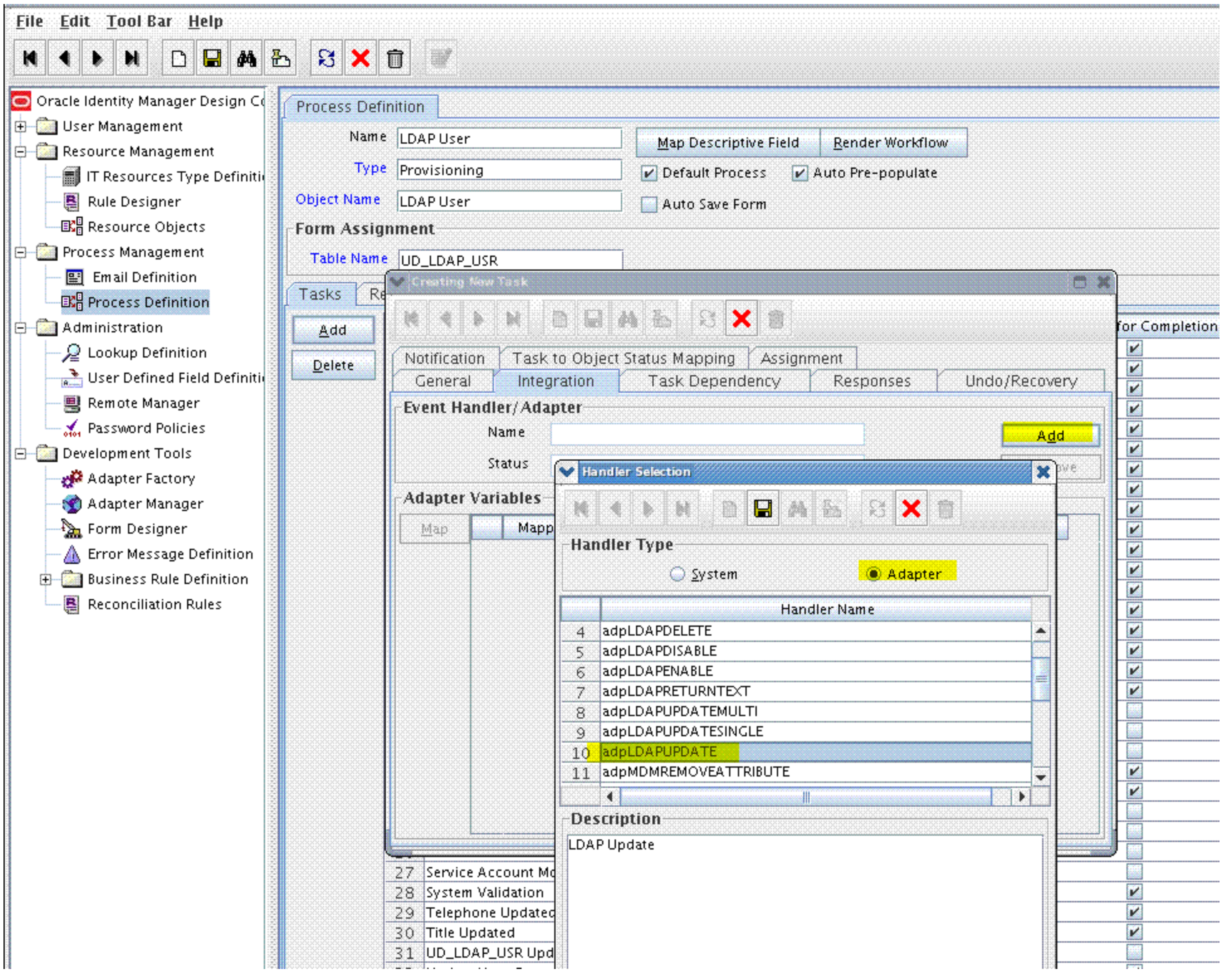
   a. Go to the Integration tab, and click **Add**.

   b. In the Handler Selection dialog box, select **Adapter**.

   c. From the Handler Name column, select **adpLDAPUPDATE** or **adpLDAPCHILDUPDATE**.

      For an eDirectory target, select **adpEDIRUPDATE** or **adpEDIRCHILDUPDATE**.

   d. Click **Save** and close the dialog box. For example:



Name: LDAP User

Type: Provisioning

Object Name: LDAP User

☑ Default Process ☑ Auto Pre-populate

□ Auto Save Form

Table Name: UD_LDAP_USR

Handler Type: ○ System ● Adapter

	Handler Name
4	adpLDAPDELETE
5	adpLDAPDISABLE
6	adpLDAPENABLE
7	adpLDAPRETURNTEXT
8	adpLDAPUPDATEMULTI
9	adpLDAPUPDATESINGLE
10	adpLDAPUPDATE
11	adpMDMREMOVEATTRIBUTE

Description: LDAP Update

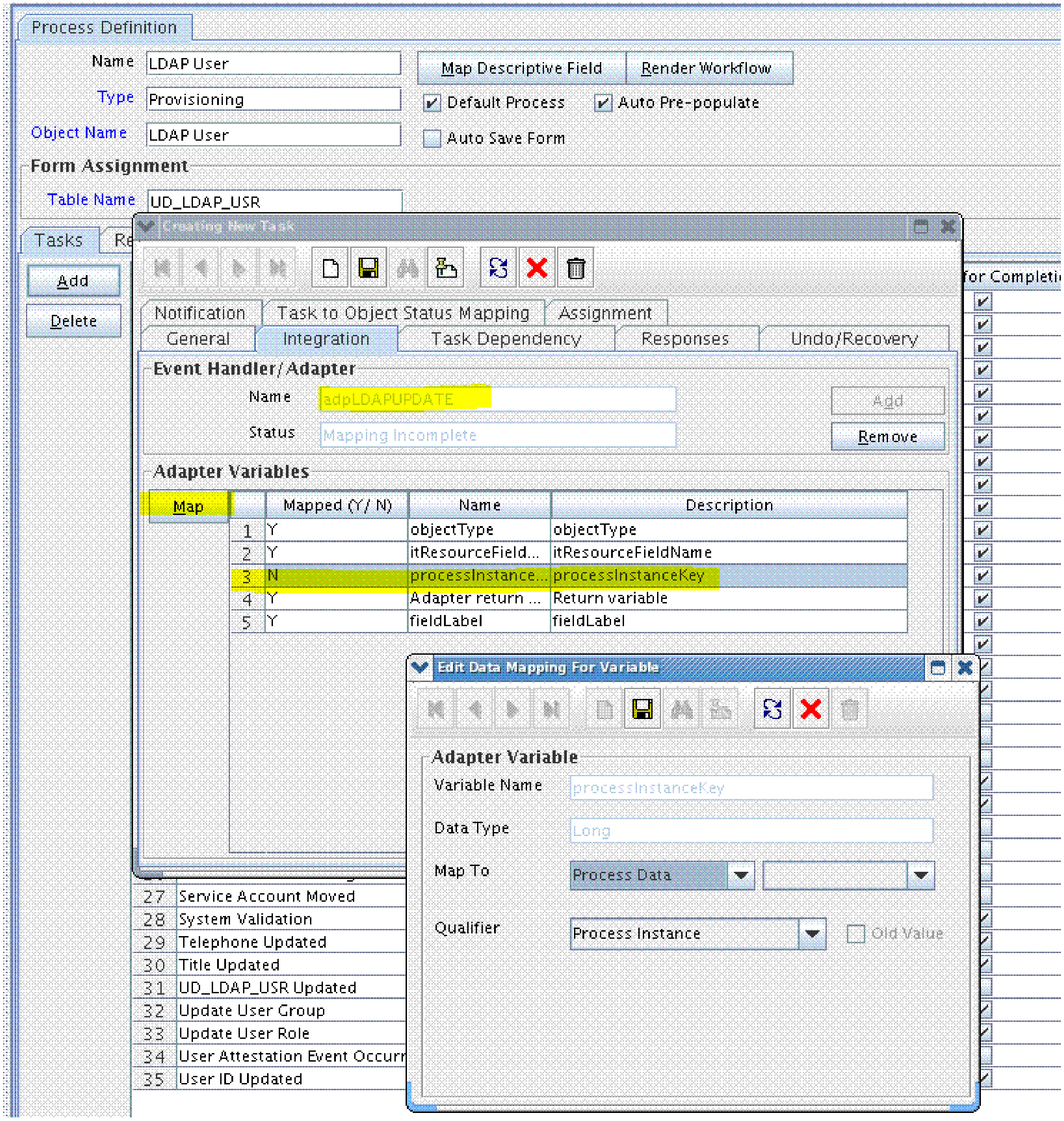
27	Service Account Mo
28	System Validation
29	Telephone Updated
30	Title Updated
31	UD_LDAP_USR Upd

3. In the Adapter Variables region, click the **procInstanceKey** variable.
4. In the dialog box that is displayed, create the following mapping:

   Variable Name: `procInstanceKey`

   Map To: `Process Data`

   Qualifier: `Process Instance`
5. Click **Save** and close the dialog box. For example:



Process Definition

Name: LDAP User

Type: Provisioning

Object Name: LDAP User

☑ Default Process ☑ Auto Pre-populate

☐ Auto Save Form

Form Assignment

Table Name: UD_LDAP_USR

Event Handler/ Adapter

Name: adpLDAPUPDATE

Status: Mapping Incomplete

Adapter Variables

	Mapped (Y/ N)	Name	Description
1	Y	objectType	objectType
2	Y	itResourceField...	itResourceFieldName
3	N	processInstance...	processInstanceKey
4	Y	Adapter return ...	Return variable
5	Y	fieldLabel	fieldLabel

27	Service Account Moved
28	System Validation
29	Telephone Updated
30	Title Updated
31	UD_LDAP_USR Updated
32	Update User Group
33	Update User Role
34	User Attestation Event Occurr
35	User ID Updated

Adapter Variable

Variable Name: processInstanceKey

Data Type: Long

Map To: Process Data

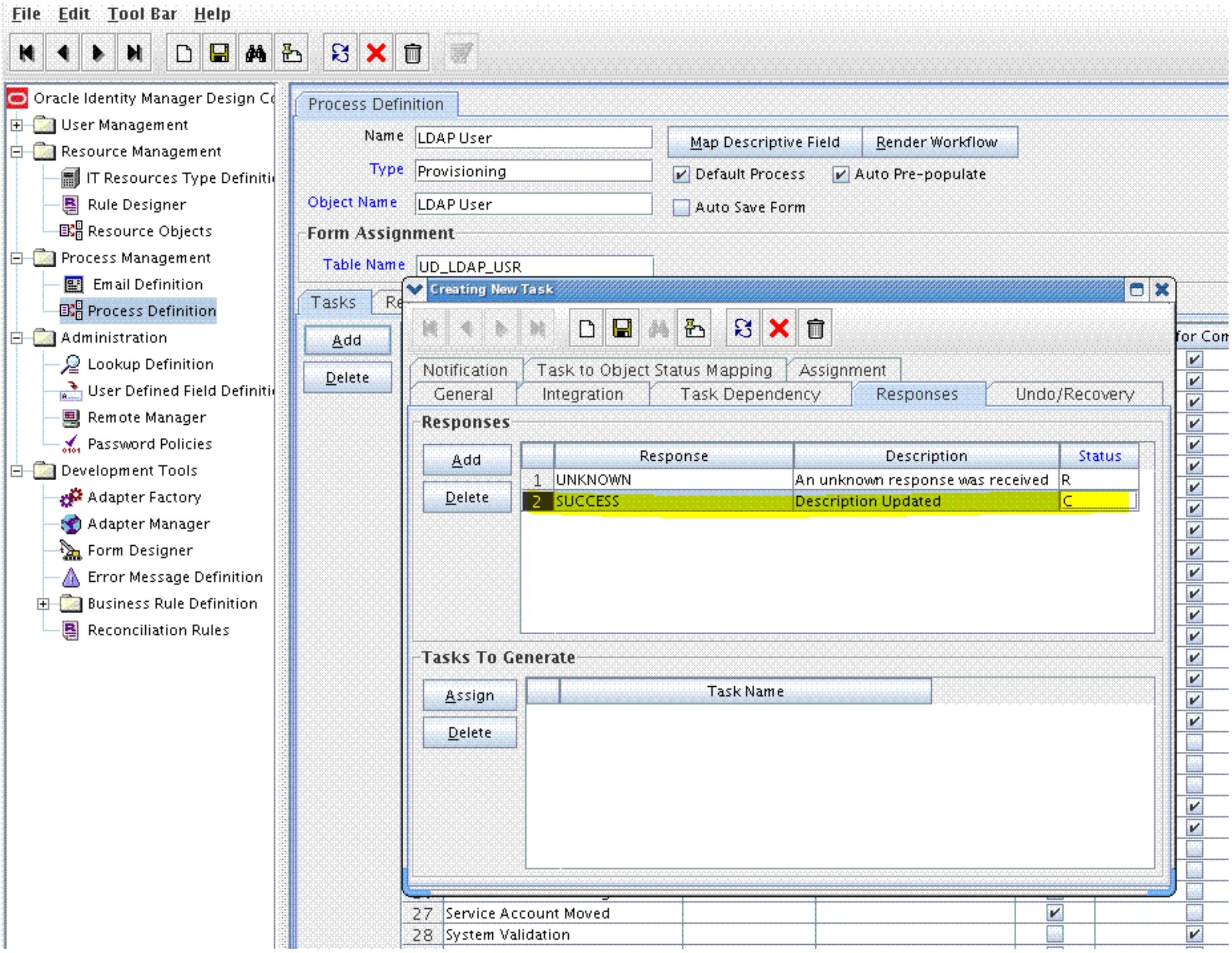
Qualifier: Process Instance ☐ Old Value

6. Repeat Steps 3 through 5 in Enabling Update Provisioning Operations on the Custom Field 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:

Variable	Map To	Qualifier	Literal Value
Adapter Return Variable	Response Code	NA	NA
processInstanceKey	Process Data	Process Instance	NA

Variable	Map To	Qualifier	Literal Value
itResourceName or itresourceFieldname for an OID target	Literal	String	UD_LDAP_USR_SERVER, UD_OID_USR_SERVER, or UD_EDIR_USR_SERVER
attrFieldName	Literal	String	Description
objectType	Literal	String	User

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



Name: LDAP User

Type: Provisioning

Object Name: LDAP User

☑ Default Process ☑ Auto Pre-populate

□ Auto Save Form

Table Name: UD_LDAP_USR

Responses

	Response	Description	Status
1	UNKNOWN	An unknown response was received	R
2	SUCCESS	Description Updated	C

	Task Name

27	Service Account Moved
28	System Validation

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

9.3.5 Updating the Request Dataset

> **Note:**
>
> Perform steps in this section and Running the PurgeCache Utility and Importing the Request Dataset Definition to MDS only if you want to perform request-based provisioning.

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

1. In a text editor, open the XML file located in the *OIM_HOME*/dataset/file directory for editing.
2. Add the AttributeReference element and specify values for the mandatory attributes of this element.

   For example, while performing the procedure in Adding the new Field to the Process Form, if you added Employee ID as an attribute on the process form, then enter the following line:

   ```
   <AttributeReference
   name = "Employee ID"
   attr-ref = "Employee ID"
   type = "String"
   widget = "text"
   length = "50"
   available-in-bulk = "false"/>
   ```

   In this AttributeReference element:

   - For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

     For example, if the employee ID is the value in the Name column of the process form, then you must specify `Employee ID` as the value of the name attribute in the AttributeReference element.
   - For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing Adding the new Field to the Process Form.
   - For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Adding the new Field to the Process Form.
   - For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Adding the new Field to the Process Form.
   - For the length attribute, enter the value that you entered in the Length column of the process form while performing Adding the new Field to the Process Form.
   - For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

While performing the steps in Adding the new Field to the Process Form, if you added more than one attribute on the process form, then repeat this step for each attribute added.

3. Save and close the XML file.

9.3.6 Running the PurgeCache Utility and Importing the Request Dataset Definition to MDS

Run the PurgeCache utility to clear content related to request datasets from the server cache.

See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about the PurgeCache utility.

Import into MDS, the request dataset definitions in XML format.

See Importing Request Datasets for detailed information about the procedure.

9.4 Adding New Multivalued Fields for Provisioning

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to add multivalued fields for provisioning.

To add new multivalued fields for provisioning, perform the following procedures:

- Creating an Entry for the Field in the Lookup Definition for Provisioning
- Adding the Task for Provisioning Multivalued Attributes in the Process Definition
- Updating the Request Dataset
- Running the PurgeCache Utility and Importing the Request Dataset Definition to MDS

> **Note:**
>
> Before starting the following procedure, perform the procedures described in Creating a Form for the Multivalued Field through Adding the New Multivalued Field to the Resource Object Reconciliation Fields. If these steps have been performed while adding new multivalued fields for target resource reconciliation, then you need not repeat the steps.

9.4.1 Creating an Entry for the Field in the Lookup Definition for Provisioning

Create an entry for the field in the lookup definition for provisioning as follows:

1. Log in to Oracle Identity Manager Design Console.

2. Expand **Administration** and double-click **Lookup Definition.**
3. Search for and open one of the lookup definitions, depending on your target system:
   - For a group field, open **Lookup.LDAP.Group.ProvAttrMap** or **Lookup.OID.Group.ProvAttrMap**
   - For a organizational unit field, open **Lookup.LDAP.OU.ProvAttrMap** or **Lookup.OID.OU.ProvAttrMap**
   - For a role field, open **Lookup.LDAP.Role.ProvAttrMap**
4. Click **Add** and then enter the Code Key and Decode values for the field. The Code Key and Decode values must be in the following format:

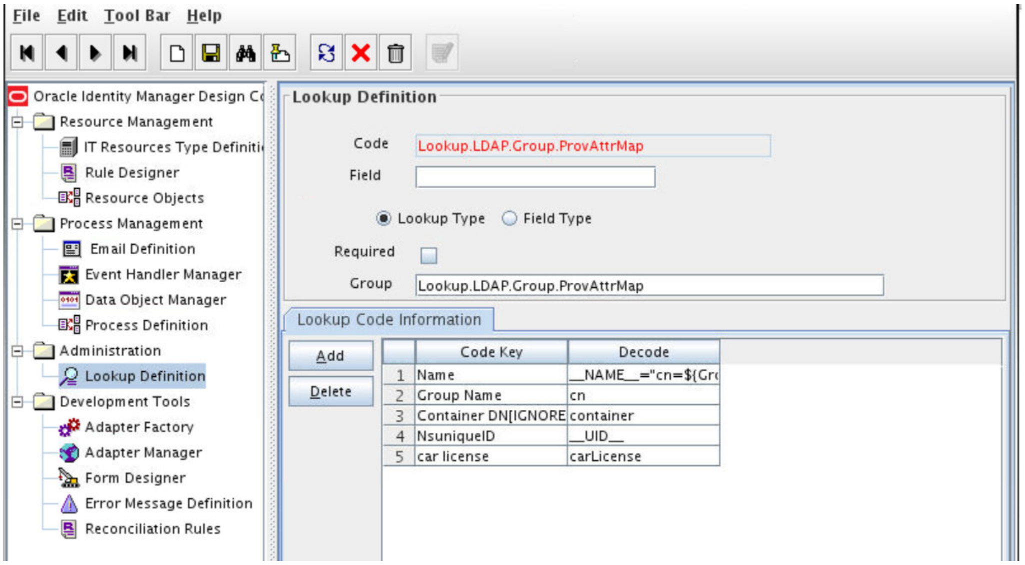
   Code Key: *CHILD_FORM_NAME~CHILD_FIELD_LABEL*

   In this format, *CHILD_FORM_NAME* specifies the name of the child form. *CHILD_FIELD_NAME* specifies the name of the field on the OIM User child form in the Administrative and User Console.

   Decode: Corresponding target system attribute

   > **Note:**
   >
   > For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the field names are case-sensitive.

   For example, enter `UD_CARLICEN~Car License` in the **Code Key** field and then enter `carLicense` in the **Decode** field.



Lookup Definition

Code: Lookup.LDAP.Group.ProvAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: Lookup.LDAP.Group.ProvAttrMap

Lookup Code Information

	Code Key	Decode
1	Name	__NAME__="cn=${Grc
2	Group Name	cn
3	Container DN[IGNORE	container
4	NsuniqueID	__UID__
5	car license	carLicense

9.4.2 Adding the Task for Provisioning Multivalued Attributes in the Process Definition

To add the task for provisioning multivalued attributes in the process definition, perform the following procedures:

- Updating the Process Definition
- Selecting the Adapter
- Creating the Adapter Variables Mapping
- Updating the Process Tasks

9.4.2.1 Updating the Process Definition

In the process definition, add the task for provisioning multivalued attributes as follows:

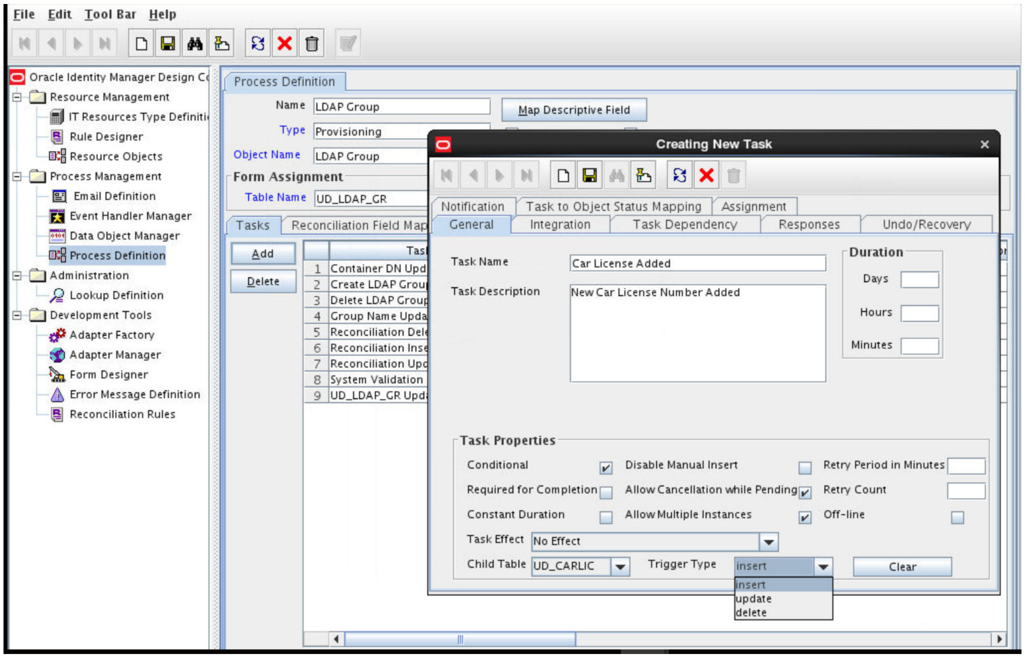
1. Expand **Process Management**.
2. Double-click **Process Definition**.
3. Search for and open one of the following process definitions:

   For groups: **LDAP Group** or **OID Group**

   For organizational units: **LDAP Organizational Unit** or **OID Organizational Unit**

   For roles: **LDAP Role**
4. Click **Add** and enter the task name and description. For example, enter `Car License Added` as the task name and task description.
5. In the Task Properties section, select the following:
   - Conditional
   - Allow cancellation while Pending
   - Allow Multiple Instances
   - **UD_CARLICEN**, to add the child table from the Child Table list
   - **Insert**, to add the data from the Trigger Type list

     For example:



Process Definition

Name: LDAP Group

Type: Provisioning

Object Name: LDAP Group

Form Assignment

Table Name: UD_LDAP_GR

	Task
1	Container DN Upd
2	Create LDAP Grou
3	Delete LDAP Group
4	Group Name Upda
5	Reconciliation Dele
6	Reconciliation Inse
7	Reconciliation Upc
8	System Validation
9	UD_LDAP_GR Upd

Creating New Task

Task Name: Car License Added

Task Description: New Car License Number Added

Duration: Days / Hours / Minutes

Task Properties

- Conditional ☑
- Required for Completion □
- Constant Duration □
- Disable Manual Insert □
- Allow Cancellation while Pending ☑
- Allow Multiple Instances ☑
- Retry Period in Minutes
- Retry Count
- Off-line □

Task Effect: No Effect

Child Table: UD_CARLIC

Trigger Type: insert (insert / update / delete)

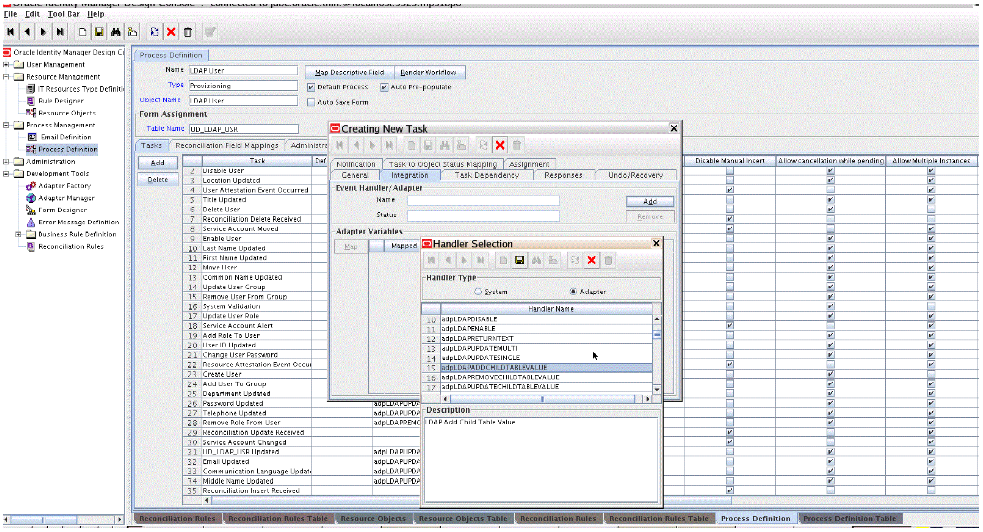
6. Click **Save**.

9.4.2.2 Selecting the Adapter

Select the adapter as follows:

1. On the Integration tab in the **LDAP User**, **OID User**, or **eDirectory User** provisioning process, click **Add** and then select **Adapter**.

   From the list of adapters, select **adpLDAPADDCHILDTABLEVALUE** or **adpOIDADDCHILDTABLEVALUE**.



Process Definition

Name: LDAP User

Type: Provisioning

Object Name: LDAP User

☑ Default Process ☑ Auto Pre-populate □ Auto Save Form

Form Assignment

Table Name: UD_LDAP_USR

Creating New Task

Event Handler/Adapter

Handler Selection

Handler Type: ○ System ● Adapter

	Handler Name
10	adpLDAPDISABLE
11	adpLDAPENABLE
12	adpLDAPRETURNTEXT
13	adpLDAPUPDATEMULTI
14	adpLDAPUPDATESINGLE
15	adpLDAPADDCHILDTABLEVALUE
16	adpLDAPREMOVECHILDTABLEVALUE
17	adpLDAPUPDATECHILDTABLEVALUE

Description: LDAP Add Child Table Value

2. Click **Save** and then close the dialog box.

9.4.2.3 Creating the Adapter Variables Mapping

Create the adapter variables mapping as follows:

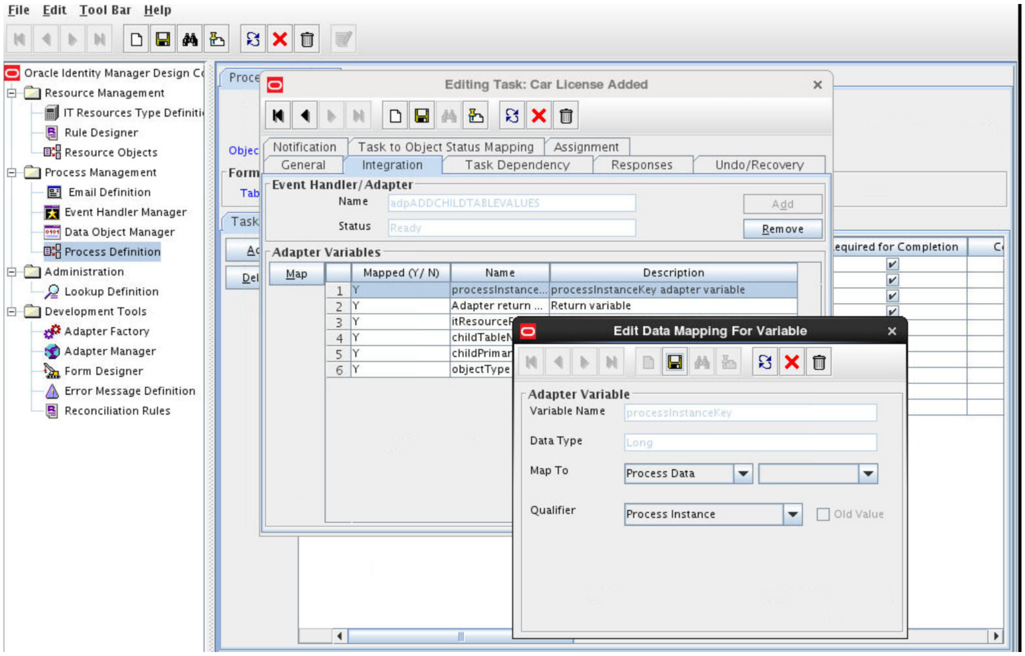
1. In the Adapter Variables region, click the **procInstanceKey** variable.
2. In the dialog box that is displayed, create the following mapping:

   Variable Name: `procInstanceKey`

   Map To: `Process Data`

   Qualifier: `Process Instance`

   For example:



Editing Task: Car License Added

Event Handler/Adapter
Name: adpADDCHILDTABLEVALUES
Status: Ready

Adapter Variables

	Mapped (Y/ N)	Name	Description
1	Y	processInstance...	processInstanceKey adapter variable
2	Y	Adapter return ...	Return variable
3	Y	itResourceN	
4	Y	childTableN	
5	Y	childPrimar	
6	Y	objectType	

Edit Data Mapping For Variable

Adapter Variable
Variable Name: processInstanceKey
Data Type: Long
Map To: Process Data
Qualifier: Process Instance

3. Click **Save** and close the dialog box.
4. Perform one of the following steps:

   For users:

   Repeat Steps 1 through 3 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:

Variable	Map To	Qualifier	Literal Value
processInstanceKey	Process Data	Process Instance	NA
Adapter Return Variable	Response Code	NA	NA
itResourceName	Literal	String	UD_LDAP_USR_SERVER, UD_OID_USR_SERVER, or UD_EDIR_USR_SERVER
childTableName	Literal	String	UD_CARLICEN
objectType	Literal	String	User
childPrimarykey	Process Data (Child Table description)	Child Primary Key	NA

   For groups:

Repeat Steps 1 through 3 for all the variables listed in the following table. This table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

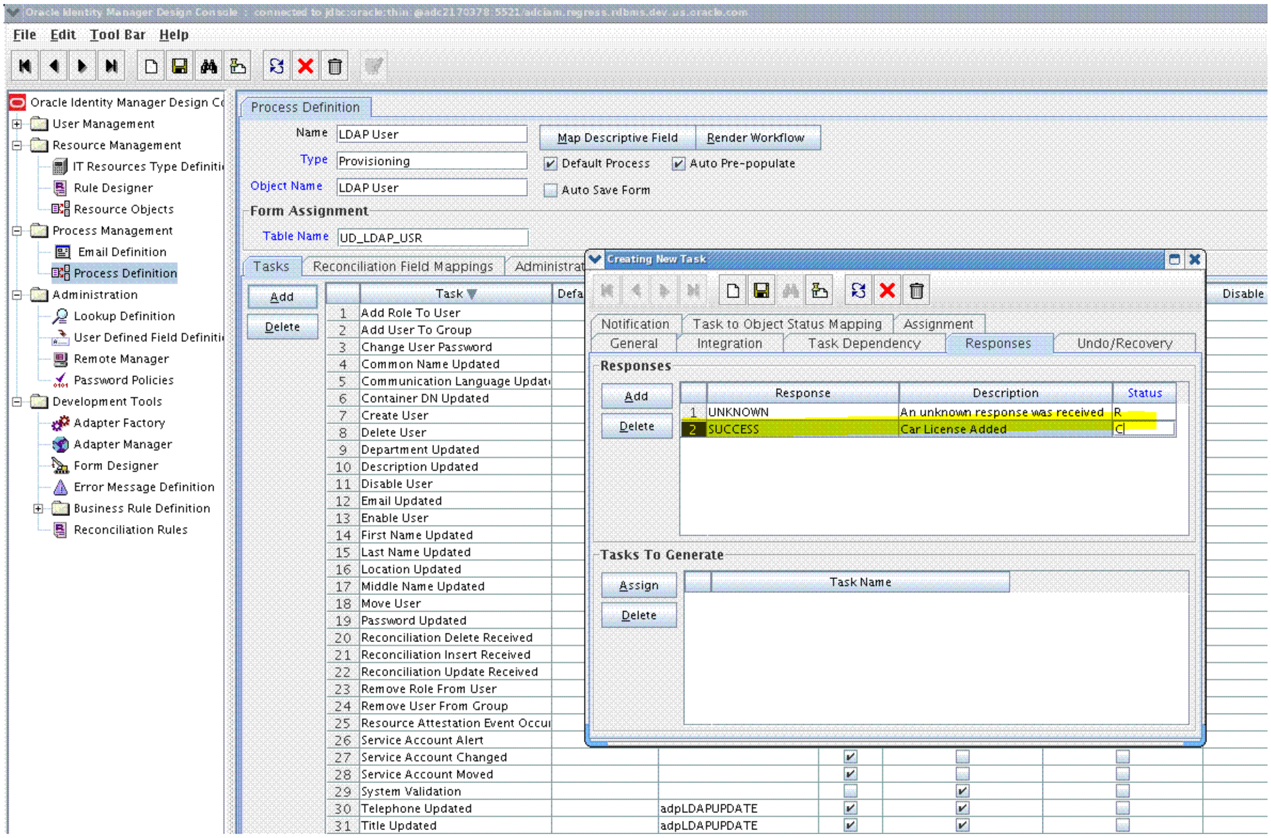
Variable	Map To	Qualifier	Literal Value
procInstanceKey	Process Data	Process Instance	NA
Adapter Return Variable	Response Code	NA	NA
itResourceName	Literal	String	UD_LDAP_USR_SERVER, UD_OID_USR_SERVER, or UD_EDIR_USR_SERVER
childTableName	Literal	String	UD_*CHILD_PROCESS_FORM_NAME*
objectType	Literal	String	Group
childPrimarykey	Process Data (Child Table description)	Child Primary Key	NA

For organizational units:

Repeat Steps 1 through 3 for all the variables listed in the following table. This table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

Variable	Map To	Qualifier	Literal Value
procInstanceKey	Process Data	Process Instance	NA
Adapter Return Variable	Response Code	NA	NA
itResourceName	Literal	String	UD_LDAP_USR_SERVER, UD_OID_USR_SERVER, or UD_EDIR_USR_SERVER
childTableName	Literal	String	UD_*CHILD_PROCESS_FORM_NAME*
objectType	Literal	String	OU
childPrimarykey	Process Data (Child Table description)	Child Primary Key	NA

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



Name: LDAP User

Type: Provisioning

Object Name: LDAP User

☑ Default Process ☑ Auto Pre-populate

□ Auto Save Form

Form Assignment

Table Name: UD_LDAP_USR

Responses

	Response	Description	Status
1	UNKNOWN	An unknown response was received	R
2	SUCCESS	Car License Added	C

Tasks To Generate

	Task Name

	Task	Defa					Disable
1	Add Role To User						
2	Add User To Group						
3	Change User Password						
4	Common Name Updated						
5	Communication Language Updat						
6	Container DN Updated						
7	Create User						
8	Delete User						
9	Department Updated						
10	Description Updated						
11	Disable User						
12	Email Updated						
13	Enable User						
14	First Name Updated						
15	Last Name Updated						
16	Location Updated						
17	Middle Name Updated						
18	Move User						
19	Password Updated						
20	Reconciliation Delete Received						
21	Reconciliation Insert Received						
22	Reconciliation Update Received						
23	Remove Role From User						
24	Remove User From Group						
25	Resource Attestation Event Occu						
26	Service Account Alert						
27	Service Account Changed			☑	□	□	
28	Service Account Moved			☑	□	□	
29	System Validation			□	☑	□	
30	Telephone Updated		adpLDAPUPDATE	☑	☑	□	
31	Title Updated		adpLDAPUPDATE	☑	☑	□	

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

9.4.2.4 Updating the Process Tasks

Update the process tasks as follows:

1. Add the Car License Update process task by performing the procedures described in Updating the Process Definition through Creating the Adapter Variables Mapping with the following difference:

   - While performing Step 5 of Updating the Process Definition, instead of selecting **UD_CARLICEN** from the Child Table list, select **UD_CARLICN**. Similarly, instead of selecting **Insert** from the Trigger Type list, select **Update**.
   - While performing Step 4 of Creating the Adapter Variables Mapping, the childPrimarykey variable will not appear. Instead, map the following variable with its respective values in addition to the other variables:

Variable	Map To	Qualifier	Literal Value
taskInstanceKey	Task Information	Task Instance Key	NA

2. Add the Car License Delete process task by performing the procedures described in Updating the Process Definition through Creating the Adapter Variables Mapping with the following difference:

   - While performing Step 5 of Updating the Process Definition, instead of selecting **UD_CARLICEN** from the Child Table list, select **UD_CARLICN**. Similarly, instead of selecting **Insert** from the Trigger Type list, select **Delete**.

- While performing Step 4 of Creating the Adapter Variables Mapping, the childPrimarykey variable will not appear. Instead, map the following variable with its respective values in addition to the other variables:

Variable	Map To	Qualifier	Literal Value
taskInstanceKey	Task Information	Task Instance Key	NA

3. Click **Save** on Process Task.

> **Note:**
>
> During a provisioning operation, you can either add or remove values of multivalued fields. You cannot update these values.

9.4.3 Updating the Request Dataset

Update the request dataset.

> **Note:**
>
> Perform the steps in this section and Running the PurgeCache Utility and Importing the Request Dataset Definition to MDS only if you enabled request-based provisioning.

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

1. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.
2. Add the AttributeReference element and specify values for the mandatory attributes of this element.

   For example, if you added Car License as an attribute on the process form, then enter the following line:

   ```
   <AttributeReference
   name = "Car License"
   attr-ref = "Car License"
   type = "String"
   widget = "text"
   length = "50"
   available-in-bulk = "false"/>
   ```

   In this AttributeReference element:

   - For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

     For example, if UD_CAR_LICENSE is the value in the Name column of the process form, then you must specify `Car License` as the value of the name attribute in the AttributeReference element.

- For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form.
- For the type attribute, enter the value that you entered in the Variant Type column of the process form.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form.
- For the length attribute, enter the value that you entered in the Length column of the process form.
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

If you add more than one attribute on the process form, then repeat this step for each attribute added.

3. Save and close the XML file.

9.4.4 Running the PurgeCache Utility and Importing the Request Dataset Definition to MDS

Run the PurgeCache utility to clear content related to request datasets from the server cache.

See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Governance* for more information about the PurgeCache utility.

Import into MDS the request dataset definitions in XML format.

9.5 Adding New Fields for Trusted Source Reconciliation

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to add new fields for trusted source reconciliation.

By default, the attributes listed in Table 1-33 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new fields for trusted source reconciliation. To do so, perform the following procedures:

- Adding the New Field on the OIM User Process Form
- Adding the New Field to the Resource Object Reconciliation Fields
- Creating a Reconciliation Field Mapping
- Creating an Entry for the Field in the Lookup Definition for Reconciliation

9.5.1 Adding the New Field on the OIM User Process Form

To add the new field to the OIM User process form:

1. Log in to Oracle Identity Manager Design Console.

2. If you are using a release prior to Oracle Identity Manager release 11.1.1.5.3, then add the new field on the OIM User process form as follows:
   a. Expand **Administration**.
   b. Double-click **User Defined Field Definition**.
   c. Search for and open the **Users** form.
   d. Click **Add** and enter the details of the field.

      For example, if you are adding the Employee ID field, then enter `Employee ID` in the **Name** field, set the data type to **String**, enter `USR_UDF_EMPLOYEE_ID` as the column name, and enter a field size value.
   e. Click **Save**.
3. If you are using Oracle Identity Manager release 11.1.1.5.3, then add the new field on the OIM User process form by using the Oracle Identity Advanced Administration interface.
4. If you are using Oracle Identity Manager release 11.1.2 or later, then add the new field on the OIM User process form by performing the procedure described in Configuring Custom Attributes of *Oracle Fusion Middleware Administering Oracle Identity Manager.*

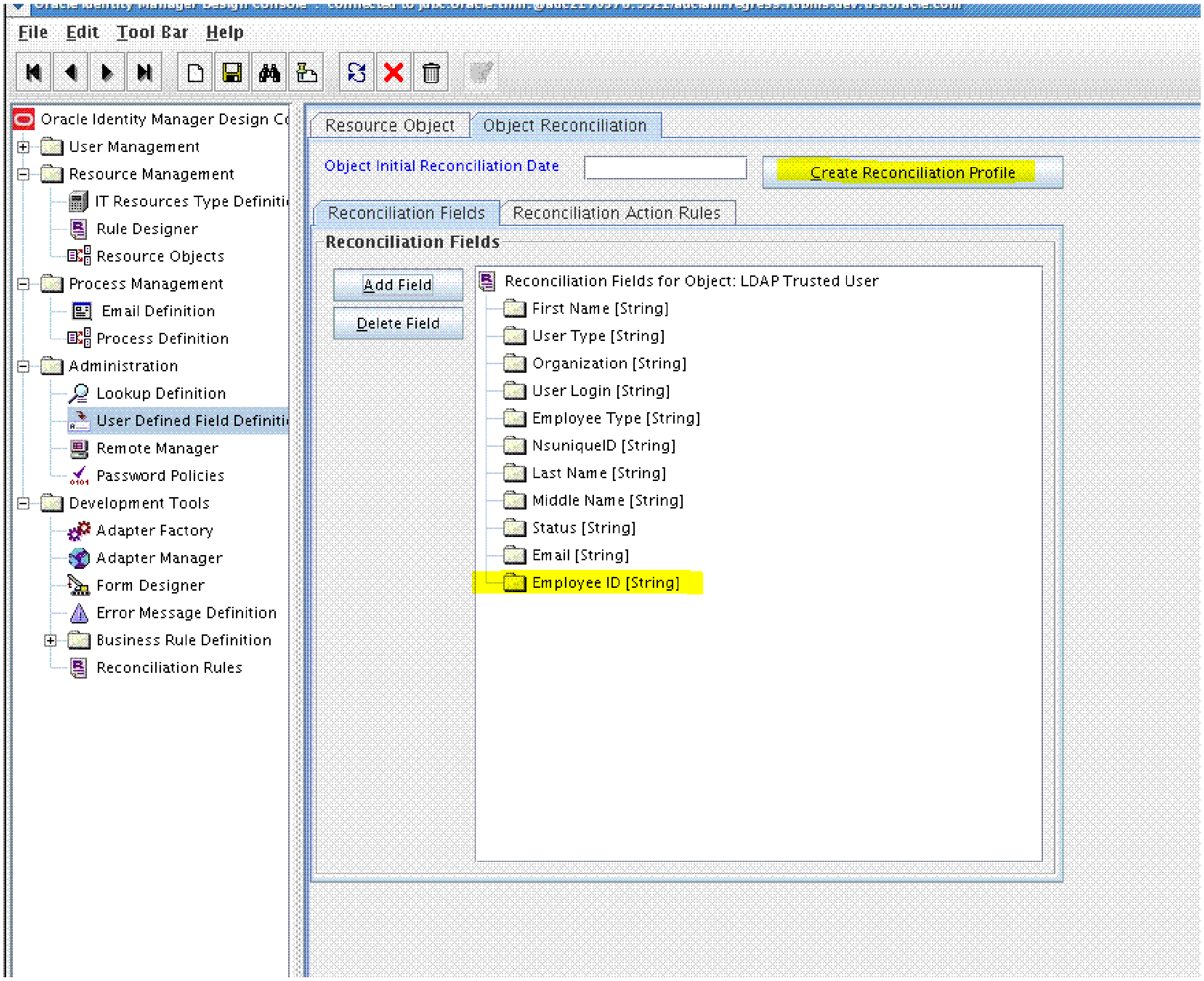
9.5.2 Adding the New Field to the Resource Object Reconciliation Fields

Add the new field to the list of reconciliation fields in the resource object as follows:

1. Expand the **Resource Management** folder.
2. Double-click **Resource Objects**.
3. Search for and open the **LDAP Trusted User** or **OID Trusted User** resource object.
4. On the Object Reconciliation tab, click **Add Field**.
5. Enter the details of the field and click **Save**.

   For example, enter `Employee ID` in the **Field Name** field and select **String** from the Field Type list.

   Later in this procedure, you will enter the field name as the Decode value of the entry that you create in the lookup definition for reconciliation.
6. Click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS. For example:

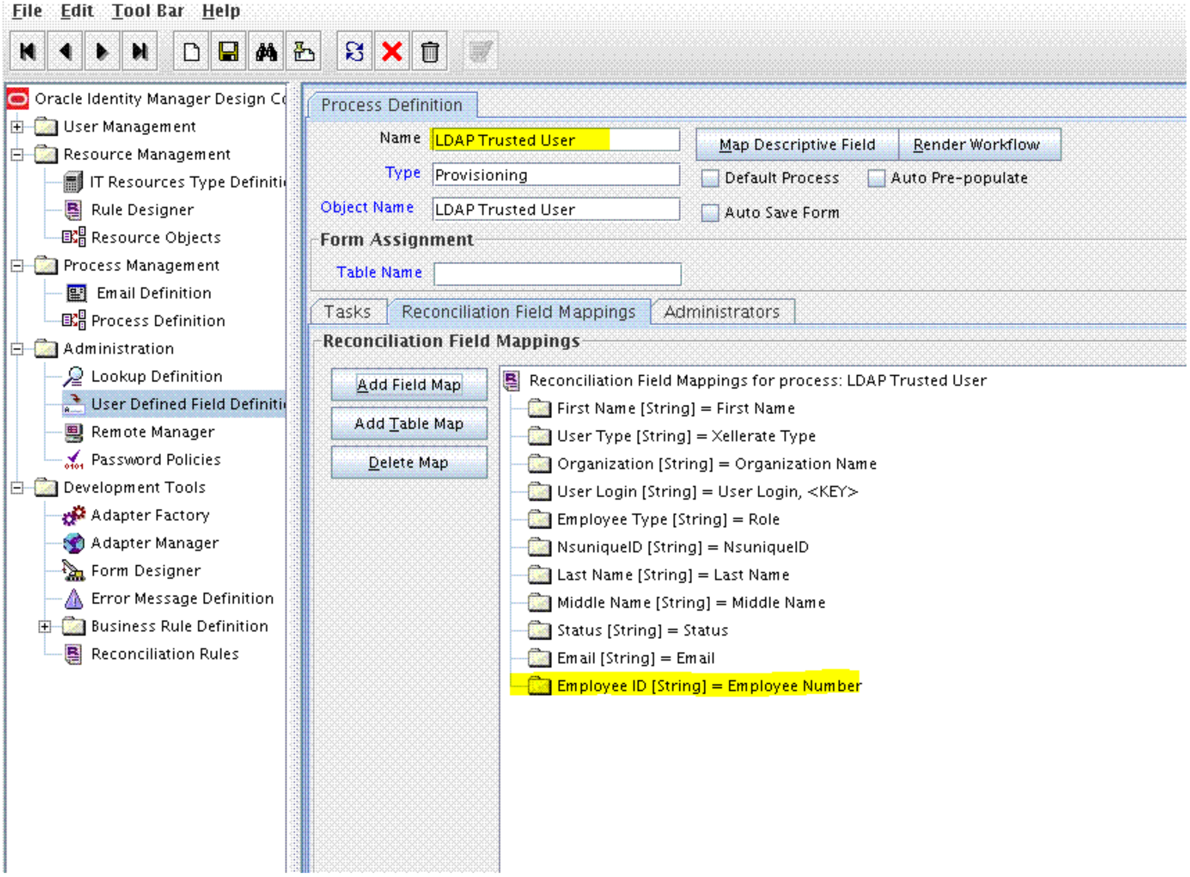


9.5.3 Creating a Reconciliation Field Mapping

Create a reconciliation field mapping for the new field as follows:

1. Expand **Process Management**.
2. Double-click **Process Definition**.
3. Search for and open the **LDAP Trusted User** or **OID Trusted User** process definition.
4. On the Reconciliation Field Mappings tab, click **Add Field Map**.
5. In the **Field Name** field, select the value for the field that you want to add.

   For example, select **Employee ID = Employee ID**. For example:



Name: LDAP Trusted User

Type: Provisioning

Object Name: LDAP Trusted User

Table Name:

☐ Default Process ☐ Auto Pre-populate

☐ Auto Save Form

Reconciliation Field Mappings

Reconciliation Field Mappings for process: LDAP Trusted User
- First Name [String] = First Name
- User Type [String] = Xellerate Type
- Organization [String] = Organization Name
- User Login [String] = User Login, <KEY>
- Employee Type [String] = Role
- NsuniqueID [String] = NsuniqueID
- Last Name [String] = Last Name
- Middle Name [String] = Middle Name
- Status [String] = Status
- Email [String] = Email
- Employee ID [String] = Employee Number

6. Click **Save**.

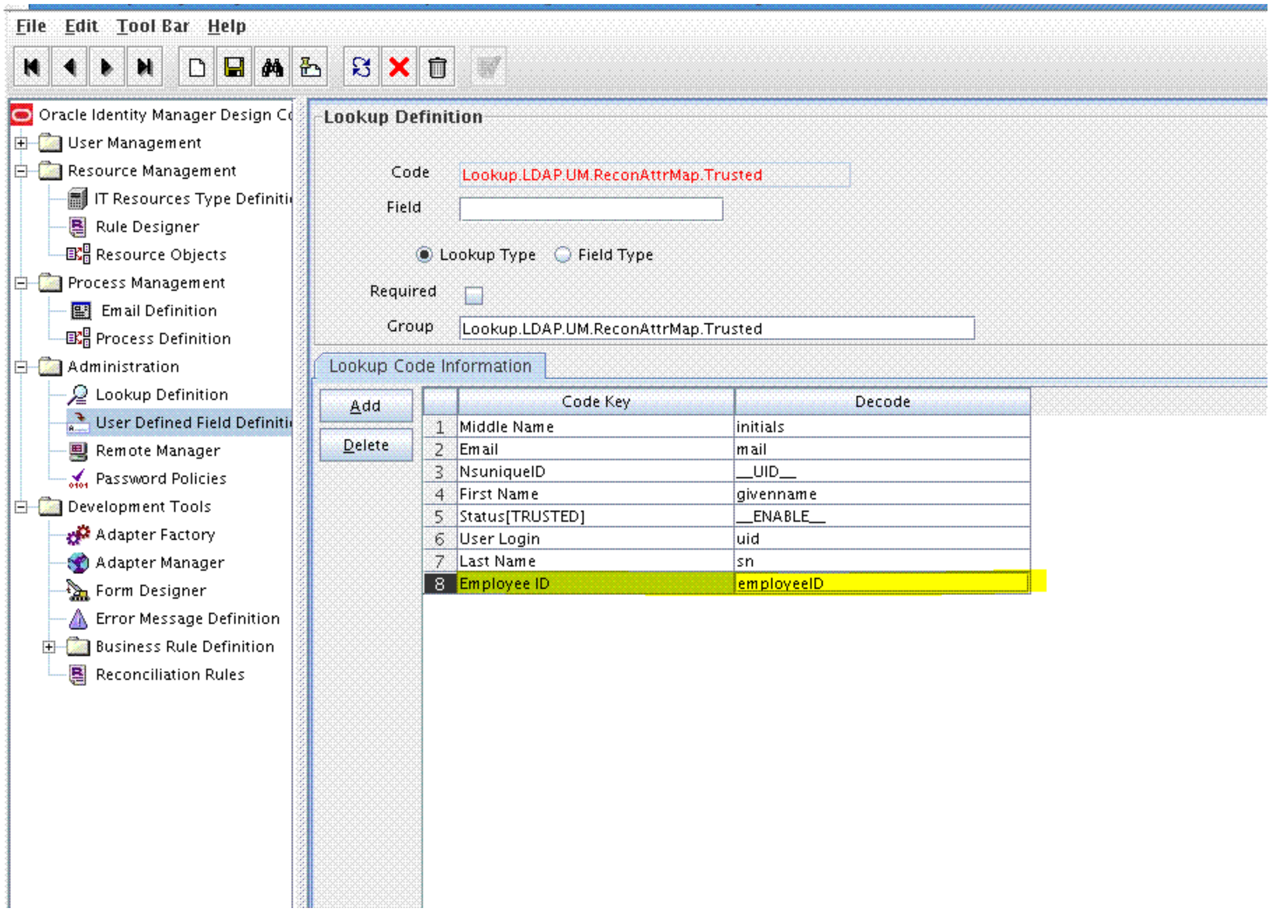
9.5.4 Creating an Entry for the Field in the Lookup Definition for Reconciliation

Create an entry for the field in the lookup definition for reconciliation as follows:

1. Expand **Administration** and then double-click **Lookup Definition.**
2. Search for and open the **Lookup.LDAP.UM.ReconAttrMap.Trusted**, **Lookup.OID.UM.ReconAttrMap.Trusted**, or **LookupEDIR.UM.ReconAttrMap.Trusted** lookup definition.
3. Click **Add** and then enter the Code Key and Decode values for the field. The Code Key value must be the name of the field created in the **LDAP Trusted User**, **OID Trusted User**, or **eDirectory User Trusted** resource object. The Decode value is the name of the corresponding field on the target system.

> **Note:**
>
> For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the field names are case-sensitive.

For example, enter `employee ID` in the Code Key field and then enter `EmployeeID` in the Decode field.



Code: Lookup.LDAP.UM.ReconAttrMap.Trusted

Field:

● Lookup Type ○ Field Type

Required □

Group: Lookup.LDAP.UM.ReconAttrMap.Trusted

	Code Key	Decode
1	Middle Name	initials
2	Email	mail
3	NsuniqueID	__UID__
4	First Name	givenname
5	Status[TRUSTED]	__ENABLE__
6	User Login	uid
7	Last Name	sn
8	Employee ID	employeeID

4. Click **Save**.
5. Select **Field Type** and click **Save**.

9.6 Configuring Transformation of Data During Reconciliation

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to configure transformation of data during reconciliation.

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

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

1. Write code that implements the required transformation logic in a Java class with a fully qualified domain name (FQDN), such as `com.transformationexample.MyTransformer`.

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

```
package com.transformationexample;

import java.util.HashMap;


public class MyTransformer {
    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 sFirstName = (String) hmUserDetails.get("First Name");
        String sLastName = (String) hmUserDetails.get("Last Name");
        return sFirstName + "." + sLastName;

    }
}
```

2. Log in to the Design Console.
3. Create a new lookup definition named **Lookup.LDAP.UM.ReconTransformation**, **Lookup.OID.UM.ReconTransformation**, or **Lookup.EDIR.UM.ReconTransformation**.
4. In the **Code Key** column, enter the resource object field name you want to transform. For example, `givenName`.
5. In the **Decode** column, enter the class name. For example, `com.transformationexample.MyTransformer`.
6. Save the changes to the lookup definition.
7. Search for and open the **Lookup.LDAP.UM.Configuration** or **Lookup.OID.UM.Configuration** lookup definition.
8. In the **Code Key** column, enter **Recon Transformation Lookup**.
9. In the **Decode** column, enter **Lookup.LDAP.UM.ReconTransformation** or **Lookup.OID.UM.ReconTransformation**.
10. Save the changes to the lookup definition.
11. Create a JAR with the class and upload it to the Oracle Identity Manager database as follows:

    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.

12. Run the PurgeCache utility to clear content related to request datasets from the server cache.

13. Perform reconciliation to verify transformation of the field, for example, SimpleDisplayName.

9.7 Configuring Validation of Data During Reconciliation and Provisioning

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to configure 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 First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class with a fully qualified domain name (FQDN), such as `com.validationexample.MyValidator`.

   This validation class must implement the validate method. The following sample validation class checks if the value in the First Name attribute contains the number sign (#):

   ```
   package com.validationexample;

   import java.util.HashMap;

   public class MyValidator {
       public boolean validate(HashMap hmUserDetails, HashMap hmEntitlementDetails,
   ```

```
String sField) throws ConnectorException {

        /* 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.
                 */
                 * The transform method can throw

*oracle.iam.connectors.icfcommon.extension.ValidationException
                 * in case the validation fails.
                 */
        /*
        * In this sample code, the value "false" is returned if the field
        * contains the number sign (#). Otherwise, the value "true" is
        * returned.
        */
        boolean valid = true;
        String sFirstName = (String) hmUserDetails.get(sField);
        for (int i = 0; i < sFirstName.length(); i++) {
            if (sFirstName.charAt(i) == '#') {
                valid = false;
                break;
            }
        }
        return valid;

    }
}
```

2. Log in to the Design Console.
3. Create one of the following new lookup definitions:
   - To configure validation of data for reconciliation:

     `Lookup.LDAP.UM.ReconValidation` or `Lookup.OID.UM.ReconValidation`
   - To configure validation of data for provisioning:

     `Lookup.LDAP.UM.ProvValidation` or `Lookup.OID.UM.ProvValidation`
4. In the **Code Key** column, enter the resource object field name that you want to validate. For example, `givenName`.
5. In the **Decode** column, enter the class name. For example, `com.validationexample.MyValidator`.
6. Save the changes to the lookup definition.
7. Search for and open the **Lookup.LDAP.UM.Configuration** or **Lookup.OID.UM.Configuration** lookup definition.
8. In the **Code Key** column, enter one of the following entries:
   - To configure validation of data for reconciliation:

     `Recon Validation Lookup`
   - To configure validation of data for provisioning:

     `Provisioning Validation Lookup`

9. In the **Decode** column, enter one of the following entries:
   - To configure validation of data for reconciliation:

     `Lookup.LDAP.UM.ReconValidation` or `Lookup.OID.UM.ReconValidation`
   - To configure validation of data for provisioning:

     `Lookup.LDAP.UM.ProvValidation` or `Lookup.OID.UM.ProvValidation`
10. Save the changes to the lookup definition.
11. Create a JAR with the class and upload it to the Oracle Identity Manager database as follows:

    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.
12. Run the PurgeCache utility to clear content related to request datasets from the server cache.
13. Perform reconciliation or provisioning to verify validation for the field, for example, SimpleDisplayName.

9.8 Configuring the Connector for User-Defined Object Classes

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to configure the connector for user-defined object classes.

To configure the connector for user-defined object classes:

1. Create the object class and assign mandatory and optional attributes to the object class.

   Refer to the target system documentation for information about creating the object class.

> **Note:**
>
> Assign the user object class as the parent of the object class that you create.

2. Refresh the schema.
3. To add the mandatory and optional attributes of the object class for provisioning, perform the procedure described in Adding Custom Fields for Provisioning.
4. In the configuration lookup definition for the target system:
   - Change the decode value of the **ObjectClass** code key value to include the new object class name.
   - Set the **readSchema** parameter to true.

     The lookup names can be Lookup.LDAP.Configuration, Lookup.LDAP.OUD.Configuration, or Lookup.OID.Configuration.

9.9 Configuring the Connector to Use Custom Object Classes

If you want to use a custom object class, you need to perform the following procedure. Note that the procedure in this section has been described by using User object class as an example.

1. Modify the **LDAP User** process definition as follows:
   a. Log in to the Design Console.
   b. Expand **Process Management** and then double-click **Process Definition.**
   c. Search for and open the **LDAP User** process definition.
   d. On the Tasks tab, double-click the **Create LDAP User** process task.
   e. Change the value of the objectType adapter variable, to the name of the custom object class.
   f. Click **Save**
   g. Repeat steps 'd' through 'g' to edit and update each of the process tasks associated with the User object class. For example, Delete LDAP User and UD_LDAP_USR Updated.
2. Before you run any of the following scheduled jobs, set the value of the Object Type attribute of the scheduled jobs to the custom object class value:
   - LDAP Connector User Search Delete Reconciliation
   - LDAP Connector User Search Reconciliation
   - LDAP Connector User Sync Reconciliation
   - LDAP Connector Trusted User Reconciliation
   - LDAP Connector Trusted User Delete Reconciliation

9.10 Configuring the Connector for Multiple Trusted Source Reconciliation

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to configure the connector for multiple trusted source reconciliation.

The following are examples of scenarios in which there is more than one trusted source for user data in an organization:

- One of the target systems is a trusted source for data about employees. The second target system is a trusted source for data about contractors. The third target system is a trusted source for data about interns.
- One target system holds the data of some of the identity fields that constitute an OIM User. Two other systems hold data for the remaining identity fields. In other words, to create an OIM User, data from all three systems would need to be reconciled.

If the operating environment of your organization is similar to that described in either one of these scenarios, then this connector enables you to use the target system as one of the trusted sources of user data in your organization.

9.11 Configuring the Connector to Support POSIX Groups and Accounts

This procedure allows the connector to support POSIX groups (posixGroups) and POSIX accounts (posixAccounts).

After you complete this configuration:

- The connector will support POSIX groups.
- The sync reconciliation operation will not return the POSIX group membership changes. You must use the full search reconciliation task to get these changes.

To configure the connector to support POSIX groups and accounts:

1. Log in to Oracle Identity Manager Design Console.
2. Modify the **Lookup.LDAP.Configuration**, **Lookup.LDAP.OUD.Configuration**, or **Lookup.OID.Configuration** lookup definition as follows:
   a. Set **maintainPosixGroupMembership** to true.
   b. For **accountObjectClasses**, add "posixGroup","posixAccount".
   c. For **objectClassesToSynchronize**, add "posixGroup","posixAccount".
   d. Set **groupObjectClasses** to "top", "posixGroup".
   e. Set **readSchema** to true.

3. In the **Lookup.LDAP.UM.ProvAttrMap** and **Lookup.LDAP.UM.ReconAttrMap** lookup definitions, replace "ldapGroups" with "posixGroups".

   For OID, update the **Lookup.OID.UM.ProvAttrMap** and **Lookup.OID.UM.ReconAttrMap** lookup definitions.

   For eDirectory, update the **Lookup.EDIR.UM.ProvAttrMap** and **Lookup.EDIR.UM.ReconAttrMap** lookup definitions.

4. In the **Lookup.LDAP.Group.ProvAttrMap** and **Lookup.LDAP.Group.ReconAttrMap** lookup definitions, add the following mapping as a String:

   GID NUMBER to gidNumber

   For OID, update the **Lookup.OID.Group.ProvAttrMap** and **Lookup.OID.Group.ReconAttrMap** lookup definitions.

   For OID, update the **Lookup.EDIR.Group.ProvAttrMap** and **Lookup.EDIR.Group.ReconAttrMap** lookup definitions.

5. In the **LDAP Group**, **OID Group**, or **eDirectory Group** resource object, add the GID NUMBER field as follows:

   Select the group (**LDAP Group**, **OID Group**, or **eDirectory Group**), **Object Reconciliation**, **Add Field**, and then add GID NUMBER.

6. In the **LDAP Group**, **OID Group**, or **eDirectory Group** process form, add the GID NUMBER field.

7. In the **LDAP Group**, **OID Group**, or **eDirectory Group** process definition, add the mapping as a String for GID Number.

8. In the **Lookup.LDAP.UM.ProvAttrMap** and **Lookup.LDAP.UM.ReconAttrMap** lookup definitions, add the following mappings as Strings:

   - GID NUMBER to gidNumber
   - UID NUMBER to uidNumber
   - HOME DIRECTORY to homedirectory

   For OID, update the **Lookup.OID.UM.ProvAttrMap** and **Lookup.OID.UM.ReconAttrMap** lookup definitions.

   For eDirectory, update the **Lookup.EDIR.UM.ProvAttrMap** and **Lookup.EDIR.UM.ReconAttrMap** lookup definitions.

9. In the **LDAP User**, **OID User**, or **eDirectory User** resource object, add mappings as Strings for these fields:

   - GID NUMBER
   - UID NUMBER
   - HOME DIRECTORY

10. In the **LDAP User**, **OID User**, or **eDirectory User** process form, add mappings as Strings for these fields:

    - GID NUMBER
    - UID NUMBER
    - HOME DIRECTORY

11. In the **LDAP User**, **OID User**, or **eDirectory User** process definition, add mappings as Strings for these fields:

- GID NUMBER
- UID NUMBER
- HOME DIRECTORY

12. After you are finished, click **Create Reconciliation Profile**.

9.12 Configuring the Connector to Support Provisioning of Custom Object Classes while Provisioning Organizational Unit

Provisioning of custom object-classes while provisioning Organizational Unit (OU) to target systems is supported. In order to change the object classes used for OU, you need to add the Key OU ObjectClasses in the appropriate lookup definitions.

This section contains the following topics:

- Modifying the Configuration Lookup Definition
- About Adding Custom Object Classes

9.12.1 Modifying the Configuration Lookup Definition

In the Design Console, modify the configuration lookup definition by performing the following procedure:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Administratio**n and double-click **Lookup Definition.**
3. Depending on the target system you are using, search for and open one of the following lookup definitions:
    - For ODSEE or OUD: **Lookup.LDAP.Configuration**
    - For OID: **Lookup.OID.Configuration**
    - For eDirectory: **Lookup.EDIR.Configuration**
4. Click **Add.**

    A new row is added.
5. In the Code Key column, enter `ouObjectClasses`.
6. In the Decode column, enter the name of the custom object class.

    For example, `top`, `organizationalUnit`, `custom ObjectClass 1`, or `custom ObjectClass 2`.
7. Click **Save.**

9.12.2 About Adding Custom Object Classes

If you are adding custom object classes, then the scheduled task (LDAP Connector OU Lookup Reconciliation) used to reconcile the OU container lookup populates those OUs that have the objectClasses specified as the decode value of the ouObjectClasses code key in the configuration lookup definition.

However, the scheduled task (LDAP Connector OU Lookup Reconciliation) does not update the lookup if the OU container in LDAP does not have the custom objectclass associated with it. To reconcile the default OU container loopkup, enter `organizationalUnit` as the value of the Object Type parameter in the LDAP Connector OU Lookup Reconciliation scheduled job. This will populate the lookup with all the OUs. This because, the default ObjectClass for OU is organizationalUnit.

Similar behavior is observed with the scheduled task LDAP/OID/eDirectory OU search reconciliation operation and synchronized reconciliation operation. These operations will fetch those OUs having objectClasses provided in decode key of the ouObjectClasses.

In order to get the default behavior, you must specify the decode key value as `top` or `organizationalUnit` for the code key `ouObjectClasses`.

10 Troubleshooting

This chapter provides solutions to problems you might encounter with the OID connector.

Table 10-1 Troubleshooting for the OID Connector

Problem	Solution
User Sync Reconciliation initiation fails against OUD 11.1.1.5.0 with an error message. For example: Can not use cookie based sync strategy because control 1.3.6.1.4.1.26027.1.5.4 is not supported for OUD	This problem can be caused by either: • You are not using OUD Release 2 or later. Upgrade to supported release of OUD, as listed in Certified Components. • You did not enable the changelog. The OUD changelog is automatically enabled when enabling replication.
Multiple reconciliation events are generated during reconciliation of groups that are deleted and then created again on the target system. For example: 1. Create two groups in the target system, create similar organizations in Oracle Identity Manager, and then run group reconciliation. The events are linked. 2. Delete the two groups and run group delete reconciliation. The events are linked and then revoked. 3. Create the same two groups in the target system again and run target reconciliation. Result: Four reconciliation events are created for the two groups (two reconciliation events per group). Two events are linked, and two are not linked.	This result is the expected behavior by the connector. The sync reconciliation task reads the changelog, and every record (create, update, or delete) related to the specific object class is returned from the connector.
A group provisioning operation fails when you try to provision it to a user that already has another virtual static group provisioned. The same happens during a delete provisioning operation as well.	This problem is caused because virtual static groups are not supported by default. To use the connector for dynamic or virtual static groups, you must apply the following guidelines: • Ensure referential integrity in OUD is enabled. • Set the value of the maintainLdapGroupMembership entry in the Lookup.LDAP.OUD.Configuration lookup definition to `false`.

11 Known Issues and Workarounds

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

11.1 Failure in Provisioning a User with a Backslash

Provisioning a user with a backslash in the uid and other mandatory fields fails.

To workaround this issue, avoid using backslash in the uid and other mandatory fields.

11.2 Incremental User Sync Reconciliation Does not Function as Expected

The User Sync Reconciliation scheduled job attaches multiple resources to a user.

This issue has been fixed in Oracle Identity Manager release 11*g* R1 PS2 (11.1.1.7.0) and release 11*g* R2 PS1 (11.1.2.1.0)

A

Files and Directories on the OID Connector Installation Media

This appendix lists the components of the connector installation media that comprise the OID connector.

Table A-1 describes the files and directories on the connector installation media that comprise the OID connector.

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

File in the Installation Media Directory	Description
bundle/org.identityconnectors.ldap-1.0.6380.jar	This JAR file contains the connector bundle. The connector bundle includes the required version of the LDAP Booster Pack (ldapbp.jar file).
configuration/ODSEE-OUD-LDAPV3-CI.xml configuration/EDIR-CI.xml configuration/OID-CI.xml	These XML files contain configuration information that is used during the connector installation process. For an ODSEE or OUD target system: ODSEE-OUD-LDAPV3-CI.xml For an eDirectory target system: EDIR-CI.xml For an OID target system: OID-CI.xml
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the Oracle Identity Manager database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that include GUI element labels and messages. Three sets of resource bundles are available: One each for ODSEE-OUD, OID, and eDirectory.
xml/ODSEE-OUD-LDAPV3-ConnectorConfig.xml xml/OID-ConnectorConfig.xml xml/eDirectory-ConnectorConfig.xml	These XML files contain definitions for the following connector components: • Resource objects • IT resource types • IT resource instance • Process forms • Process tasks and adapters • Process definition • Prepopulate rules • Lookup definitions • Reconciliation rules • Scheduled tasks

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

File in the Installation Media Directory	Description
xml/ODSEE-OUD-LDAPV3-Datasets.xml xml/OID-Datasets.xml xml/eDirectory-Datasets.xml **Note:** The dataset XML files are applicable only if you are using Oracle Identity Manager release 11.1.1.*x*.	These XML files contain dataset-related definitions for the create and modify user provisioning operations. Use one of the following files if you want to enable request-based provisioning by using the deployment manager: • ODSEE or OUD target system: ODSEE-OUD-LDAPV3-Datasets.xml • OID target system: OID-Datasets.xml • eDirectory target system: eDirectory-Datasets.xml

Index