

Oracle® Identity Manager

Connector Guide for Database User Management

Release 9.1.0

E11193-01

December 2009

Oracle Identity Manager Connector Guide for Database User Management, Release 9.1.0

E11193-01

Copyright © 2009, Oracle and/or its affiliates. All rights reserved.

Primary Author: Alankrita Prakash

Contributing Authors: Devanshi Mohan, Lyju Vadassery

Contributor: Sanjay Rallapalli

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	xv
Audience.....	xv
Documentation Accessibility	xv
Related Documents	xvi
Documentation Updates	xvi
Conventions	xvi
 What's New in the Oracle Identity Manager Connector for Database User Management?	xvii
Software Updates	xvii
Documentation-Specific Updates.....	xviii
 1 About the Connector	
1.1 Certified Components	1-1
1.2 Certified Languages.....	1-2
1.3 Connector Architecture.....	1-2
1.3.1 Reconciliation Process.....	1-3
1.3.2 Provisioning Process	1-4
1.4 Features of the Connector	1-10
1.4.1 Mapping Standard and Custom Attributes for Reconciliation and Provisioning ..	1-10
1.4.2 Predefined and Custom Reconciliation Queries	1-11
1.4.3 Predefined and Custom Provisioning Statements	1-11
1.4.4 Framework for Supporting Connector Operations on JDBC-Based Databases	1-11
1.4.5 Support for Creating Global and External Users In Oracle Database.....	1-11
1.4.6 Support for Configuring the Connector for Reconciling and Provisioning Object-Level Privileges in Oracle Database	1-11
1.4.7 Dependent Lookup Fields	1-12
1.4.8 Full and Incremental Reconciliation	1-12
1.4.9 Limited (Filtered) Reconciliation.....	1-12
1.4.10 Batched Reconciliation.....	1-12
1.4.11 Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations.	1-13
1.4.12 Connection Pooling	1-13
1.4.13 Support for Creating Connector Copies.....	1-13

1.4.14	Transformation and Validation of Account Data	1-13
1.4.15	Support for Reconciling Data About Deleted Login Entities	1-13
1.4.16	Separate Scheduled Tasks for Reconciliation of Users, Logins, and Deleted Login Entities 1-14	
1.4.17	Support for SSL Communication Between the Target System and Oracle Identity Manager 1-14	
1.4.18	Support for Managing Authorization to Oracle Database Vault Realms	1-14
1.4.19	Support for Configuring the Connector for Enterprise User Security	1-15
1.5	Lookup Definitions Used During Connector Operations	1-15
1.5.1	Lookup Definitions Synchronized with the Target System	1-15
1.5.1.1	Lookup Fields Synchronized with IBM DB2 UDB	1-16
1.5.1.2	Lookup Fields Synchronized with Microsoft SQL Server	1-17
1.5.1.3	Lookup Fields Synchronized with Oracle Database	1-17
1.5.1.4	Lookup Fields Synchronized with Sybase	1-17
1.5.2	Preconfigured Lookup Definitions	1-17
1.5.2.1	Lookup Definitions for IBM DB2 UDB	1-18
1.5.2.2	Lookup Definitions for Microsoft SQL Server	1-19
1.5.2.3	Lookup Definitions for Oracle Database	1-20
1.5.2.4	Lookup Definitions for Sybase	1-21
1.6	Connector Objects Used During Reconciliation	1-21
1.6.1	Reconciliation Queries	1-22
1.6.2	Target System Columns Used in Reconciliation	1-24
1.6.2.1	Target System Columns Used in Target Resource Reconciliation	1-24
1.6.2.2	Target System Columns Used in Trusted Source Reconciliation	1-25
1.6.3	Reconciliation Rules	1-26
1.6.3.1	Reconciliation Rules for Target Resource Reconciliation	1-26
1.6.3.1.1	Reconciliation Rules for the Login Entity	1-26
1.6.3.1.2	Reconciliation Rules for the User Entity	1-27
1.6.3.2	Reconciliation Rules for Trusted Source Reconciliation	1-27
1.6.3.3	Viewing Reconciliation Rules in the Design Console	1-27
1.6.4	Reconciliation Action Rules	1-27
1.6.4.1	Reconciliation Action Rules for Target Resource Reconciliation	1-28
1.6.4.2	Reconciliation Action Rules for Trusted Source Reconciliation	1-28
1.6.4.3	Viewing Reconciliation Action Rules	1-28
1.7	Connector Objects Used During Provisioning	1-29
1.7.1	Provisioning Functions	1-29
1.7.1.1	Provisioning Functions for IBM DB2 UDB	1-29
1.7.1.2	Provisioning Functions for Microsoft SQL Server	1-30
1.7.1.3	Provisioning Functions for Oracle Database	1-31
1.7.1.4	Provisioning Functions for Sybase	1-31
1.7.2	Attributes for Provisioning	1-32
1.7.2.1	Attributes for Provisioning in IBM DB2 UDB	1-32
1.7.2.2	Attributes for Provisioning in Microsoft SQL Server	1-33
1.7.2.3	Attributes for Provisioning in Oracle Database	1-34
1.7.2.4	Attributes for Provisioning in Sybase	1-35
1.8	Roadmap for Deploying and Using the Connector	1-36

2 Deploying the Connector

2.1	Preinstallation.....	2-1
2.1.1	Preinstallation on Oracle Identity Manager.....	2-1
2.1.1.1	Files and Directories on the Installation Media	2-1
2.1.1.2	Determining the Release Number of the Connector	2-3
2.1.1.3	Creating a Backup of the Existing Common.jar File	2-3
2.1.2	Preinstallation on the Target System	2-4
2.1.2.1	Configuring Microsoft SQL Server	2-4
2.1.2.2	Using External Code Files	2-5
2.1.2.2.1	Copying External Code Files for IBM DB2 UDB	2-5
2.1.2.2.2	Copying External Code Files for Microsoft SQL Server	2-5
2.1.2.2.3	Copying External Code Files for Oracle Database	2-5
2.1.2.2.4	Copying External Code Files for Sybase	2-6
2.2	Installation	2-6
2.2.1	Running the Connector Installer	2-6
2.2.2	Copying Files to the Oracle Identity Manager Host Computer.....	2-8
2.3	Postinstallation	2-8
2.3.1	Postinstallation on Oracle Identity Manager	2-8
2.3.1.1	Configuring the Target System As a Trusted Source	2-9
2.3.1.2	Changing to the Required Input Locale	2-10
2.3.1.3	Modifying the SVP Table.....	2-10
2.3.1.4	Clearing Content Related to Connector Resource Bundles from the Server Cache ... 2-10	
2.3.1.5	Enabling Logging	2-11
2.3.1.6	Configuring the Connector for Incremental Reconciliation.....	2-13
2.3.2	Creating the Administrator Account on Oracle Database Vault	2-14
2.3.3	Configuring Secure Communication Between the Target System and Oracle Identity Manager 2-15	
2.3.3.1	Configuring Secure Communication Between IBM DB2 UDB and Oracle Identity Manager 2-16	
2.3.3.2	Configuring Secure Communication Between Microsoft SQL Server and Oracle Identity Manager 2-17	
2.3.3.3	Configuring Secure Communication Between Oracle Database and Oracle Identity Manager 2-17	
2.3.3.3.1	Configuring Data Encryption and Integrity in Oracle Database	2-18
2.3.3.3.2	Configuring SSL Communication in Oracle Database	2-18
2.3.3.4	Configuring Secure Communication Between Sybase and Oracle Identity Manager 2-19	
2.3.4	Determining Values for the JDBC URL and Connection Properties Parameters....	2-19
2.3.4.1	JDBC URL and Connection Properties for IBM DB2 UDB	2-20
2.3.4.2	JDBC URL and Connection Properties for Microsoft SQL Server	2-21
2.3.4.3	JDBC URL and Connection Properties for Oracle Database	2-22
2.3.4.3.1	Only Data Encryption and Integrity Is Configured	2-22
2.3.4.3.2	Only SSL Communication Is Configured	2-23
2.3.4.3.3	Both Data Encryption and Integrity and SSL Communication Are Configured . 2-24	
2.3.4.3.4	JDBC URL and Connection Properties for Oracle RAC	2-25

2.3.4.4	JDBC URL and Connection Properties for Sybase Adaptive Server Enterprise	2-25
2.3.5	Configuring the IT Resource	2-26

3 Using the Connector

3.1	Setting Up Lookup Definitions in Oracle Identity Manager	3-1
3.1.1	Setting Up the Configuration Lookup Definition for a Target Resource	3-2
3.1.2	Setting Up the Configuration Lookup Definition for a Trusted Source	3-2
3.1.3	Setting Up the ExclusionList Lookup Definition	3-3
3.2	Guidelines on Configuring Reconciliation.....	3-4
3.3	Scheduled Task for Lookup Field Synchronization.....	3-4
3.4	Configuring Reconciliation.....	3-6
3.4.1	Performing Full Reconciliation.....	3-6
3.4.2	Reconciliation Time Stamp.....	3-7
3.4.3	Batched Reconciliation	3-7
3.4.4	Configuring Limited Reconciliation	3-8
3.4.4.1	Specifying a Value for the Custom Query Attribute.....	3-8
3.4.4.2	Adding a Filter Parameter in the Reconciliation Query	3-9
3.4.5	Reconciliation Scheduled Tasks.....	3-10
3.4.5.1	Scheduled Tasks for Reconciling Data About Users and Logins	3-11
3.4.5.2	Scheduled Tasks for Reconciling Data About Deleted Users or Logins.....	3-16
3.5	Configuring Scheduled Tasks	3-19
3.6	Guidelines on Performing Provisioning Operations	3-23
3.6.1	Guidelines Common to Performing Provisioning Operations on Any Target System.....	3-24
3.6.2	Guidelines on Performing Provisioning Operations in IBM DB2 UDB.....	3-24
3.6.3	Guidelines on Performing Provisioning Operations in Microsoft SQL Server	3-25
3.6.4	Guidelines on Performing Provisioning Operations in Oracle Database.....	3-25
3.6.5	Guidelines on Performing Provisioning Operations in Sybase	3-26
3.7	Performing Provisioning Operations.....	3-27

4 Extending the Functionality of the Connector

4.1	Guidelines on Extending the Functionality of the Connector	4-1
4.1.1	Guidelines for Configuring Queries Used in Lookup Field Synchronization.....	4-2
4.1.2	Guidelines for Configuring Queries Used in Reconciliation.....	4-2
4.1.3	Guidelines Common to Configuring Both Types of Queries.....	4-3
4.1.4	Guidelines on Modifying Predefined Attribute Mappings for Provisioning	4-4
4.2	Adding or Removing Attributes for Reconciliation	4-4
4.2.1	Adding New Standard and Custom Attributes for Reconciliation.....	4-4
4.2.2	Adding New Standard and Custom Multivalued Attributes for Target Resource Reconciliation	4-7
4.2.3	Removing Attributes Used for Reconciliation.....	4-11
4.3	Adding or Removing Attribute Mappings for Provisioning.....	4-15
4.3.1	Adding New Standard and Custom Attributes for Provisioning	4-16
4.3.2	Adding New Standard and Custom Multivalued Attributes for Provisioning	4-18
4.3.3	Removing Attributes for Provisioning	4-23
4.4	Modifying Field Lengths on the Process Form.....	4-26

4.5	Configuring the Connector for Multiple Installations of the Target System	4-26
4.5.1	Enabling the Dependent Lookup Fields Feature	4-39
4.6	Configuring the Connector for Multiple Trusted Source Reconciliation	4-45
4.7	Configuring Reconciliation Queries.....	4-45
4.8	Configuring Validation of Data During Reconciliation and Provisioning.....	4-46
4.9	Configuring Transformation of Data During Reconciliation	4-49
4.10	Configuring the Connector for Reconciling and Provisioning Object-Level Privileges	4-50
4.10.1	Configuring the Connector for Provisioning Object-Level Privileges.....	4-51
4.10.2	Configuring the Connector for Reconciling Object-Level Privileges.....	4-57
4.11	Configuring the Connector for Reconciling and Provisioning Authorization to Oracle Database Vault Realms	4-60
4.11.1	Configuring the Connector for Provisioning Authorization to Oracle Database Vault Realms	4-61
4.11.2	Configuring the Connector for Reconciling Authorization to Oracle Database Vault Realms	4-66

5 Configuring the Connector for a JDBC-Based Database

5.1	Deploying the Connector.....	5-1
5.2	Creating an IT Resource for Your Database.....	5-2
5.3	Creating a Resource Object.....	5-4
5.4	Creating a Process Form	5-5
5.5	Adding Attributes for Provisioning	5-5
5.6	Creating Lookup Definitions Used During Connector Operations	5-6
5.7	Creating a Process Definition.....	5-8
5.8	Adding Process Tasks, Assigning Adapters, and Mapping Adapter Variables.....	5-8
5.9	Adding Attributes for Reconciliation.....	5-13
5.10	Guidelines on Creating or Configuring Queries Used for Reconciliation and Lookup Synchronization	5-13
5.11	Creating Scheduled Tasks.....	5-13
5.12	Configuring Status Reconciliation.....	5-14

6 Testing the Connector

7 Known Issues

A Preconfigured Lookup Definitions

A.1	Lookup Definitions for IBM DB2 UDB	A-1
A.1.1	Lookup.DBUM.DB2.Configuration	A-2
A.1.2	Lookup.DBUM.DB2.Error.Mapping.....	A-3
A.1.3	Lookup.DBUM.DB2.ExclusionList.....	A-4
A.1.4	Lookup.DBUM.DB2.Parameter.Configuration	A-4
A.1.5	Lookup.DBUM.DB2.Provisioning.Validation	A-6
A.1.6	Lookup.DBUM.DB2.Query.Configuration	A-6
A.1.7	Lookup.DBUM.DB2.TargetRecon.Delete.Mapping	A-7
A.1.8	Lookup.DBUM.DB2.TargetRecon.Mapping	A-8
A.1.9	Lookup.DBUM.DB2.TargetRecon.QueryFilter	A-10

A.1.10	Lookup.DBUM.DB2.TargetRecon.Schema.Configuration	A-10
A.1.11	Lookup.DBUM.DB2.TargetRecon.Schema.Mapping	A-11
A.1.12	Lookup.DBUM.DB2.TargetRecon.Schema.QueryFilter	A-12
A.1.13	Lookup.DBUM.DB2.TargetRecon.Tablespace.Configuration.....	A-12
A.1.14	Lookup.DBUM.DB2.TargetRecon.Tablespace.Mapping	A-13
A.1.15	Lookup.DBUM.DB2.TargetRecon.Tablespace.QueryFilter	A-13
A.1.16	Lookup.DBUM.DB2.TargetRecon.Transformation	A-13
A.1.17	Lookup.DBUM.DB2.TargetRecon.UserTypeMapping	A-14
A.1.18	Lookup.DBUM.DB2.TargetRecon.Validation	A-14
A.1.19	Lookup.DBUM.DB2.TrustedRecon.Configuration.....	A-14
A.1.20	Lookup.DBUM.DB2.TrustedRecon.Delete.Mapping	A-15
A.1.21	Lookup.DBUM.DB2.TrustedRecon.ExclusionList	A-16
A.1.22	Lookup.DBUM.DB2.TrustedRecon.Mapping	A-16
A.1.23	Lookup.DBUM.DB2.TrustedRecon.QueryFilter	A-18
A.1.24	Lookup.DBUM.DB2.TrustedRecon.Transformation	A-18
A.1.25	Lookup.DBUM.DB2.TrustedRecon.Validation	A-18
A.1.26	Lookup.DBUM.DB2.UserType	A-19
A.1.27	Lookup.DBUM.DB2.WithGrantOption.....	A-19
A.2	Lookup Definitions for Microsoft SQL Server.....	A-19
A.2.1	Lookup.DBUM.MSSQL.AuthType	A-20
A.2.2	Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateLogin	A-20
A.2.3	Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateUser	A-21
A.2.4	Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteLogin	A-22
A.2.5	Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteUser	A-22
A.2.6	Lookup.DBUM.MSSQL.AuthType.KeyMapping.DisableLogin	A-22
A.2.7	Lookup.DBUM.MSSQL.AuthType.KeyMapping.EnableLogin	A-23
A.2.8	Lookup.DBUM.MSSQL.Configuration	A-23
A.2.9	Lookup.DBUM.MSSQL.Error.Mapping.....	A-25
A.2.10	Lookup.DBUM.MSSQL.ExclusionList.....	A-26
A.2.11	Lookup.DBUM.MSSQL.Parameter.Configuration	A-26
A.2.12	Lookup.DBUM.MSSQL.Provisioning.Validation	A-28
A.2.13	Lookup.DBUM.MSSQL.Query.Configuration	A-28
A.2.14	Lookup.DBUM.MSSQL.TargetRecon.Auth.Mapping.....	A-29
A.2.15	Lookup.DBUM.MSSQL.TargetRecon.Delete.Login.Mapping	A-30
A.2.16	Lookup.DBUM.MSSQL.TargetRecon.Delete.User.Mapping	A-31
A.2.17	Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping	A-31
A.2.18	Lookup.DBUM.MSSQL.TargetRecon.Login.Transformation	A-34
A.2.19	Lookup.DBUM.MSSQL.TargetRecon.Login.Validation	A-34
A.2.20	Lookup.DBUM.MSSQL.TargetRecon.QueryFilter	A-34
A.2.21	Lookup.DBUM.MSSQL.TargetRecon.Role.Mapping	A-34
A.2.22	Lookup.DBUM.MSSQL.TargetRecon.User.Mapping	A-35
A.2.23	Lookup.DBUM.MSSQL.TargetRecon.User.Transformation	A-36
A.2.24	Lookup.DBUM.MSSQL.TrustedRecon.Configuration.....	A-36
A.2.25	Lookup.DBUM.MSSQL.TrustedRecon.Delete.Mapping	A-37
A.2.26	Lookup.DBUM.MSSQL.TrustedRecon.ExclusionList.....	A-38
A.2.27	Lookup.DBUM.MSSQL.TrustedRecon.Mapping	A-38
A.2.28	Lookup.DBUM.MSSQL.TrustedRecon.QueryFilter	A-40

A.2.29	Lookup.DBUM.MSSQL.TrustedRecon.Transformation	A-40
A.2.30	Lookup.DBUM.MSSQL.TrustedRecon.Validation	A-40
A.3	Lookup Definitions for Oracle Database	A-41
A.3.1	Lookup.DBUM.Oracle.AuthType	A-41
A.3.2	Lookup.DBUM.Oracle.AuthType.KeyMapping.CreateUser	A-42
A.3.3	Lookup.DBUM.Oracle.AuthType.KeyMapping.UpdateUser	A-43
A.3.4	Lookup.DBUM.Oracle.Configuration	A-43
A.3.5	Lookup.DBUM.Oracle.Error.Mapping.....	A-46
A.3.6	Lookup.DBUM.Oracle.ExclusionList.....	A-46
A.3.7	Lookup.DBUM.Oracle.Parameter.Configuration	A-47
A.3.8	Lookup.DBUM.Oracle.Provisioning.Validation	A-49
A.3.9	Lookup.DBUM.Oracle.Query.Configuration	A-49
A.3.10	Lookup.DBUM.Oracle.TargetRecon.Delete.Mapping	A-51
A.3.11	Lookup.DBUM.Oracle.TargetRecon.Mapping.....	A-52
A.3.12	Lookup.DBUM.Oracle.TargetRecon.Privilege.Configuration	A-54
A.3.13	Lookup.DBUM.Oracle.TargetRecon.Privilege.Mapping	A-55
A.3.14	Lookup.DBUM.Oracle.TargetRecon.Privilege.QueryFilter.....	A-56
A.3.15	Lookup.DBUM.Oracle.TargetRecon.QueryFilter	A-56
A.3.16	Lookup.DBUM.Oracle.TargetRecon.Role.Configuration	A-56
A.3.17	Lookup.DBUM.Oracle.TargetRecon.Role.Mapping.....	A-57
A.3.18	Lookup.DBUM.Oracle.TargetRecon.Role.QueryFilter	A-58
A.3.19	Lookup.DBUM.Oracle.TargetRecon.Transformation	A-58
A.3.20	Lookup.DBUM.Oracle.TargetRecon.Validation	A-58
A.3.21	Lookup.DBUM.Oracle.WithAdminOption	A-58
A.3.22	Lookup.DBUM.Oracle.TrustedRecon.Configuration.....	A-59
A.3.23	Lookup.DBUM.Oracle.TrustedRecon.Delete.Mapping	A-60
A.3.24	Lookup.DBUM.Oracle.TrustedRecon.ExclusionList.....	A-61
A.3.25	Lookup.DBUM.Oracle.TrustedRecon.Mapping	A-61
A.3.26	Lookup.DBUM.Oracle.TrustedRecon.QueryFilter	A-63
A.3.27	Lookup.DBUM.Oracle.TrustedRecon.Transformation	A-64
A.3.28	Lookup.DBUM.Oracle.TrustedRecon.Validation	A-64
A.4	Lookup Definitions for Sybase	A-64
A.4.1	Lookup.DBUM.Sybase.Configuration	A-65
A.4.2	Lookup.DBUM.Sybase.Error.Mapping	A-66
A.4.3	Lookup.DBUM.Sybase.ExclusionList	A-67
A.4.4	Lookup.DBUM.Sybase.Parameter.Configuration.....	A-67
A.4.5	Lookup.DBUM.Sybase.Provisioning.Validation	A-69
A.4.6	Lookup.DBUM.Sybase.Query.Configuration.....	A-69
A.4.7	Lookup.DBUM.Sybase.TargetRecon.Delete.Login.Mapping.....	A-70
A.4.8	Lookup.DBUM.Sybase.TargetRecon.Delete.User.Mapping.....	A-71
A.4.9	Lookup.DBUM.Sybase.TargetRecon.Login.Mapping.....	A-71
A.4.10	Lookup.DBUM.Sybase.TargetRecon.Login.Transformation	A-74
A.4.11	Lookup.DBUM.Sybase.TargetRecon.Login.Validation	A-74
A.4.12	Lookup.DBUM.Sybase.TargetRecon.QueryFilter.....	A-74
A.4.13	Lookup.DBUM.Sybase.TargetRecon.Role.Mapping	A-74
A.4.14	Lookup.DBUM.Sybase.TargetRecon.User.Mapping	A-75
A.4.15	Lookup.DBUM.Sybase.TargetRecon.User.Transformation.....	A-76

A.4.16	Lookup.DBUM.Sybase.TargetRecon.User.Validation.....	A-77
A.4.17	Lookup.DBUM.Sybase.TrustedRecon.Configuration	A-77
A.4.18	Lookup.DBUM.Sybase.TrustedRecon.Delete.Mapping.....	A-78
A.4.19	Lookup.DBUM.Sybase.TrustedRecon.ExclusionList	A-78
A.4.20	Lookup.DBUM.Sybase.TrustedRecon.Mapping	A-79
A.4.21	Lookup.DBUM.Sybase.TrustedRecon.QueryFilter.....	A-81
A.4.22	Lookup.DBUM.Sybase.TrustedRecon.Transformation	A-81
A.4.23	Lookup.DBUM.Sybase.TrustedRecon.Validation.....	A-81
A.5	Other Lookup Definitions.....	A-82
A.5.1	Lookup.DBUM.TargetRecon.StatusMapping.....	A-82
A.5.2	Lookup.DBUM.TrustedRecon.StatusMapping	A-82

Index

List of Tables

1-1	Certified Components	1-2
1-2	Lookup Definitions Synchronized with IBM DB2 UDB.....	1-17
1-3	Lookup Definitions Synchronized with Microsoft SQL Server	1-17
1-4	Lookup Definitions Synchronized with Oracle Database.....	1-17
1-5	Lookup Definitions Synchronized with Sybase	1-17
1-6	Action Rules for Target Resource Reconciliation.....	1-28
1-7	Action Rules for Trusted Source Reconciliation.....	1-28
1-8	Provisioning Functions for IBM DB2 UDB	1-29
1-9	Provisioning Functions for Microsoft SQL Server	1-30
1-10	Provisioning Functions for Oracle Database	1-31
1-11	Provisioning Functions for Sybase	1-32
1-12	Attributes for Provisioning in IBM DB2 UDB	1-32
1-13	Attributes for Provisioning in Microsoft SQL Server	1-33
1-14	Attributes for Provisioning in Oracle Database	1-34
1-15	Attributes for Provisioning in Sybase	1-35
2-1	Files and Directories on the Installation Media.....	2-2
2-2	Files to Be Copied to the Oracle Identity Manager Host Computer	2-8
2-3	Truststore Locations on Supported Application Servers.....	2-16
2-4	Truststore Locations on Supported Application Servers.....	2-17
2-5	Truststore Locations on Supported Application Servers.....	2-18
2-6	Truststore Locations on Supported Application Servers.....	2-19
2-7	IT Resource Parameters.....	2-27
3-1	Attributes of the DBUM Lookup reconciliation Scheduled Task	3-5
3-2	Attributes of Scheduled Tasks for Fetching Data About Users or Logins During Target Resource Reconciliation	3-12
3-3	Attributes of Scheduled Tasks for Fetching Data About Deleted Users or Logins During Target Resource Reconciliation	3-18
4-1	Entries in the Configuration Lookup Definition for a Multivalued Attribute.....	4-9
4-2	Connector Objects and Their Associations.....	4-27
4-3	Queries for Lookup Field Synchronization.....	4-40
5-1	Adapters Used During Provisioning Operations.....	5-9
5-2	Adapter Variables	5-10
A-1	Entries in the Lookup.DBUM.DB2.Configuration Lookup Definition	A-2
A-2	Entries in the Lookup.DBUM.DB2.Error.Mapping Lookup Definition.....	A-4
A-3	Entries in the Lookup.DBUM.DB2.ExclusionList Lookup Definition	A-4
A-4	Entries in the Lookup.DBUM.DB2.Parameter.Configuration Lookup Definition.....	A-6
A-5	Entries in the Lookup.DBUM.DB2.Query.Configuration Lookup Definition.....	A-7
A-6	Entries in the Lookup.DBUM.DB2.TargetRecon.Delete.Mapping Lookup Definition ..	A-8
A-7	Entries in the Lookup.DBUM.DB2.TargetRecon.Mapping Lookup Definition.....	A-10
A-8	Entries in the Lookup.DBUM.DB2.TargetRecon.Schema.Configuration Lookup Definition	A-11
A-9	Entries in the Lookup.DBUM.DB2.TargetRecon.Schema.Mapping Lookup Definition	A-12
A-10	Entries in the Lookup.DBUM.DB2.TargetRecon.Tablespace.Configuration Lookup Definition	A-12
A-11	Entries in the Lookup.DBUM.DB2.TargetRecon.Tablespace.Mapping Lookup Definition ...	A-13
A-12	Entries in the Lookup.DBUM.DB2.TargetRecon.UserTypeMapping Lookup Definition	A-14
A-13	Entries in the Lookup.DBUM.DB2.TrustedRecon.Configuration Lookup Definition..	A-15
A-14	Entries in the Lookup.DBUM.DB2.TrustedRecon.Delete.Mapping Lookup Definition.....	A-16
A-15	Entries in the Lookup.DBUM.DB2.TrustedRecon.ExclusionList Lookup Definition...	A-16

A-16	Entries in the Lookup.DBUM.DB2.TrustedRecon.Mapping Lookup Definition	A-18
A-17	Entries in the Lookup.DBUM.DB2.UserType Lookup Definition	A-19
A-18	Entries in the Lookup.DBUM.DB2.WithGrantOption Lookup Definition	A-19
A-19	Entries in the Lookup.DBUM.MSSQL.AuthType Lookup Definition	A-20
A-20	Entries in the Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateLogin Lookup Definition A-21	
A-21	Entries in the Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateUser Lookup Definition A-22	
A-22	Entries in the Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteLogin Lookup Definition A-22	
A-23	Entries in the Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteUser Lookup Definition A-22	
A-24	Entries in the Lookup.DBUM.MSSQL.AuthType.KeyMapping.DisableLogin Lookup Definition A-23	
A-25	Entries in the Lookup.DBUM.MSSQL.AuthType.KeyMapping.EnableLogin Lookup Definition A-23	
A-26	Entries in the Lookup.DBUM.MSSQL.Configuration Lookup Definition	A-24
A-27	Entries in the Lookup.DBUM.MSSQL.Error.Mapping Lookup Definition	A-26
A-28	Entries in the Lookup.DBUM.MSSQL.ExclusionList Lookup Definition	A-26
A-29	Entries in the Lookup.DBUM.MSSQL.Parameter.Configuration Lookup Definition ..	A-28
A-30	Entries in the Lookup.DBUM.MSSQL.Query.Configuration Lookup Definition	A-29
A-31	Entries in the Lookup.DBUM.MSSQL.TargetRecon.Auth.Mapping Lookup Definition	A-30
A-32	Entries in the Lookup.DBUM.MSSQL.TargetRecon.Delete.Login.Mapping Lookup Definition A-30	
A-33	Entries in the Lookup.DBUM.MSSQL.TargetRecon.Delete.User.Mapping Lookup Definition A-31	
A-34	Entries in the Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping Lookup Definition	A-33
A-35	Entries in the Lookup.DBUM.MSSQL.TargetRecon.Role.Mapping Lookup Definition	A-35
A-36	Entries in the Lookup.DBUM.MSSQL.TargetRecon.User.Mapping Lookup Definition	A-36
A-37	Entries in the Lookup.DBUM.MSSQL.TrustedRecon.Configuration Lookup Definition	A-37
A-38	Entries in the Lookup.DBUM.MSSQL.TrustedRecon.Delete.Mapping Lookup Definition ...	A-38
A-39	Entries in the Lookup.DBUM.MSSQL.TrustedRecon.ExclusionList Lookup Definition	A-38
A-40	Entries in the Lookup.DBUM.DB2.TrustedRecon.Mapping Lookup Definition	A-40
A-41	Entries in the Lookup.DBUM.Oracle.AuthType Lookup Definition	A-42
A-42	Entries in the Lookup.DBUM.Oracle.AuthType.KeyMapping.CreateUser Lookup Definition A-42	
A-43	Entries in the Lookup.DBUM.Oracle.AuthType.KeyMapping.UpdateUser Lookup Definition A-43	
A-44	Entries in the Lookup.DBUM.Oracle.Configuration Lookup Definition	A-44
A-45	Entries in the Lookup.DBUM.Oracle.Error.Mapping Lookup Definition	A-46
A-46	Entries in the Lookup.DBUM.Oracle.ExclusionList Lookup Definition	A-46
A-47	Entries in the Lookup.DBUM.Oracle.Parameter.Configuration Lookup Definition	A-48
A-48	Entries in the Lookup.DBUM.Oracle.Query.Configuration Lookup Definition	A-50
A-49	Entries in the Lookup.DBUM.Oracle.TargetRecon.Delete.Mapping Lookup Definition	A-52
A-50	Entries in the Lookup.DBUM.Oracle.TargetRecon.Mapping Lookup Definition	A-54
A-51	Entries in the Lookup.DBUM.Oracle.TargetRecon.Privilege.Configuration Lookup Definition A-55	

A-52	Entries in the Lookup.DBUM.Oracle.TargetRecon.Privilege.Mapping Lookup Definition...	A-56
A-53	Entries in the Lookup.DBUM.Oracle.TargetRecon.Role.Configuration Lookup Definition..	A-57
A-54	Entries in the Lookup.DBUM.Oracle.TargetRecon.Role.Mapping Lookup Definition	A-58
A-55	Entries in the Lookup.DBUM.DB2.WithGrantOption Lookup Definition.....	A-59
A-56	Entries in the Lookup.DBUM.Oracle.TrustedRecon.Configuration Lookup Definition.....	A-59
A-57	Entries in the Lookup.DBUM.Oracle.TrustedRecon.Delete.Mapping Lookup Definition	A-60
A-58	Entries in the Lookup.DBUM.DB2.TrustedRecon.ExclusionList Lookup Definition...	A-61
A-59	Entries in the Lookup.DBUM.Oracle.TrustedRecon.Mapping Lookup Definition	A-63
A-60	Entries in the Lookup.DBUM.Sybase.Configuration Lookup Definition.....	A-65
A-61	Entries in the Lookup.DBUM.Sybase.Error.Mapping Lookup Definition	A-67
A-62	Entries in the Lookup.DBUM.Sybase.ExclusionList Lookup Definition	A-67
A-63	Entries in the Lookup.DBUM.Sybase.Parameter.Configuration Lookup Definition ...	A-69
A-64	Entries in the Lookup.DBUM.Sybase.Query.Configuration Lookup Definition	A-70
A-65	Entries in the Lookup.DBUM.Sybase.TargetRecon.Delete.Login.Mapping Lookup Definition	A-71
A-66	Entries in the Lookup.DBUM.Sybase.TargetRecon.Delete.User.Mapping Lookup Definition	A-71
A-67	Entries in the Lookup.DBUM.Sybase.TargetRecon.Login.Mapping Lookup Definition.....	A-73
A-68	Entries in the Lookup.DBUM.Sybase.TargetRecon.Role.Mapping Lookup Definition	A-75
A-69	Entries in the Lookup.DBUM.Sybase.TargetRecon.User.Mapping Lookup Definition.....	A-76
A-70	Entries in the Lookup.DBUM.Sybase.TrustedRecon.Configuration Lookup Definition	A-77
A-71	Entries in the Lookup.DBUM.Sybase.TrustedRecon.Delete.Mapping Lookup Definition	A-78
A-72	Entries in the Lookup.DBUM.Sybase.TrustedRecon.ExclusionList Lookup Definition	A-78
A-73	Entries in the Lookup.DBUM.Sybase.TrustedRecon.Mapping Lookup Definition.....	A-81
A-74	Entries in the Lookup.DBUM.TargetRecon.StatusMapping Lookup Definition	A-82
A-75	Entries in the Lookup.DBUM.TrustedRecon.StatusMapping Lookup Definition	A-83

Preface

This guide describes the connector that is used to set up Oracle Identity Manager for database user management.

Audience

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

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at <http://www.fcc.gov/cgb/consumerfacts/trs.html>, and a list of phone numbers is available at <http://www.fcc.gov/cgb/dro/trsphonebk.html>.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

<http://www.oracle.com/technology/documentation/oim1014.html>

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://www.oracle.com/technology/documentation/oim1014.html>

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	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 the Oracle Identity Manager Connector for Database User Management?

This chapter provides an overview of the updates made to the software and documentation for release 9.1.0 of the Database User Management connector.

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

- [Software Updates](#)

These include updates made to the connector software.

- [Documentation-Specific Updates](#)

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

Software Updates

The following sections discuss software updates:

Software Updates in Release 9.1.0

The following features have been introduced in this release:

See Also: [Section 1.4, "Features of the Connector"](#) for information about these new features

- Mapping standard and custom attributes for reconciliation and provisioning
- Predefined and custom reconciliation queries
- Predefined and custom provisioning statements
- Framework for supporting connector operations on JDBC-based databases
- Support for creating global and external users in Oracle Database
- Support for configuring the connector for reconciling and provisioning object-level privileges in Oracle Database
- Dependent lookup fields
- Specifying accounts to be excluded from reconciliation and provisioning operations
- Connection pooling
- Support for creating connector copies

- Transformation and validation of account data
- Support for reconciling data about deleted login entities
- Separate scheduled tasks for reconciliation of users, logins, and deleted login entities
- Support for SSL communication between the target system and Oracle Identity Manager
- Support for managing authorization to Oracle Database Vault realms
- Support for configuring the connector for Oracle Enterprise User Security

Documentation-Specific Updates

Major changes have been made in the structure of the guide. The objective of these changes is to synchronize the guide with the changes made to the connector and to improve the usability of information provided by the guide.

See [Section 1.8, "Roadmap for Deploying and Using the Connector"](#) for information about the organization of content in this guide.

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 third-party applications. This guide discusses the procedure to deploy the connector that is used to integrate Oracle Identity Manager with database user management tables in IBM DB2 UDB, Microsoft SQL Server, Oracle Database, and Sybase target systems.

In Microsoft SQL Server and Sybase, database access entities can be divided into the following types:

- Login: A login entity is used for authentication purposes.
- User: A user entity is used for authorization or access control purposes.

Microsoft SQL Server and Sybase treat these entities as parent (Login) and child (User) elements. In Oracle Identity Manager, these entities are treated as separate, independent entities. In other words, the connector provides login provisioning as well as user provisioning features in both Microsoft SQL Server and Sybase.

In Oracle Database and IBM DB2 UDB, the Login and User entities are treated as a single entity. In this guide, that entity is referred to as the Login entity.

Note: At some places in this guide, Database User Management has been referred to as the **target system**.

This chapter contains the following sections:

- [Section 1.1, "Certified Components"](#)
- [Section 1.2, "Certified Languages"](#)
- [Section 1.3, "Connector Architecture"](#)
- [Section 1.4, "Features of the Connector"](#)
- [Section 1.5, "Lookup Definitions Used During Connector Operations"](#)
- [Section 1.6, "Connector Objects Used During Reconciliation"](#)
- [Section 1.7, "Connector Objects Used During Provisioning"](#)
- [Section 1.8, "Roadmap for Deploying and Using the Connector"](#)

1.1 Certified Components

[Table 1–1](#) lists the certified components for the connector.

Table 1–1 Certified Components

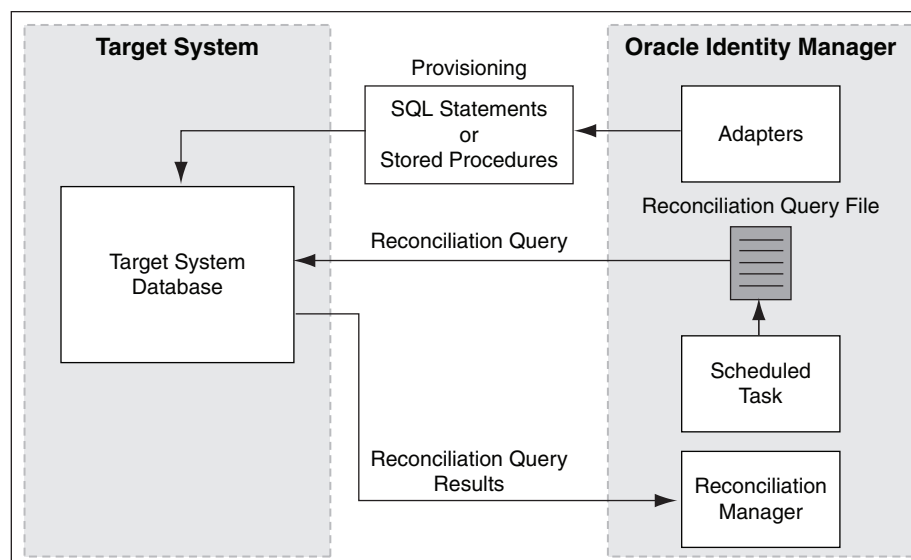
Component	Requirement
Oracle Identity Manager	Oracle Identity Manager release 9.1.0.2 BP 04 or later
Target systems	<p>The target system can be any one of the following:</p> <ul style="list-style-type: none"> ■ IBM DB2 UDB Version 9.x ■ Microsoft SQL Server 2000, 2005, 2008 ■ Oracle9i Database ■ Oracle Database 10g, 11g, as either single database or RAC implementation ■ Sybase Adaptive Server Enterprise 15.x
External code	<p>The external code consists of the following files:</p> <ul style="list-style-type: none"> ■ <code>ojdbc14.jar</code> (Oracle9i Database and Oracle Database 10g, 11g) ■ <code>msbase.jar</code>, <code>mssqlserver.jar</code>, and <code>msutil.jar</code> (Microsoft SQL Server 2000) ■ <code>sqljdbc.jar</code> (Microsoft SQL Server 2005) ■ <code>sqljdbc4.jar</code> (Microsoft SQL Server 2008) ■ <code>jconn2.jar</code> (Sybase Adaptive Server Enterprise) ■ <code>db2jcc.jar</code> and <code>db2jcc4.jar</code> (IBM DB2 UDB) <p>Note: These JAR files are available in the corresponding database installation directories.</p>
JDK	JDK 1.5 or later
Target system user account	<p>Depending on the target system, one of the following user accounts is used by Oracle Identity Manager to perform reconciliation and provisioning operations on the target system:</p> <ul style="list-style-type: none"> ■ For IBM DB2 UDB: <ul style="list-style-type: none"> Host operating system administrator account If IBM DB2 UDB DB2 is installed on a Microsoft Active Directory domain controller, then a Microsoft Windows 2003 Server (Domain Controller) Administrator account must be used. ■ For Microsoft SQL Server: <code>sa</code> (administrator) ■ For Oracle Database: <code>sys as sysdba</code>, or <code>system</code> ■ For Sybase: <code>sa</code> (administrator)

1.2 Certified Languages

The connector supports only the English language. This has been documented in [Chapter 7, "Known Issues."](#)

1.3 Connector Architecture

This connector enables management of database accounts through Oracle Identity Manager. [Figure 1–1](#) shows the architecture of the connector.

Figure 1–1 Architecture of the Connector

The architecture of the connector can be explained in terms of the connector operations it supports:

- [Section 1.3.1, "Reconciliation Process"](#)
- [Section 1.3.2, "Provisioning Process"](#)

1.3.1 Reconciliation Process

This connector can be configured to perform either trusted source reconciliation or target resource reconciliation.

Note: It is recommended that you do not configure the target system as both a trusted source and a target resource.

When you configure the target system as a target resource, the connector enables you to create and manage database accounts for OIM Users through provisioning. In addition, data related to newly created and modified target system accounts can be reconciled and linked with existing OIM Users and provisioned resources.

When you configure the target system as a trusted source, the connector fetches into Oracle Identity Manager, data about newly created or modified target system accounts. This data is used to create or update OIM Users.

See Also: The "Reconciliation" section in *Oracle Identity Manager Connector Concepts* for conceptual information about target resource reconciliation and trusted source reconciliation.

The following is an overview of the steps involved in reconciliation:

1. Depending on the target system that you are using, a SQL query or stored procedure is used to fetch target system records during reconciliation.

All predefined SQL queries and stored procedures are stored in a properties file. Each query and stored procedures in the file is identified by a name. While configuring the scheduled tasks described in Section 3.3.4, "Reconciliation

Scheduled Tasks", you specify the name of the query or stored procedure that you want to run as the value of the Query Name attribute.

2. The scheduled task is run at the time or frequency that you specify. This scheduled task contains details of the mode of reconciliation (trusted source or target resource) that you want to perform.
3. The scheduled task establishes a connection with the target system.
4. The scheduled task reads values that you set for the task attributes, maps the task attributes to parameters of the reconciliation query or stored procedure, and then runs the query or stored procedure on the target system.
5. Target system records that meet the query or stored procedure criteria are fetched into Oracle Identity Manager.
6. If you have configured your target system as a trusted source, then:
 - a. Each user record fetched from the target system is compared with existing OIM Users. The reconciliation rule is applied during the comparison process. See Section 1.6.3.2, "Reconciliation Rules for Trusted Source Reconciliation" for information about the reconciliation rule.
 - b. The next step of the process depends on the outcome of the matching operation:
 - If a match is found between the target system record and the OIM User, then the OIM User attributes are updated with changes made to the target system record.
 - If no match is found, then the target system record is used to create an OIM User.
7. If you have configured your target system as a target resource, then:
 - a. Each user record fetched from the target system is compared with existing target system resources assigned to OIM Users. The reconciliation rule is applied during the comparison process. See Section 1.6.3.1, "Reconciliation Rules for Target Resource Reconciliation" for information about the reconciliation rule.
 - b. The next step of the process depends on the outcome of the matching operation:
 - If a match is found between the target system record and a resource provisioned to an OIM User, then the database user resource is updated with changes made to the target system record.
 - If no match is found, then the target system user record is compared with existing OIM Users. The next step depends on the outcome of the matching operation:

If a match is found, then the target system record is used to provision a resource for the OIM User.

If no match is found, then the status of the reconciliation event is set to No Match Found.

1.3.2 Provisioning Process

See Also: The "Provisioning" section in *Oracle Identity Manager Connector Concepts* for conceptual information about provisioning

Provisioning involves creating and managing user accounts. When you allocate (or provision) a database resource to an OIM User, the operation results in the creation of an account on the target database for that user. Similarly, when you update the resource on Oracle Identity Manager, the same update is made to the account on the target system.

The provisioning process can be started through one of the following events:

- Direct provisioning

The Oracle Identity Manager administrator uses the Administrative and User Console to create a target system account for a user.
- Provisioning triggered by access policy changes

An access policy related to accounts on the target system is modified. When an access policy is modified, it is reevaluated for all users to which it applies.

The following is an overview of the Create User provisioning process in Oracle Database that is started through direct provisioning. The provisioning process for other supported target systems is similar to the process described here.

1. On the Create User page of the Administrative and User Console, the administrator enters the data required for an OIM User account creation.

Suppose the administrator enters the following values for the fields on the Create User page:

- First Name: John
- Last Name: Doe
- User ID: jdoe

An OIM User account is created for John Doe.

2. The administrator selects the resource to be provisioned to the OIM User account that has been created. In this example, the administrator selects the Oracle DB User resource.
3. The administrator enters the data required for provisioning the Oracle DB User resource. Suppose that the administrator wants to create a local user that requires a password to log in to the database. Therefore, the administrator enters the following values on the resource provisioning process form:

- IT Resource: Oracle
- Username: JDoe
- Authentication Type: PASSWORD
- Password: my_pa55word
- Default Tablespace: example
- Profile Name: dba_user

In addition, the administrator also enters the following values on the process form for granting roles:

- Role: 3~JAVA_ADMIN
- Role Admin Option: WITH ADMIN OPTION

4. From the information available in the IT resource for the target system, the Configuration (Lookup.DBUM.Oracle.Configuration) lookup definition is

identified. This lookup definition stores configuration information that is used during connector operations.

5. The following entry in the Configuration lookup definition is read, and the Authentication Type Create User (Lookup.DBUM.Oracle.AuthType.KeyMapping.CreateUser) lookup definition is identified:

Code Key	Decode
AuthType QueryCodeKey Mapping Lookup For CreateUser	Lookup.DBUM.Oracle.AuthType.KeyMapping.CreateUser

Note: If your database does not support authentication types for your database users, then the preceding lookup entry must not be present in your configuration lookup definition.

6. The Authentication Type Create User lookup definition holds mapping between authentication types and name of SQL statement used for creating users.

In Oracle Database, you can create a local database user, external database user, or global database user. Depending on the authentication type that the administrator selects while performing Step 3, the name of the SQL statement to be run is identified.

In this example, the following entry in the Authentication Type Create User lookup definition is read because the administrator selects password-based authentication while performing Step 3:

Code Key	Decode
PASSWORD	ORA_CREATE_USER

7. Information in the Configuration lookup definition is read to identify the Query Configuration (Lookup.DBUM.Oracle.Query.Configuration) lookup definition maps SQL statement names with the SQL statements used for performing provisioning operations.

The following entry in the Configuration lookup definition is read to identify the Query Configuration lookup definition:

Code Key	Decode
Query Configuration Lookup	Lookup.DBUM.Oracle.Query.Configuration

8. The SQL statement name identified in Step 6 is used to determine the statement to be run to perform the provisioning operation.

In Step 6, ORA_CREATE_USER, is identified as the name of the SQL statement to be run. The corresponding entry in the Query Configuration lookup definition is as follows:

Code Key	Decode
ORA_CREATE_USER	CREATE USER :ora_user_id IDENTIFIED BY :ora_password ACCOUNT UNLOCK~TABLESPACE_QUERY~TEMP_TABLESPACE_QUERY~PR OFILE_QUERY~DEFAULTTS_QUOTA_QUERY~TEMPTS_QUOTA_Q UERY

The Decode value in the preceding table is a combination of the following elements:

- SQL Keywords:

For example, CREATE, USER, IDENTIFIED, and BY.

- Identifiers:

For example, ora_user_id and ora_password.

Note: The actual values for these identifiers are determined later.

- Name of SQL statement fragment: In the SQL statement used for the Create User provisioning operation, the following are the names of the SQL statement fragments:

Note: Each SQL statement fragment name is separated by the tilde (~) character. Every SQL statement fragment name that is separated by the tilde character is optional.

- TABLESPACE_QUERY
- TEMP_TABLESPACE_QUERY
- PROFILE_QUERY
- DEFAULTTS_QUOTA_QUERY
- TEMPTS_QUOTA_QUERY

9. While performing Step 3, depending on whether the administrator had entered values in the Default Tablespace, Default Tablespace Quota (in MB), Temporary Tablespace, Temporary Tablespace Quota (in MB), or Profile Name process form fields, the Decode values of the corresponding SQL fragment name will be used.

While provisioning the Oracle DB User resource in Step 3, the administrator had entered values for the Default Table Space and Profile Name process form fields. Therefore, the following lookup entries in the Query Configuration lookup definition are read:

Code Key	Decode
TABLESPACE_QUERY	DEFAULT TABLE SPACE :ora_default_tablespace
PROFILE_QUERY	PROFILE :ora_profile

10. The complete SQL statement that must be run to perform the Create User provisioning operation is formed. In the example, this SQL statement is as follows:

```
CREATE USER :ora_user_id IDENTIFIED BY :ora_password ACCOUNT
UNLOCK DEFAULT TABLE SPACE :ora_default_tablespace PROFILE :ora_profile
```

11. All input parameters required to run the SQL statement are stored in the Parameter Configuration (Lookup.DBUM.Oracle.Parameter.Configuration) lookup definition. The input parameters for the SQL statement (formed in Step 10) are retrieved by reading the following lookup entries:

Code Key	Decode
ora_user_id	UD_DB_ORA_U_USERNAME~varchar2~IN~UPPERCASE
ora_password	UD_DB_ORA_U_PASSWORD~varchar2~IN
ora_default_tablespace	UD_DB_ORA_U_TABLESPACE~varchar2~IN~EXCLUDE_VALIDATION
ora_profile	UD_DB_ORA_U_PROFILE~varchar2~IN~EXCLUDE_VALIDATION

12. The identifiers in the SQL statement (formed in Step 10) are replaced with the input parameters fetched from the Decode values of the Parameter Configuration lookup definition. Then, the SQL statement with actual values is formed.

Suppose that while performing Step 1, the administrator enters `jdoe` as the value of the User ID field. While performing Step 3 of this procedure, the Username field is prepopulated with the value that the administrator had entered in the User ID field. Now, suppose that while performing Step 3 of this procedure, the administrator enters `example` and `my_pa55word` as the values of the Default Table Space and Profile Name process form fields, respectively. The SQL statement with the actual values is as follows:

```
CREATE USER jdoe IDENTIFIED BY my_pa55word ACCOUNT UNLOCK
DEFAULT TABLE SPACE example PROFILE db_user
```

13. The adapter runs the SQL statement on the target system (Oracle database) and creates the `jdoe` account on the target system. The next step of the process depends on whether the administrator had entered data for granting roles or privileges to the target system account.

If the administrator did not enter any values for granting roles, then the provisioning process ends here. Otherwise, the process continues to Step 14.

14. While performing Step 3, the administrator had entered the required data for granting roles to the `jdoe` account. Therefore, the following lookup entry in the Query Configuration lookup definition is read:

Code Key	Decode
ORA_ADD_ROLE	GRANT :ora_role_name TO :ora_user_id_external~ROLE_WITH_ADMIN_OPTION

In the preceding lookup entry, the SQL statement to grant a role is identified.

The Decode value in the preceding table is a combination of the following elements:

- SQL Keywords:
For example, GRANT and TO.

- Identifiers:

For example, ora_role_name and ora_user_id_external.

- SQL statement fragment name: ROLE_WITH_ADMIN_OPTION is the SQL fragment.

- While performing Step 3, in addition to specifying a value for the Role lookup field, if the administrator did not specify a value for the Role Admin Option lookup field, then proceed to Step 16.

If the administrator had specified a value for the Role Admin Option lookup field, then the following lookup entry in the Query Configuration lookup definition is read:

Code Key	Decode
ROLE_WITH_ADMIN_OPTION	:ora_role_admin_option

- The complete SQL statement that must be run to perform the Add role provisioning operation is formed. Depending on whether the administrator had granted a role with the admin option, the SQL statement is one of the following:

If the administrator specified a value for granting the role with the admin option, then the following SQL statement is formed.

```
GRANT :ora_role_name TO :ora_user_id_external :ora_role_admin_option
```

If the administrator did not specify a value for granting role with the admin option, the following SQL statement is formed:

```
GRANT :ora_role_name TO :ora_user_id_external
```

- The input parameters required to run the SQL statement are fetched from the Parameter Configuration (Lookup.DBUM.Oracle.Parameter.Configuration) lookup definition by reading the following lookup entries:

Code Key	Decode
ora_role_name	UD_DB_ORA_R_ROLE~varchar2~IN~EXCLUDE_VALIDATION
ora_user_id_external	UD_DB_ORA_U_USERNAME~varchar2~IN~DOUBLE_QUOTE~EXCLUDE_VALIDATION~UPPERCASE

- The identifiers in the SQL statement (formed in Step 16) are replaced with the input parameters fetched from the Decode values of the Parameter Configuration lookup definition. Then, the SQL statement with actual values is formed.

While performing Step 3, the administrator had specified 3~JAVA_ADMIN as the value of the Role lookup field and WITH ADMIN OPTION as the value of the Role Admin Option lookup field. Therefore, the SQL statement with the actual values is as follows:

```
GRANT 3~JAVA_ADMIN TO jdoe WITH ADMIN OPTION
```

While performing Step 3, if the administrator did not specify a value for the Role Admin Option lookup field, then the SQL statement with the actual values is as follows:

```
GRANT 3~JAVA_ADMIN TO jdoe
```

- The adapter runs the SQL statement on the target system (Oracle database) and grant the role 3~JAVA_ADMIN to the jdoe target system account.

20. While performing Step 3, if the administrator had also specified required data for granting privileges then Steps 14 through 19 will be performed by reading the appropriate lookup entries in the Query Configuration and Parameter Configuration lookup definitions.

1.4 Features of the Connector

The following are features of the connector:

- [Section 1.4.1, "Mapping Standard and Custom Attributes for Reconciliation and Provisioning"](#)
- [Section 1.4.2, "Predefined and Custom Reconciliation Queries"](#)
- [Section 1.4.3, "Predefined and Custom Provisioning Statements"](#)
- [Section 1.4.4, "Framework for Supporting Connector Operations on JDBC-Based Databases"](#)
- [Section 1.4.5, "Support for Creating Global and External Users In Oracle Database"](#)
- [Section 1.4.6, "Support for Configuring the Connector for Reconciling and Provisioning Object-Level Privileges in Oracle Database"](#)
- [Section 1.4.7, "Dependent Lookup Fields"](#)
- [Section 1.4.8, "Full and Incremental Reconciliation"](#)
- [Section 1.4.9, "Limited \(Filtered\) Reconciliation"](#)
- [Section 1.4.10, "Batched Reconciliation"](#)
- [Section 1.4.11, "Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations"](#)
- [Section 1.4.12, "Connection Pooling"](#)
- [Section 1.4.13, "Support for Creating Connector Copies"](#)
- [Section 1.4.14, "Transformation and Validation of Account Data"](#)
- [Section 1.4.15, "Support for Reconciling Data About Deleted Login Entities"](#)
- [Section 1.4.16, "Separate Scheduled Tasks for Reconciliation of Users, Logins, and Deleted Login Entities"](#)
- [Section 1.4.17, "Support for SSL Communication Between the Target System and Oracle Identity Manager"](#)
- [Section 1.4.18, "Support for Managing Authorization to Oracle Database Vault Realms"](#)
- [Section 1.4.19, "Support for Configuring the Connector for Enterprise User Security"](#)

1.4.1 Mapping Standard and Custom Attributes for Reconciliation and Provisioning

You can create mappings for single-valued and multivalued target system attributes that are not included in the list of default attribute mappings. These attributes can be part of the standard set of attributes provided by the target system or custom attributes that you add on the target system.

See [Chapter 4, "Extending the Functionality of the Connector"](#) for more information.

1.4.2 Predefined and Custom Reconciliation Queries

Reconciliation involves running a SQL query or stored procedure on the target system database to fetch the required user account records to Oracle Identity Manager.

The connector provides predefined SQL queries and stored procedures that enable you to reconcile user data from the target system. These predefined SQL queries and stored procedures are stored in a file in the connector deployment package.

You can modify these SQL queries or stored procedures. In addition, you can add your own SQL queries or stored procedures for reconciliation.

See the following sections for more information:

- [Section 1.6.1, "Reconciliation Queries"](#)
- [Section 4.7, "Configuring Reconciliation Queries"](#)

1.4.3 Predefined and Custom Provisioning Statements

Provisioning involves running statements such as CREATE USER, ALTER USER, and DROP USER to perform Create User and Update user operations on the target system through Oracle Identity Manager.

The connector provides predefined statements that enable you to perform provisioning operations such as create, enable, and update target system accounts. These statements are stored in a lookup definition, which is created when you deploy the connector.

You can modify and use any of the predefined provisioning statements. In addition, you can create your own provisioning statements.

1.4.4 Framework for Supporting Connector Operations on JDBC-Based Databases

The Database User Management connector is built on a framework designed for JDBC-based databases. This framework enables you to perform connector operations on a target system other than IBM DB2, Microsoft SQL Server, Oracle Database, and Sybase. You can configure the connector and add code to perform connector operations on your target system by performing the procedures described in [Chapter 5, "Configuring the Connector for a JDBC-Based Database"](#).

1.4.5 Support for Creating Global and External Users In Oracle Database

A local database user is a user who can be authenticated using a password stored in the database. In addition to support for local database users, the connector can also be used to work with the following types of users in Oracle Database:

- Global users: These are database users who must be authorized by an enterprise directory service such as Oracle Internet Directory.
- External users: These are database users who must be authenticated by an external service, such as an operating system or a third-party service.

See [Section A.3.9, "Lookup.DBUM.Oracle.Query.Configuration"](#) for information about the SQL statements that are used for provisioning local, global, and external users.

1.4.6 Support for Configuring the Connector for Reconciling and Provisioning Object-Level Privileges in Oracle Database

You can configure this connector to reconcile and provision object-level privileges to a database user in Oracle Database. An object-level privilege is permission that is

granted to a database user to perform a particular action on a database object. This connector treats object-level privileges that are granted to a database user as an entitlement.

See [Section 4.10, "Configuring the Connector for Reconciling and Provisioning Object-Level Privileges"](#) for more information.

1.4.7 Dependent Lookup Fields

In earlier releases, if you had multiple installations of the target system, then entries in a lookup definition were not linked with the target system installation from which the entries were copied. During a provisioning operation, you could not select lookup field values that were specific to the target system installation on which the provisioning operation was to be performed.

From this release onward, entries in lookup definitions can be linked to the target system installation from which they are copied by enabling the dependent lookup fields feature.

See [Section 4.5.1, "Enabling the Dependent Lookup Fields Feature"](#) for information about enabling this feature.

See [Section 1.5.1, "Lookup Definitions Synchronized with the Target System"](#) for more information about the format in which data is stored in dependent lookup definitions.

1.4.8 Full and Incremental Reconciliation

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, you can configure your connector for incremental reconciliation. In incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Manager.

See the following sections for more information:

- [Section 3.4.1, "Performing Full Reconciliation"](#)
- [Section 3.4.2, "Reconciliation Time Stamp"](#)

1.4.9 Limited (Filtered) Reconciliation

To limit or filter the records that are fetched into Oracle Identity Manager during a reconciliation run, you can add conditions either in the WHERE clause of the reconciliation query that you run or in the Custom Query attribute of the scheduled task.

See [Section 3.4.4, "Configuring Limited Reconciliation"](#) for more information.

1.4.10 Batched Reconciliation

You can break down a reconciliation run into batches by specifying the number of records that must be included in each batch and the query that must be used to perform batched reconciliation.

Note: Microsoft SQL Server and Sybase use stored procedures to perform reconciliation. Therefore, the connector does not support batched reconciliation.

See [Section 3.4.3, "Batched Reconciliation"](#) for more information.

1.4.11 Specifying Accounts to Be Excluded from Reconciliation and Provisioning Operations

You can specify a list of target system accounts that must be excluded from all reconciliation and provisioning operations. Accounts whose users attributes you specify in the exclusion list are not affected by reconciliation and provisioning operations.

See [Section 3.1.3, "Setting Up the ExclusionList Lookup Definition"](#) for more information.

1.4.12 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 like 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 will be created, one for each target system installation.

The configuration properties of the connection pool are part of the IT resource definition. [Section 2.3.5, "Configuring the IT Resource"](#) provides information about setting up the connection pool.

1.4.13 Support for Creating Connector Copies

You can configure this connector for multiple installations of your target system by creating copies of connector objects such as lookup definitions, resource objects, and process forms.

See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for more information.

1.4.14 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:

- [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#)
- [Section 4.9, "Configuring Transformation of Data During Reconciliation"](#)

1.4.15 Support for Reconciling Data About Deleted Login Entities

You can reconcile data about login entities that have been deleted on the target system that has been configured as a trusted source or target resource.

After the records are fetched in to Oracle Identity Manager, depending on whether you have configured your target system as a target resource or trusted source, the records are compared with existing OIM Users or database resources provisioned to existing OIM Users.

See [Section 3.4.5.2, "Scheduled Tasks for Reconciling Data About Deleted Users or Logins"](#) for more information.

1.4.16 Separate Scheduled Tasks for Reconciliation of Users, Logins, and Deleted Login Entities

You can reconcile data about users, logins, or deleted login entities from a target system that is configured as a trusted source or target resource. Depending on the target system that you are using, the mode in which it is configured, and the type of data that you want to reconcile, separate scheduled tasks have been created.

See [Section 3.4.5, "Reconciliation Scheduled Tasks"](#) for more information.

1.4.17 Support for SSL Communication Between the Target System and Oracle Identity Manager

You can configure SSL to secure communication between Oracle Identity Manager and the target system.

See [Section 2.3.3, "Configuring Secure Communication Between the Target System and Oracle Identity Manager"](#) for more information.

1.4.18 Support for Managing Authorization to Oracle Database Vault Realms

Oracle Database Vault restricts access to specific areas in an Oracle Database from any user, including users who have administrative access. For example, you can restrict administrative access to employee salaries, customer medical records, or other sensitive information. This enables you to apply fine-grained access control to your sensitive data in a variety of ways. It hardens your Oracle Database instance and enforces industry standard best practices in terms of separating duties from users with administrative access. Most importantly, it protects data from super-privileged users but still allows them to manage the Oracle Database installation.

With Oracle Database Vault, you can address business requirements such as protecting against insider threats, meeting regulatory compliance requirements, and enforcing separation of duty.

You configure Oracle Database Vault to manage the security of an individual Oracle Database instance. You can install Oracle Database Vault on standalone Oracle Database installations, in multiple Oracle homes, and in Oracle Real Application Clusters (RAC) environments.

In Oracle Database installations on which Oracle Database Vault is installed, the connector can be used to grant and manage authorization to Oracle Database Vault realms. The connector treats access to Oracle Database Vault realms as an entitlement. You can use the connector to provision database users with access to multiple realms with different levels of access.

Because Oracle Identity Manager is an enterprise application for managing user accounts and access to entitlements, the connector does not support management of the following:

- Realms

- Command rules and rule sets
- Factors
- Secure Application Roles

See the following sections for more information:

- [Section 2.3.2, "Creating the Administrator Account on Oracle Database Vault"](#)
- [Section 4.11, "Configuring the Connector for Reconciling and Provisioning Authorization to Oracle Database Vault Realms"](#)

1.4.19 Support for Configuring the Connector for Enterprise User Security

Oracle Enterprise User Security addresses user, administrative, and security challenges by using the identity management services supplied by Oracle Internet Directory, an LDAP-compliant directory service. Enterprise users are provisioned and managed centrally in an LDAP-compliant directory, such as Oracle Internet Directory, for database access. Enterprise users have a unique identity in the directory called the distinguished name (DN). When enterprise users log on to a database, the database authenticates those users by using their DN.

In Oracle Database installations configured with Oracle Enterprise User Security, the connector supports the creation of globally and externally authenticated users.

Note: You must use either Oracle Identity Manager LDAP connectors or some other means to create the user in the LDAP-compliant directory.

You can use the connector to create and manage accounts of these enterprise users on the target database.

1.5 Lookup Definitions Used During Connector Operations

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

- [Section 1.5.1, "Lookup Definitions Synchronized with the Target System"](#)
- [Section 1.5.2, "Preconfigured Lookup Definitions"](#)

1.5.1 Lookup Definitions Synchronized with the Target System

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 Role lookup field to select a role to be assigned to the user from the list of available roles. 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.

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

- Code Key value: *IT_RESOURCE_KEY~LOOKUP_FIELD_ID*

In this format:

- *IT_RESOURCE_KEY* is the numeric code assigned to each IT resource in Oracle Identity Manager.

- *LOOKUP_FIELD_ID* is the target system code assigned to each lookup field entry.

Sample value: 1~SYS_ADM

- Decode value: *IT_RESOURCE_NAME*~*LOOKUP_FIELD_ID*

In this format:

- *IT_RESOURCE_NAME* is the name of the IT resource in Oracle Identity Manager.
- *LOOKUP_FIELD_ID* is the target system code assigned to each lookup field entry.

Sample value: Oracle~SYS_ADM

The DBUM Lookup reconciliation scheduled task is used to synchronize values of these lookup definitions with the target system. See [Section 3.3, "Scheduled Task for Lookup Field Synchronization"](#) for more information about this scheduled task.

While performing a provisioning operation on the Administrative and User Console, you select the IT resource for the target system on which you want to perform the operation. When you perform this action, the lookup definitions on the page are automatically populated with values corresponding to the IT resource (target system installation) that you select. If your environment has multiple installations of the target system, then values corresponding to all IT resources are displayed. However, if you enable the Dependent Lookup Field feature, then only values that correspond to the IT resource that you select are displayed. See [Section 4.5.1, "Enabling the Dependent Lookup Fields Feature"](#) for information about enabling this feature.

During lookup field synchronization, new entries are appended to the existing set of entries in the lookup definitions. If you enable the Dependent Lookup Field feature, then you can switch between multiple installations of the same target system. Because the IT resource key is part of each entry created in each lookup definition, only lookup field entries that are specific to the IT resource you select during a provisioning operation are displayed.

Note: The format in which data is stored after lookup definition synchronization remains the same whether or not the Dependent Lookup Field feature is enabled.

The following sections provide information about the lookup definitions in Oracle Identity Manager that correspond to each of the target systems:

- [Section 1.5.1.1, "Lookup Fields Synchronized with IBM DB2 UDB"](#)
- [Section 1.5.1.2, "Lookup Fields Synchronized with Microsoft SQL Server"](#)
- [Section 1.5.1.3, "Lookup Fields Synchronized with Oracle Database"](#)
- [Section 1.5.1.4, "Lookup Fields Synchronized with Sybase"](#)

1.5.1.1 Lookup Fields Synchronized with IBM DB2 UDB

[Table 1–2](#) lists column names of the tables in IBM DB2 UDB that are synchronized with their corresponding lookup definitions in Oracle Identity Manager.

Table 1–2 Lookup Definitions Synchronized with IBM DB2 UDB

Lookup Definition	Target Table Name	Target Column Name
Lookup.DBUM.DB2.Tablespace	syscat.tablespace	tblspace
Lookup.DBUM.DB2.Schema	syscat.tables	tblschema

1.5.1.2 Lookup Fields Synchronized with Microsoft SQL Server

[Table 1–3](#) lists column names of the tables in Microsoft SQL Server that are synchronized with their corresponding lookup definitions in Oracle Identity Manager.

Table 1–3 Lookup Definitions Synchronized with Microsoft SQL Server

Lookup Definition	Target Table Name	Target Column Name
Lookup.DBUM.MSSQL.DBNames	sys.sysdatabases	name
Lookup.DBUM.MSSQL.DBRoles	sysusers	name
Lookup.DBUM.MSSQL.DefaultLang	sys.syslanguages	alias

1.5.1.3 Lookup Fields Synchronized with Oracle Database

[Table 1–4](#) lists column names of the tables in Oracle Database that are synchronized with their corresponding lookup definitions in Oracle Identity Manager.

Table 1–4 Lookup Definitions Synchronized with Oracle Database

Lookup Definition	Target Table Name	Target Column Name
Lookup.DBUM.Oracle.Profiles	dba_profiles	DISTINCT profile
Lookup.DBUM.Oracle.Roles	dba_roles	role
Lookup.DBUM.Oracle.Privileges	system_privilege_map	name
Lookup.DBUM.Oracle.Temp.Tablespace	dba_tablespace	tablespace_name
Lookup.DBUM.Oracle.Tablespace	dba_tablespace	tablespace_name

1.5.1.4 Lookup Fields Synchronized with Sybase

[Table 1–5](#) lists column names of the tables in Sybase that are synchronized with their corresponding lookup definitions in Oracle Identity Manager.

Table 1–5 Lookup Definitions Synchronized with Sybase

Lookup Definition	Target Table Name	Target Column Name
Lookup.DBUM.Sybase.Databases	sysdatabases	name
Lookup.DBUM.Sybase.Roles	sysrvroles	name
Lookup.DBUM.Sybase.DefaultLang	syslanguages	alias
Lookup.DBUM.Sybase.DBGroups	sysusers	name

1.5.2 Preconfigured Lookup Definitions

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

The following sections discuss lookup definitions in Oracle Identity Manager for each target system:

- [Section 1.5.2.1, "Lookup Definitions for IBM DB2 UDB"](#)
- [Section 1.5.2.2, "Lookup Definitions for Microsoft SQL Server"](#)
- [Section 1.5.2.3, "Lookup Definitions for Oracle Database"](#)
- [Section 1.5.2.4, "Lookup Definitions for Sybase"](#)

1.5.2.1 Lookup Definitions for IBM DB2 UDB

The following are the lookup definitions that are created in Oracle Identity Manager for IBM DB2 UDB:

Note: See [Appendix A.1, "Lookup Definitions for IBM DB2 UDB"](#) for information about each of the look up definitions.

Lookup.DBUM.DB2.Configuration
 Lookup.DBUM.DB2.Error.Mapping
 Lookup.DBUM.DB2.ExclusionList
 Lookup.DBUM.DB2.Parameter.Configuration
 Lookup.DBUM.DB2.Provisioning.Validation
 Lookup.DBUM.DB2.Query.Configuration
 Lookup.DBUM.DB2.TargetRecon.Delete.Mapping
 Lookup.DBUM.DB2.TargetRecon.Mapping
 Lookup.DBUM.DB2.TargetRecon.QueryFilter
 Lookup.DBUM.DB2.TargetRecon.Schema.Configuration
 Lookup.DBUM.DB2.TargetRecon.Schema.Mapping
 Lookup.DBUM.DB2.TargetRecon.Schema.QueryFilter
 Lookup.DBUM.DB2.TargetRecon.Tablespace.Configuration
 Lookup.DBUM.DB2.TargetRecon.Tablespace.Mapping
 Lookup.DBUM.DB2.TargetRecon.Tablespace.QueryFilter
 Lookup.DBUM.DB2.TargetRecon.Transformation
 Lookup.DBUM.DB2.TargetRecon.UserTypeMapping
 Lookup.DBUM.DB2.TargetRecon.Validation
 Lookup.DBUM.DB2.TrustedRecon.Configuration
 Lookup.DBUM.DB2.TrustedRecon.Delete.Mapping
 Lookup.DBUM.DB2.TrustedRecon.ExclusionList
 Lookup.DBUM.DB2.TrustedRecon.Mapping
 Lookup.DBUM.DB2.TrustedRecon.QueryFilter
 Lookup.DBUM.DB2.TrustedRecon.Transformation
 Lookup.DBUM.DB2.TrustedRecon.Validation

Lookup.DBUM.DB2.UserType

Lookup.DBUM.DB2.WithGrantOption

1.5.2.2 Lookup Definitions for Microsoft SQL Server

The following are lookup definitions that are created in Oracle Identity Manager for Microsoft SQL Server:

Note: See [Appendix A.2, "Lookup Definitions for Microsoft SQL Server"](#) for information about each of the look up definitions.

Lookup.DBUM.MSSQL.AuthType

Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateLogin

Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateUser

Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteLogin

Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteUser

Lookup.DBUM.MSSQL.AuthType.KeyMapping.DisableLogin

Lookup.DBUM.MSSQL.AuthType.KeyMapping.EnableLogin

Lookup.DBUM.MSSQL.Configuration

Lookup.DBUM.MSSQL.Error Mapping

Lookup.DBUM.MSSQL.ExclusionList

Lookup.DBUM.MSSQL.Parameter.Configuration

Lookup.DBUM.MSSQL.Provisioning.Validation

Lookup.DBUM.MSSQL.Query.Configuration

Lookup.DBUM.MSSQL.TargetRecon.Auth.Mapping

Lookup.DBUM.MSSQL.TargetRecon.Delete.Login.Mapping

Lookup.DBUM.MSSQL.TargetRecon.Delete.User.Mapping

Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping

Lookup.DBUM.MSSQL.TargetRecon.Login.Transformation

Lookup.DBUM.MSSQL.TargetRecon.Login.Validation

Lookup.DBUM.MSSQL.TargetRecon.QueryFilter

Lookup.DBUM.MSSQL.TargetRecon.Role.Mapping

Lookup.DBUM.MSSQL.TargetRecon.User.Mapping

Lookup.DBUM.MSSQL.TargetRecon.User.Transformation

Lookup.DBUM.MSSQL.TrustedRecon.Configuration

Lookup.DBUM.MSSQL.TrustedRecon.Delete.Mapping

Lookup.DBUM.MSSQL.TrustedRecon.ExclusionList

Lookup.DBUM.MSSQL.TrustedRecon.Mapping

Lookup.DBUM.MSSQL.TrustedRecon.QueryFilter

Lookup.DBUM.MSSQL.TrustedRecon.Transformation

Lookup.DBUM.MSSQL.TrustedRecon.Validation

1.5.2.3 Lookup Definitions for Oracle Database

The following are lookup definitions that are created in Oracle Identity Manager for Oracle Database:

Note: See [Appendix A.3, "Lookup Definitions for Oracle Database"](#) for information about each of the look up definitions.

Lookup.DBUM.Oracle.AuthType
Lookup.DBUM.Oracle.AuthType.KeyMapping.CreateUser
Lookup.DBUM.Oracle.AuthType.KeyMapping.UpdateUser
Lookup.DBUM.Oracle.Configuration
Lookup.DBUM.Oracle.Error Mapping
Lookup.DBUM.Oracle.ExclusionList
Lookup.DBUM.Oracle.Parameter.Configuration
Lookup.DBUM.Oracle.Provisioning.Validation
Lookup.DBUM.Oracle.Query.Configuration
Lookup.DBUM.Oracle.TargetRecon.Delete.Mapping
Lookup.DBUM.Oracle.TargetRecon.Mapping
Lookup.DBUM.Oracle.TargetRecon.Privilege.Configuration
Lookup.DBUM.Oracle.TargetRecon.Privilege.Mapping
Lookup.DBUM.Oracle.TargetRecon.Privilege.QueryFilter
Lookup.DBUM.Oracle.TargetRecon.QueryFilter
Lookup.DBUM.Oracle.TargetRecon.Role.Configuration
Lookup.DBUM.Oracle.TargetRecon.Role.Mapping
Lookup.DBUM.Oracle.TargetRecon.Role.QueryFilter
Lookup.DBUM.Oracle.TargetRecon.Transformation
Lookup.DBUM.Oracle.TargetRecon.Validation
Lookup.DBUM.Oracle.TrustedRecon.Configuration
Lookup.DBUM.Oracle.TrustedRecon.Delete.Mapping
Lookup.DBUM.Oracle.TrustedRecon.ExclusionList
Lookup.DBUM.Oracle.TrustedRecon.Mapping
Lookup.DBUM.Oracle.TrustedRecon.QueryFilter
Lookup.DBUM.Oracle.TrustedRecon.Transformation
Lookup.DBUM.Oracle.TrustedRecon.Validation
Lookup.DBUM.Oracle.WithAdminOption

1.5.2.4 Lookup Definitions for Sybase

The following are lookup definitions that are created in Oracle Identity Manager for Sybase:

Note: See [Appendix A.4, "Lookup Definitions for Sybase"](#) for information about each of the look up definitions.

Lookup.DBUM.Sybase.Configuration
 Lookup.DBUM.Sybase.Error Mapping
 Lookup.DBUM.Sybase.ExclusionList
 Lookup.DBUM.Sybase.Parameter.Configuration
 Lookup.DBUM.Sybase.Provisioning.Validation
 Lookup.DBUM.Sybase.Query.Configuration
 Lookup.DBUM.Sybase.TargetRecon.Delete.Login.Mapping
 Lookup.DBUM.Sybase.TargetRecon.Delete.User.Mapping
 Lookup.DBUM.Sybase.TargetRecon.Login.Mapping
 Lookup.DBUM.Sybase.TargetRecon.Login.Transformation
 Lookup.DBUM.Sybase.TargetRecon.Login.Validation
 Lookup.DBUM.Sybase.TargetRecon.Role.Mapping
 Lookup.DBUM.Sybase.TargetRecon.User.Mapping
 Lookup.DBUM.Sybase.TargetRecon.User.Transformation
 Lookup.DBUM.Sybase.TargetRecon.User.Validation
 Lookup.DBUM.Sybase.TrustedRecon.Configuration
 Lookup.DBUM.Sybase.TrustedRecon.Delete.Mapping
 Lookup.DBUM.Sybase.TrustedRecon.ExclusionList
 Lookup.DBUM.Sybase.TrustedRecon.Mapping
 Lookup.DBUM.Sybase.TrustedRecon.QueryFilter
 Lookup.DBUM.Sybase.TrustedRecon.Transformation
 Lookup.DBUM.Sybase.TrustedRecon.Validation
 Lookup.DBUM.TrustedRecon.StatusMapping

1.6 Connector Objects Used During Reconciliation

The following sections discuss connector objects used during reconciliation:

- [Section 1.6.1, "Reconciliation Queries"](#)
- [Section 1.6.2, "Target System Columns Used in Reconciliation"](#)
- [Section 1.6.3, "Reconciliation Rules"](#)
- [Section 1.6.4, "Reconciliation Action Rules"](#)

1.6.1 Reconciliation Queries

As mentioned earlier in this chapter, a SQL query or stored procedure is used to fetch target system records during reconciliation. All predefined SQL queries and stored procedures are stored in the DBUMReconQuery.properties file.

Note: Depending on your requirements, you can modify existing queries or add your own query in the properties file. Alternatively, you can create and use your own properties file. [Section 4.1, "Guidelines on Extending the Functionality of the Connector"](#) provides more information.

Some of the predefined queries for Oracle Database are used in conjunction with the Last Execution Time scheduled task attribute. This attribute stores the time stamp at which the last reconciliation run started. When the next reconciliation run begins, only target system records for which the LAST UPDATED column value is greater than the value of the Last Execution Time attribute are fetched into Oracle Identity Manager. In other words, only records that were added or modified after the last reconciliation run started are considered for the current reconciliation run.

You can specify a value for the Last Execution Time attribute. See [Section 3.4.2, "Reconciliation Time Stamp"](#) for more information.

The following are predefined queries and stored procedures in the DBUMReconQuery.properties file:

■ IBM DB2 UDB

The following are the predefined queries for IBM DB2 UDB:

– DB2_TARGET_USER_RECON

This query is used to fetch all grantee records from the SYSIBM.SYSDBAUTH table. It is used during target resource reconciliation.

– DB2_TARGET_USER_RECON_WITH_BATCH

This query is used to fetch from the SYSIBM.SYSDBAUTH table, grantee records that are present within the specified range. It is used to perform batched reconciliation on a target system that is configured as a target resource.

– DB2_TARGET_USER_SCHEMA

This query is used to fetch from the SYSIBM.SYSSCHEMAAUTH table, the name of the schema that a particular user can access.

– DB2_TARGET_USER_TABLESPACE

This query is used to fetch from the SYSIBM.SYSTBSPACEAUTH table, the name of the tablespace that a particular user can access.

– DB2_TRUSTED_USER_RECON

This query is used to fetch all grantee records from the SYSIBM.SYSDBAUTH table. It is used during trusted source reconciliation.

– DB2_TRUSTED_USER_RECON_WITH_BATCH

This query is used to fetch from the SYSIBM.SYSDBAUTH table grantee records that are present within the specified range. It is used to perform batched reconciliation on a target system that is configured as a trusted source.

- DB2_DELETE_USER

This query is used to fetch all grantee records from the SYSIBM.SYSDBAUTH tables. It is used to perform delete user reconciliation.

- **Microsoft SQL Server**

The following are the predefined queries and stored procedures for Microsoft SQL Server:

- SQL_SERVER_DATABASE

This query is used to fetch names of all databases that are managed by the Microsoft SQL Server instance.

- SQL_SERVER_LOGIN

This query is used to fetch all logins names.

- SQL_SERVER_LOGIN_DETAILS

This stored procedure is used to fetch information about a given login and the users associated with it in each database.

- SQL_SERVER_USER_DETAILS

This stored procedure is used to fetch information about users in the current database.

- SQL_SERVER_STATUS_AUTH_TYPE

This query is used to fetch the status of a given login account on the target system. The result set specifies whether the login account is disabled. In addition, the result set specifies the authentication type used by the login account.

- SQL_SERVER_LOGIN_USER_DELETE

This query is used to fetch all login names. It is used to perform delete login reconciliation or delete user reconciliation.

- **Oracle Database**

The following are the predefined queries for Oracle Database:

- ORACLE_TARGET_USER_RECON

This query is used to fetch all user records from the DBA_USERS table. It is used during target resource reconciliation.

- ORACLE_TARGET_USER_RECON_WITH_BATCH

This query is used to fetch from the DBA_USERS table user records that are present within the specified range. It is used to perform batched reconciliation on a target system that is configured as a target resource.

- ORACLE_TARGET_USER_ROLE

This query is used to fetch from the DBA_ROLE_PRIVS table, details of roles granted to a particular user.

- ORACLE_TARGET_USER_PRIVILEGE

This query is used to fetch from the DBA_SYS_PRIVS table, details of privileges granted to a given user.

- ORACLE_TRUSTED_USER_RECON

This query is used to fetch all user records from the DBA_USERS table. It is used to perform trusted source reconciliation

- ORACLE_TRUSTED_USER_RECON_WITH_BATCH

This query is used to fetch from the DBA_USERS table, user records that are present within the specified range. This query is used to perform batched reconciliation on a target system that is configured as a trusted source.

- ORACLE_RECON_TIME

This query is used to determine the current time of the target system by calculating the difference in current date and 1st January, 1970 in milliseconds. This time is used as value for the Last Execution Time attribute of the scheduled task.

- ORACLE_DELETE_USER

This query is used to fetch all user records from the DBA_USERS table. It is used to perform delete user reconciliation.

- **Sybase**

The following are the predefined queries and stored procedures for Sybase:

- SYBASE_DATABASE

This query is used to fetch the names of all databases managed by the Sybase server instance.

- SYBASE_LOGIN

This query is used to fetch details of all login accounts.

- SYBASE_LOGIN_DETAILS

This stored procedure is used to display information about a given login account.

- SYBASE_USER_DETAILS

This stored procedure is used to fetch information about all users in the current database.

- SYBASE_LOGIN_DELETE_USER

This query is used to fetch all login accounts. It is used to perform delete login reconciliation.

1.6.2 Target System Columns Used in Reconciliation

As mentioned earlier in this guide, this connector can be configured to perform either target resource reconciliation or trusted source reconciliation. This section discusses the following topics:

- [Section 1.6.2.1, "Target System Columns Used in Target Resource Reconciliation"](#)
- [Section 1.6.2.2, "Target System Columns Used in Trusted Source Reconciliation"](#)

1.6.2.1 Target System Columns Used in Target Resource Reconciliation

Depending on the target system that you use, the following are the lookup definitions that map resource object fields and target system columns or column aliases used in the reconciliation query:

- **For IBM DB2 UDB**

The Lookup.DBUM.DB2.TargetRecon.Mapping lookup definition holds attribute mappings for user reconciliation. See [Appendix A.1.8](#), "[Lookup.DBUM.DB2.TargetRecon.Mapping](#)" for more information about this lookup definition.

- **For Microsoft SQL Server login entity**

The Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping lookup definition holds attribute mappings for login data reconciliation. See [Appendix A.2.17](#), "[Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping](#)" for more information about this lookup definition.

- **For Microsoft SQL Server user entity**

The Lookup.DBUM.MSSQL.TargetRecon.User.Mapping lookup definition holds the attribute mappings for user data reconciliation. See [Appendix A.2.22](#), "[Lookup.DBUM.MSSQL.TargetRecon.User.Mapping](#)" for more information about this lookup definition.

- **For Oracle Database**

The Lookup.DBUM.Oracle.TargetRecon.Mapping lookup definition holds attribute mappings for user reconciliation. See [Appendix A.3.11](#), "[Lookup.DBUM.Oracle.TargetRecon.Mapping](#)" for more information about this lookup definition.

- **For Sybase login entity**

The Lookup.DBUM.Sybase.TargetRecon.Login.Mapping lookup definition holds attribute mappings for login data reconciliation. See [Appendix A.4.9](#), "[Lookup.DBUM.Sybase.TargetRecon.Login.Mapping](#)" for more information about this lookup definition.

- **For Sybase user entity**

The Lookup.DBUM.Sybase.TargetRecon.User.Mapping lookup definition holds attribute mappings for user data reconciliation. See [Appendix A.4.14](#), "[Lookup.DBUM.Sybase.TargetRecon.User.Mapping](#)" for more information about this lookup definition.

1.6.2.2 Target System Columns Used in Trusted Source Reconciliation

Depending on the target system that you use, the following are the lookup definitions that map resource object fields and target system columns or column aliases used in the reconciliation query:

- **For IBM DB2 UDB**

The Lookup.DBUM.DB2.TrustedRecon.Mapping lookup definition holds attribute mappings for reconciliation. See [Appendix A.1.22](#), "[Lookup.DBUM.DB2.TrustedRecon.Mapping](#)" for more information about this lookup definition.

- **For Microsoft SQL Server**

The Lookup.DBUM.MSSQL.TrustedRecon.Mapping lookup definition holds attribute mappings for reconciliation. See [Appendix A.2.27](#), "[Lookup.DBUM.MSSQL.TrustedRecon.Mapping](#)" for more information about this lookup definition.

- **For Oracle Database**

The Lookup.DBUM.Oracle.TrustedRecon.Mapping lookup definition holds attribute mappings for reconciliation. See [Appendix A.3.25](#),

["Lookup.DBUM.Oracle.TrustedRecon.Mapping"](#) for more information about this lookup definition.

- **For Sybase**

The Lookup.DBUM.Sybase.TrustedRecon.Mapping lookup definition holds attribute mappings for reconciliation. See [Appendix A.4.20](#), ["Lookup.DBUM.Sybase.TrustedRecon.Mapping"](#) for more information about this lookup definition.

1.6.3 Reconciliation Rules

See Also: *Oracle Identity Manager Connector Concepts* for generic information about reconciliation rules and reconciliation action rules

The following sections provide information about reconciliation rules used by the reconciliation engine for this connector:

- [Section 1.6.3.1, "Reconciliation Rules for Target Resource Reconciliation"](#)
- [Section 1.6.3.2, "Reconciliation Rules for Trusted Source Reconciliation"](#)
- [Section 1.6.3.3, "Viewing Reconciliation Rules in the Design Console"](#)

1.6.3.1 Reconciliation Rules for Target Resource Reconciliation

Reconciliation rules for target resource reconciliation can be divided into the following categories:

- [Section 1.6.3.1.1, "Reconciliation Rules for the Login Entity"](#)
- [Section 1.6.3.1.2, "Reconciliation Rules for the User Entity"](#)

1.6.3.1.1 Reconciliation Rules for the Login Entity Depending on the target system that you are using, the following are the reconciliation rules for the login entity:

- Rule name for IBM DB2 UDB:
DBUM DB2 Target Recon
- Rule name for Microsoft SQL Server:
DBUM MSSQL Login Target Recon
- Rule name for Oracle Database:
DBUM Oracle Target Recon
- Rule name for Sybase:
DBUM Sybase Login Target Recon

Rule element for IBM DB2 UDB and Oracle Database: User Login Equals User Name

In this rule:

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

Rule element for Microsoft SQL Server and Sybase: User Login Equals Login Name

In this rule:

- User Login is the field on the OIM User form.

- Login Name is the target system field.

1.6.3.1.2 Reconciliation Rules for the User Entity Depending on the target system that you are using, the following are the reconciliation rules for the user entity:

- Rule name for Microsoft SQL Server:
DBUM MSSQL User Target Recon
- Rule name for Sybase:
DBUM Sybase User Target Recon

Rule element for all user entity reconciliation rules : User Login Equals User Name

In this rule:

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

1.6.3.2 Reconciliation Rules for Trusted Source Reconciliation

For trusted source reconciliation, the same reconciliation rule is used for all target systems:

Rule name: DBUM Trusted Recon Rule

Rule element: User Login Equals User Login

In this rule element:

- The User Login field to the left of "Equals" is the field on the OIM User form.
- The User Login field to the right of "Equals" is the target system field.

1.6.3.3 Viewing Reconciliation Rules in the Design Console

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

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for the rule name.

1.6.4 Reconciliation Action Rules

The following sections provide information on the reconciliation action rules for reconciliation:

- [Section 1.6.4.1, "Reconciliation Action Rules for Target Resource Reconciliation"](#)
- [Section 1.6.4.2, "Reconciliation Action Rules for Trusted Source Reconciliation"](#)
- [Section 1.6.4.3, "Viewing Reconciliation Action Rules"](#)

1.6.4.1 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–6 lists the action rules for target resource reconciliation.

Table 1–6 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 *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

1.6.4.2 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–7 lists the action rules for trusted source reconciliation.

Table 1–7 Action Rules for Trusted Source Reconciliation

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

Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

1.6.4.3 Viewing Reconciliation Action Rules

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the resource object. The following are the names of the resource objects for each target system database:
 - Resource object for IBM DB2 UDB:
DB2 DB User
 - Resource object for Microsoft SQL Server login entity
MSSQL DB User Login
 - Resource object for Microsoft SQL Server user entity
MSSQL DB User

- Resource object for Oracle Database
Oracle DB User
 - Resource object for Sybase login entity
Sybase DB User Login
 - Resource object for Sybase login entity
Sybase DB User Login
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.

1.7 Connector Objects Used During Provisioning

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

See Also: The "Provisioning" section in *Oracle Identity Manager Connector Concepts* for conceptual information about provisioning

This section is divided into the following topics:

- [Section 1.7.1, "Provisioning Functions"](#)
- [Section 1.7.2, "Attributes for Provisioning"](#)

1.7.1 Provisioning Functions

The following sections list the supported provisioning functions and the corresponding adapters that perform these functions for each target system:

- [Section 1.7.1.1, "Provisioning Functions for IBM DB2 UDB"](#)
- [Section 1.7.1.2, "Provisioning Functions for Microsoft SQL Server"](#)
- [Section 1.7.1.3, "Provisioning Functions for Oracle Database"](#)
- [Section 1.7.1.4, "Provisioning Functions for Sybase"](#)

1.7.1.1 Provisioning Functions for IBM DB2 UDB

[Table 1–8](#) lists the supported provisioning functions and the adapters that perform these functions.

See Also: *Oracle Identity Manager Connector Concepts* for generic information about process tasks and adapters

Table 1–8 Provisioning Functions for IBM DB2 UDB

Function	Adapter
Create user	adpDBUMExecuteQuery
Delete user	adpDBUMExecuteQuery
Enable user	adpDBUMExecuteQuery
Disable user	adpDBUMExecuteQuery
Add tablespace	adpDBUMExecuteQuery

Table 1–8 (Cont.) Provisioning Functions for IBM DB2 UDB

Function	Adapter
Add schema	adpDBUMExecuteQuery
Update Tablespace	adpDBUMExecuteOldDataQuery
Delete Tablespace	adpDBUMExecuteOldDataQuery
Update Schema	adpDBUMExecuteOldDataQuery
Delete Schema	adpDBUMExecuteOldDataQuery
Update user name	adpDBUMPreventUpdate
Update tablespace grant option	adpDBUMPreventUpdate
Update schema grant option	adpDBUMPreventUpdate

1.7.1.2 Provisioning Functions for Microsoft SQL Server

Table 1–9 lists the supported provisioning functions and the adapters that perform these functions.

See Also: *Oracle Identity Manager Connector Concepts* for generic information about process tasks and adapters

Table 1–9 Provisioning Functions for Microsoft SQL Server

Function	Adapter
Login entity provisioning functions	
Create login	adpDBUMExecuteStoredProcForAuthTypeUser
Delete login	adpDBUMExecuteStoredProcForAuthTypeUser
Enable login	adpDBUMExecuteQueryForAuthTypeUser
Disable login	adpDBUMExecuteQueryForAuthTypeUser
Update login name	adpDBUMPreventUpdate
Update password	adpDBUMExecuteStoredProc
Update default language	adpDBUMExecuteStoredProc
Update default database	adpDBUMExecuteStoredProc
Update authentication type	adpDBUMPreventUpdate
User entity provisioning functions	
Create user	adpDBUMExecuteStoredProcForAuthTypeUser
Delete user	adpDBUMExecuteStoredProcForAuthTypeUser
Enable user	adpDBUMPreventEnable
Disable user	adpDBUMPreventDisable
Add role	adpDBUMExecuteStoredProc
Remove role	adpDBUMExecuteOldDataStoredProc
Update login name	adpDBUMPreventUpdate
Update user name	adpDBUMPreventUpdate
Update database group	adpDBUMExecuteStoredProc
Update role	adpDBUMExecuteOldDataStoredProc

1.7.1.3 Provisioning Functions for Oracle Database

[Table 1–10](#) lists the supported provisioning functions and the adapters that perform these functions.

See Also: *Oracle Identity Manager Connector Concepts* for generic information about process tasks and adapters

Table 1–10 Provisioning Functions for Oracle Database

Function	Adapter
Create user	adpDBUMExecuteQueryForAuthTypeUser
Delete user	adpDBUMExecuteQuery
Add role	adpDBUMExecuteQuery
Revoke role	adpDBUMExecuteOldDataQuery
Update role	adpDBUMExecuteOldDataQuery
Update role admin option	adpDBUMPreventFunctionality
Add privilege	adpDBUMExecuteQuery
Revoke privilege	adpDBUMExecuteQuery
Update privilege	adpDBUMExecuteOldDataQuery
Update privilege admin option	adpDBUMPreventFunctionality
Update user name	adpDBUMPreventFunctionality
Update default tablespace	adpDBUMExecuteQuery
Update default tablespace quota	adpDBUMExecuteQuery
Update temporary tablespace	adpDBUMExecuteQuery
Update temporary tablespace quota	adpDBUMExecuteQuery
Update authentication type	adpDBUMExecuteQueryForAuthTypeUser
Update global DN	adpDBUMExecuteQuery
Update password	adpDBUMExecuteQuery
Update profile name	adpDBUMExecuteQuery
Enable user	adpDBUMExecuteQuery
Disable user	adpDBUMExecuteQuery

1.7.1.4 Provisioning Functions for Sybase

[Table 1–11](#) lists the supported provisioning functions and the corresponding adapters that perform these functions. The functions listed in the table correspond to either a single or multiple process tasks.

See Also: *Oracle Identity Manager Connector Concepts* for generic information about process tasks and adapters

Table 1–11 Provisioning Functions for Sybase

Function	Adapter
Login entity provisioning functions	
Create login	adpDBUMExecuteStoredProc
Delete login	adpDBUMExecuteStoredProc
Enable login	adpDBUMExecuteStoredProc
Disable login	adpDBUMExecuteStoredProc
Update login name	adpDBUMPreventFunctionality
Update password	adpDBUMExecuteOldDataStoredProc
Update default language	adpDBUMExecuteStoredProc
Update default database	adpDBUMExecuteStoredProc
Update full name	adpDBUMExecuteStoredProc
Add role	adpDBUMExecuteStoredProc
Remove role	adpDBUMExecuteOldDataStoredProc
Update role	adpDBUMExecuteOldDataStoredProc
User entity provisioning functions	
Create user	adpDBUMExecuteStoredProc
Delete user	adpDBUMExecuteStoredProc
Disable user	adpDBUMPreventFunctionality
Enable user	adpDBUMPreventFunctionality
Update login name	adpDBUMPreventFunctionality
Update user name	adpDBUMPreventFunctionality

1.7.2 Attributes for Provisioning

This section discusses the following topics:

- [Section 1.7.2.1, "Attributes for Provisioning in IBM DB2 UDB"](#)
- [Section 1.7.2.2, "Attributes for Provisioning in Microsoft SQL Server"](#)
- [Section 1.7.2.3, "Attributes for Provisioning in Oracle Database"](#)
- [Section 1.7.2.4, "Attributes for Provisioning in Sybase"](#)

1.7.2.1 Attributes for Provisioning in IBM DB2 UDB

[Table 1–12](#) lists the process form fields and the corresponding target system column names for which you can specify or modify values during provisioning operations .

Table 1–12 Attributes for Provisioning in IBM DB2 UDB

Process Form Field	Target Table Name	Target Column Name	Description	Mandatory?
Username	SYSIBM.SYSDBAUTH	GRANTEE	User ID	Yes
User Type	SYSIBM.SYSDBAUTH	GRANTEETYPE	Type of user	Yes
Tablespace Child Form Fields				

Table 1–12 (Cont.) Attributes for Provisioning in IBM DB2 UDB

Process Form Field	Target Table Name	Target Column Name	Description	Mandatory?
Tablespace	SYSIBM.SYSSCHEMAAUTH	TBSPACE	Tablespace name	No
Tablespace Grant Option	NA	NA	Grant tablespace to user with the option to grant tablespaces to other users	No
Schema Child Form Fields				
Schema	SYSIBM.SYSSCHEMAAUTH	SCHEMANAME	Schema name	No
Schema Grant Option	NA	NA	Grant schema to user with the option to grant schemas to other users	No

1.7.2.2 Attributes for Provisioning in Microsoft SQL Server

Table 1–13 lists the process form fields and the corresponding target system column names for which you can specify or modify values during provisioning operations.

Table 1–13 Attributes for Provisioning in Microsoft SQL Server

Process Form Field	Stored Procedure	Description	Mandatory?
Login entity provisioning fields			
Login Name	<p>If the login account uses SQL Server authentication, then the following stored procedures are used:</p> <ul style="list-style-type: none"> sp_droplogin(:mssql_login) sp_addlogin(:mssql_login,:mssql_password,:mssql_dbname,:mssql_dbdefaultlang) <p>If the login account uses Microsoft Windows authentication, then the following stored procedures are used:</p> <ul style="list-style-type: none"> sp_revokelogin(:mssql_login) sp_grantlogin(:mssql_login) 	Login name	Yes
Password	sp_password(null,:mssql_pass,:mssql_login)	Login password	Yes, if the login account uses Microsoft SQL Server authentication.
Default Database	sp_defaultdb(:mssql_login,:mssql_dbname),	Default database name	Yes, if the login account uses Microsoft Windows authentication.
Default Language	sp_defaultlanguage(:mssql_login,:mssql_dbdefaultlang)	Default language	Yes, if the login account uses Microsoft Windows authentication.
Authentication Type		Type of authentication	Yes
User entity provisioning fields			

Table 1–13 (Cont.) Attributes for Provisioning in Microsoft SQL Server

Process Form Field	Stored Procedure	Description	Mandatory?
Login Name	sp_adduser(:mssql_parent_login,:mssql_user_id,null)	Existing login account name	Yes
Username	<p>If the login account associated with the user account uses SQL Server authentication, then the following stored procedures are used:</p> <p>sp_adduser(:mssql_parent_login,:mssql_user_id,null)</p> <p>sp_dropuser(:mssql_user_id)</p> <p>If the login account associated with the user account uses Microsoft Windows authentication, then the following stored procedures are used:</p> <p>sp_grantdbaccess(:mssql_parent_login,:mssql_user_id)</p> <p>sp_revokedbaccess(:mssql_user_id)</p>	User name	No
Database Name		Current database name in which the user account exists	No
Role Child Form Fields for User Entity			
Role	<p>sp_addrolemember(:mssql_role,:mssql_user_id)</p> <p>sp_droprolemember(:mssql_role,:mssql_user_id)</p>	Role name granted to user	no

1.7.2.3 Attributes for Provisioning in Oracle Database

Table 1–14 lists the process form fields for which you can specify or modify values during provisioning operations.

Table 1–14 Attributes for Provisioning in Oracle Database

Process Form Field	Target Table Name	Target Column Name	Description	Mandatory?
User Name	DBA_USERS	USERNAME	User name	Yes
Password	DBA_USERS	PASSWORD	User's password	Yes, if the user account uses password authentication
Authentication Type	DBA_USERS	PASSWORD	Type of authentication that user accounts use to connect to the database	Yes
Global DN	DBA_USERS	EXTERNAL_NAME	Distinguished external name that identifies the user at the enterprise directory server	No

Table 1–14 (Cont.) Attributes for Provisioning in Oracle Database

Process Form Field	Target Table Name	Target Column Name	Description	Mandatory?
Account Status	DBA_USERS	ACCOUNT_STATUS	Status of the user account	No
Default Tablespace	DBA_USERS	DEFAULT_TABLESPACE	Default tablespace	No
Default Tablespace Quota (in MB)	DBA_TS_QUOTAS	MAX_BYTES	Quota allocated to the user account on the tablespace	No
Temporary Tablespace	DBA_USERS	TEMPORARY_TABLESPACE	Temporary tablespace name	No
Temporary Tablespace Quota (in MB)	DBA_TS_QUOTAS	MAX_BYTES	Quota allocated to the user account on the tablespace	No
Profile Name	DBA_USERS	PROFILE	Name of the profile	No
Role Child Form Fields				
Role	DBA_ROLE_PRIVS	GRANTED_ROLE	Role name granted to user	No
Role Admin option	DBA_ROLE_PRIVS	ADMIN_OPTION	Grant role to user with the option to grant roles to other users	No
Privilege Child Form Fields				
Privilege	DBA_SYS_PRIVS	PRIVILEGE	Privilege name granted to user	No
Privilege Admin option	DBA_SYS_PRIVS	ADMIN_OPTION	Grant privilege to user with the option to grant privileges to other users	No

1.7.2.4 Attributes for Provisioning in Sybase

[Table 1–15](#) lists the process form fields for which you can specify or modify values during provisioning operations.

Table 1–15 Attributes for Provisioning in Sybase

Process Form Field	Stored Procedure Name	Description	Mandatory?
Login entity provisioning fields			
Login Name	sp_addlogin(:syb_login,:syb_pass ;:syb_defdb,:syb_deflang,:syb_fullname) sp_locklogin(:syb_login,'unlock') sp_locklogin(:syb_login,'lock') sp_droplogin(:syb_login)	Login name	Yes
Password	sp_password(:syb_old_pass,:syb_pass,:syb_login)	Login password	Yes
Default Database	sp_password(:syb_old_pass,:syb_pass,:syb_login)	Default database name	No

Table 1–15 (Cont.) Attributes for Provisioning in Sybase

Process Form Field	Stored Procedure Name	Description	Mandatory?
Default Language	sp_modifylogin(:syb_login,'default language';:syb_deflang),	Default language	No
Full Name	sp_modifylogin(:syb_login,'full name';:syb_fullname),	Full name of the login	No
Role Child Form Fields for Login Entity			
Role	sp_role('grant';:syb_role,:syb_login) sp_role('revoke';:syb_role,:syb_login)	Role name	No
User entity provisioning fields			
Login Name	sp_adduser(:syb_user_login,:syb_user_id,:syb_group)	Existing login account name	No
Username	sp_adduser(:syb_user_login,:syb_user_id,:syb_group) sp_dropuser(:syb_user_id)	User name	No
Database Group	sp_changegroup(:syb_group,:syb_user_id)	Database group name	No

1.8 Roadmap for Deploying and Using the Connector

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

- [Chapter 2, "Deploying the Connector"](#) describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- [Chapter 3, "Using the Connector"](#) describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- [Chapter 4, "Extending the Functionality of the Connector"](#) describes the procedures to perform if you want to extend the functionality of the connector.
- [Chapter 5, "Configuring the Connector for a JDBC-Based Database"](#) describes the procedures to perform if you want to use the connector for databases other than IBM DB2 UDB, Microsoft SQL Server, Oracle Database, and Sybase.
- [Chapter 6, "Testing the Connector"](#) describes procedures to test and troubleshoot the connector.
- [Chapter 7, "Known Issues"](#) lists known issues associated with this release of the connector.
- [Appendix A, "Preconfigured Lookup Definitions"](#) describes all the lookup definitions.

Deploying the Connector

The procedure to deploy the connector can be divided into the following stages:

- [Section 2.1, "Preinstallation"](#)
- [Section 2.2, "Installation"](#)
- [Section 2.3, "Postinstallation"](#)

2.1 Preinstallation

Preinstallation information is divided across the following sections:

- [Section 2.1.1, "Preinstallation on Oracle Identity Manager"](#)
- [Section 2.1.2, "Preinstallation on the Target System"](#)

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- [Section 2.1.1.1, "Files and Directories on the Installation Media"](#)
- [Section 2.1.1.2, "Determining the Release Number of the Connector"](#)
- [Section 2.1.1.3, "Creating a Backup of the Existing Common.jar File"](#)

2.1.1.1 Files and Directories on the Installation Media

[Table 2–1](#) describes the files and directories on the installation media.

Table 2–1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
config/DBUMLookUpQuery.properties	This file contains SQL queries that are used for lookup field synchronization.
config/DBUMReconQuery.properties	This file contains SQL queries and stored procedures that are used for reconciliation.
Files in the configuration directory	This directory contains the configuration files that are used by the Connector Installer during installation of the connector for a particular target system.
DB_User-Management-DB2-CI.xml	
DB_User-Management-MSSQL-CI.xml	
DB_User-Management-Oracle-CI.xml	
DB_User-Management-Sybase-CI.xml	
JavaDoc	This directory contains information about the Java APIs used by the connector.
lib/DBUM.jar	This file contains the class files required for performing provisioning and reconciliation. During connector deployment, this file is copied into the following directories: <i>OIM_HOME/xellerate/JavaTasks</i>
lib/DBUMCommon.jar	This JAR file contains utility classes that support provisioning and reconciliation operations. During connector deployment, this file is copied into the following directory: <i>OIM_HOME/xellerate/JavaTasks</i>
lib/Common.jar	This JAR file contains classes that are used by all release 9.1.0 connectors. During connector deployment, this file is copied into the following directory: <i>OIM_HOME/xellerate/JavaTasks</i>
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, this file is copied into the following directory: <i>OIM_HOME/xellerate/connectorResources</i> Note: A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
test/config/config.properties	This testing-utility file contains the attributes for Oracle Identity Manager to connect to the target system and perform provisioning operations.
test/config/log.properties	This file is used to store logging messages that are generated when you run the testing utility.

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

File in the Installation Media Directory	Description
test/scripts/DBUMTestingUtility.bat	These files are used to start the testing utility.
test/scripts/DBUMTestingUtility.sh	
Files in the xml directory	This directory contains XML files specific to a target system. The XML file contains definitions for the various connector objects, such as resource objects and scheduled tasks.
DBUserManagement-DB2-ConnectorConfig.xml	
DBUserManagement-MSSQL-ConnectorConfig.xml	<ul style="list-style-type: none"> Common IT resource type Process form for each login entity
DBUserManagement-Oracle-ConnectorConfig.xml	<ul style="list-style-type: none"> Process form for each user entity Adapters
DBUserManagement-Sybase-ConnectorConfig.xml	<ul style="list-style-type: none"> Process tasks for each login entity Process tasks for each user entity Resource objects for each login entity Resource objects for each user entity Provisioning Processes for each login entity
xml/DBUserManagementTrusted-ConnectorConfig.xml	This file contains the configuration for the OIM User. You import this file only if you plan to use the connector in trusted source reconciliation mode.

2.1.1.2 Determining the Release Number of the Connector

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the connector JAR file that is in the *OIM_HOME/xellerate/JavaTasks* directory.
2. Open the Manifest.mf file in a text editor. The Manifest.mf file is one of the files bundled inside the connector JAR file.

In the Manifest.mf file, the release number of the connector is displayed as the value of the Version property.

2.1.1.3 Creating a Backup of the Existing Common.jar File

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

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

If you have already installed a release 9.1.x connector (for example, Microsoft Active Directory User Management release 9.1.1) that was released after the current release of this connector, then back up the existing Common.jar file, install the Database User Management connector, and then restore the Common.jar file. The steps to perform this procedure are as follows:

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

1. Determine the release date of your existing release 9.1.x connector as follows:
 - a. Extract the contents of the following file in a temporary directory:
`OIM_HOME/xellerate/JavaTask/Common.jar`
 - b. Open the Manifest.mf file in a text editor.
 - c. Note down the Build Date and Build Version values.
2. Determine the release date of the Database User Management release 9.1.0 connector as follows:
 - a. On the installation media for the connector, extract the contents of the `lib/Common.jar` and then open the Manifest.mf file in a text editor.
 - b. Note down the Build Date and Build Version values.
3. If the Build Date and Build Version values for the Database User Management connector are less than the Build Date and Build Version values for the connector that is already installed, then:
 - a. Copy the `OIM_HOME/xellerate/JavaTask/Common.jar` to a temporary location.
 - b. After you perform the procedure described in [Section 2.2, "Installation"](#) overwrite the new Common.jar file in the `OIM_HOME/xellerate/JavaTask` directory with the Common.jar file that you backed up in the preceding step.

2.1.2 Preinstallation on the Target System

Preinstallation on the target system involves performing the following procedures:

- [Section 2.1.2.1, "Configuring Microsoft SQL Server"](#)
- [Section 2.1.2.2, "Using External Code Files"](#)

2.1.2.1 Configuring Microsoft SQL Server

If you are using Microsoft SQL Server 2000, then you must configure Microsoft SQL server by ensuring that:

- The target database in which users are to be created exists in the target Microsoft SQL Server installation.
- The TCP/IP port is enabled. The default port is 1433.

To enable the TCP/IP port:

 1. Open the Microsoft SQL Server Configuration Manager.
 2. Click **SQL Server Network Configuration**.
 3. Click **Protocols for MSSQLSERVER**.
 4. In the right frame, right-click **TCP/IP** and then click **Enable**.
- The TCP/IP port is not the only port enabled. Ports other than the TCP/IP port must also be enabled.
- Mixed mode authentication is enabled.

- The TCP/IP port is not blocked by a firewall.

2.1.2.2 Using External Code Files

Perform the steps given in one of the following sections to copy external code files:

Note: While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the contents of the `connectorResources` directory and the JAR files to the corresponding directories on each node of the cluster.

- [Section 2.1.2.2.1, "Copying External Code Files for IBM DB2 UDB"](#)
- [Section 2.1.2.2.2, "Copying External Code Files for Microsoft SQL Server"](#)
- [Section 2.1.2.2.3, "Copying External Code Files for Oracle Database"](#)
- [Section 2.1.2.2.4, "Copying External Code Files for Sybase"](#)

2.1.2.2.1 Copying External Code Files for IBM DB2 UDB Copy the `db2jcc.jar` and `db2jcc4.jar` files from the `DB2_HOME/IBM/SQLLIB/java` directory into the `OIM_HOME/xellerate/ThirdParty` directory.

2.1.2.2.2 Copying External Code Files for Microsoft SQL Server

Note: If your Oracle Identity Manager installation is running on Microsoft SQL Server, then you need not perform the instructions given in this section.

Depending on the version of Microsoft SQL Server that you are using, copy the required JAR files into the `OIM_HOME/xellerate/ThirdParty` directory:

- **Microsoft SQL Server 2000**

If you are using Microsoft SQL Server 2000 as the target system, then you must use the JDBC driver files: `mssqlserver.jar`, `msbase.jar`, and `msutil.jar`.

These files are shipped in the Microsoft SQL Server 2000 Driver for JDBC Service Pack 4, which you can download from the Microsoft Web site.

- **Microsoft SQL Server 2005**

If you are using Microsoft SQL Server 2005 as the target system, then the required external JAR file is the `sqljdbc.jar` JDBC driver file. This file can be downloaded from the Microsoft Web site.

- **Microsoft SQL Server 2008**

If you are using Microsoft SQL Server 2008 as the target system, then the required external JAR file is `sqljdbc4.jar`.

2.1.2.2.3 Copying External Code Files for Oracle Database If the connector is used with Oracle9i Database or Oracle Database 10g or 11g, then the required external code file is `ojdbc14.jar`.

These JAR files are available in the Oracle Database installation at, for example, the following path:

`ORACLE_HOME/jdbc/lib`

In this directory path, `ORACLE_HOME` is the location where Oracle Database is installed. For example, `C:\Oracle\ora92`.

You must copy the required JAR file (`classes12.jar` or `ojdbc14.jar`) into the `OIM_HOME/xellerate/ThirdParty` directory.

2.1.2.2.4 Copying External Code Files for Sybase Copy the `jconn2.jar` file from the `SYBASE_HOME/jConnect-5_5/classes` directory into the `OIM_HOME/xellerate/ThirdParty` directory.

2.2 Installation

Installing the connector on Oracle Identity Manager involves the following procedures:

- [Section 2.2.1, "Running the Connector Installer"](#)
- [Section 2.2.2, "Copying Files to the Oracle Identity Manager Host Computer"](#)

2.2.1 Running the Connector Installer

Note:

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

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory:
`OIM_HOME/xellerate/ConnectorDefaultDirectory`
2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console*.
3. Click **Deployment Management**, and then click **Install Connector**.
4. The Connector List list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory.

`OIM_HOME/xellerate/ConnectorDefaultDirectory`

You can select one of the following options:

- For IBM DB2 UDB:
DB2 DBUM User Management 9.1.0.0
- For Microsoft SQL Server:
MSSQL DBUM User Management 9.1.0.0
- For Oracle Database:
Oracle DBUM User Management 9.1.0.0
- For Sybase:
Sybase DBUM User Management 9.1.0.0

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 **DB User Management RELEASE_NUMBER**.
5. Click **Load**.
 6. To start the installation process, click **Continue**.

The following tasks are performed in sequence:

- a. Configuration of connector libraries
- b. Import of the connector XML file (through the Deployment Manager). If you want to import the target system as a trusted source for reconciliation, then see [Section 2.3.1.1, "Configuring the Target System As a Trusted Source"](#).
- c. Compilation of adapters

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

- Retry the installation by clicking **Retry**.
 - Cancel the installation and begin again from Step 1.
7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:
 - a. Ensuring that the prerequisites for using the connector are addressed

Note: At this stage, run the PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See [Section 2.3.1.4, "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 an IT resource for the connector

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

Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

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

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a clustered environment, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. Then, restart each node. See [Section 2.1.1.1, "Files and Directories on the Installation Media"](#) for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

Restoring the Common.jar File

If required, restore the Common.jar file that you had backed up by following the procedure described in [Section 2.1.1.3, "Creating a Backup of the Existing Common.jar File."](#)

2.2 Copying Files to the Oracle Identity Manager Host Computer

After you run the Connector Installer, you must manually copy the files listed in [Table 2–2](#).

Table 2–2 Files to Be Copied to the Oracle Identity Manager Host Computer

Files on the Installation Media	Destination Directory on the Oracle Identity Manager Host Computer
Files in the config directory	<i>OIM_HOME</i> /xellerate/XLintegrations/DBUM/config Note: You must create the DBUM/config directory.
Files in the test/config directory	<i>OIM_HOME</i> /xellerate/XLintegrations/DBUM/config
Files in the test/scripts directory	<i>OIM_HOME</i> /xellerate/XLintegrations/DBUM/scripts Note: You must create the DBUM/scripts directory.

2.3 Postinstallation

Postinstallation steps are divided across the following sections:

- [Section 2.3.1, "Postinstallation on Oracle Identity Manager"](#)
- [Section 2.3.2, "Creating the Administrator Account on Oracle Database Vault"](#)
- [Section 2.3.3, "Configuring Secure Communication Between the Target System and Oracle Identity Manager"](#)
- [Section 2.3.4, "Determining Values for the JDBC URL and Connection Properties Parameters"](#)
- [Section 2.3.5, "Configuring the IT Resource"](#)

2.3.1 Postinstallation on Oracle Identity Manager

This section discusses the following topics:

Note: In a clustered environment, you must perform this step on each node of the cluster.

- [Section 2.3.1.1, "Configuring the Target System As a Trusted Source"](#)
- [Section 2.3.1.2, "Changing to the Required Input Locale"](#)
- [Section 2.3.1.3, "Modifying the SVP Table"](#)

- [Section 2.3.1.4, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#)
- [Section 2.3.1.5, "Enabling Logging"](#)
- [Section 2.3.1.6, "Configuring the Connector for Incremental Reconciliation"](#)

2.3.1.1 Configuring the Target System As a Trusted Source

The target system can be designated as a trusted source or target resource. As discussed earlier in this guide, if you designate the target system as a **trusted source**, then during a reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

If you designate the target system as a **target resource**, then during a reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.
- Updates made to each account on the target system are propagated to the corresponding resource.

Note: You can skip this section if you do not want to designate the target system as a trusted source for reconciliation.

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, `DBUserManagementTrusted-ConnectorConfig.xml`, by using the Deployment Manager. This section describes the procedure to import the XML file.

Note: Only one target system can be designated as a trusted source. If you import the `DBUserManagementTrusted-ConnectorConfig.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

2. Depending on the target system that you use, specify values for the attributes of the corresponding scheduled task for trusted source reconciliation. This procedure is described later in this guide.

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the `DBUserManagementTrusted-ConnectorConfig.xml` file, which is in the `OIM_HOME/xellerate/ConnectorDefaultDirectory/DB_User_Management_9.1.0.0/xml` directory. 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**.

Note: After you import the XML file for trusted source reconciliation, you must also configure the scheduled task for trusted source reconciliation. The procedure is described in [Section 3.4.5, "Reconciliation Scheduled Tasks"](#).

2.3.1.2 Changing to the Required Input Locale

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

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

2.3.1.3 Modifying the SVP Table

Change the length of the SVP_FIELD_VALUE column in the SVP table to 2000 as follows:

1. Log in to the Oracle Identity Manager database by using the Oracle Identity Manager database user credentials.
2. Enter the following command at the SQL prompt:

For Oracle Database:

```
ALTER TABLE SVP MODIFY SVP_FIELD_VALUE VARCHAR2(2000);
```

For Microsoft SQL Server:

```
ALTER TABLE SVP ALTER COLUMN SVP_FIELD_VALUE VARCHAR(2000);
```

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

Whenever you add a new resource bundle in 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, change to the `OIM_HOME/xellerate/bin` directory.

Note: You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:

```
OIM_HOME\xellerate\bin\batch_file_name
```

2. Enter one of the following commands:

- On Microsoft Windows:

```
PurgeCache.bat ConnectorResourceBundle
```


- On UNIX:

```
PurgeCache.sh ConnectorResourceBundle
```

Note: You can ignore the exception that is thrown when you perform Step 2.

In this command, `ConnectorResourceBundle` is one of the content categories that you can remove from the server cache. Refer to the following file for information about the other content categories:

`OIM_HOME/xellerate/config/xlConfig.xml`

2.3.1.5 Enabling Logging

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. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- ALL

This level enables logging for all events.

- DEBUG

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

- INFO

This level enables logging of messages that highlight the progress of the application at a coarse-grained level.

- WARN

This level enables logging of information about potentially harmful situations.

- ERROR

This level enables logging of information about error events that may allow the application to continue running.

- FATAL

This level enables logging of information about very severe error events that could cause the application to stop functioning.

- OFF

This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **IBM WebSphere Application Server**

To enable logging:

1. Make the following changes in the `OIM_HOME/xellerate/config/log.properties`:

- Search for the following line:

```
log4j.rootLogger=WARN, stdout
```

Make this line a comment and remove the comment the line preceding this line.

- Locate and remove the comment from following lines:

```
#log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
#log4j.appender.logfile.DatePattern='.'yyyy-MM-dd
#log4j.appender.logfile.File=DIRECTORY_PATH/xel.log
#log4j.appender.logfile.MaxBackupIndex=20
#log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
#log4j.appender.logfile.layout.ConversionPattern=%p %t %c - %m%n
```

2. Specify the name and the location of the file to which the preceding logs have to be written. You can do this by changing the value of the following line:

```
log4j.appender.logfile.File=c:/oracle/xellerate/logs/xel.log
```

Replace `c:/oracle/xellerate/logs` with a valid directory location.

3. Add the following line in the `OIM_HOME/xellerate/config/log.properties` file:

```
log4j.logger.OIMCP.DBUM=log_level
log4j.logger.OIMCP.DBUMCOMMON=LOG_LEVEL
```

4. In this line, replace `log_level` with the log level to set.

For example:

```
log4j.logger.OIMCP.DBUM=DEBUG
log4j.logger.OIMCP.DBUMCOMMON=DEBUG
```

After you enable logging, the log information is written to the following file:

`DIRECTORY_PATH/xel.log`

■ JBoss Application Server

To enable logging:

1. In the `JBOSS_HOME/server/default/conf/jboss-log4j.xml` file, add the following lines:

```
<category name="OIMCP.DBUM">
  <priority value="log_level"/>
</category>
<category name="OIMCP.DBUMCOMMON">
  <priority value="LOG_LEVEL"/>
</category>
```

In case of cluster, make the changes in the following file:

`JBOSS_HOME/server/all/conf/jboss-log4j.xml`

2. In these lines, replace `log_level` with the log level that you want to set. For example:

```
<category name="OIMCP.DBUM">
  <priority value="DEBUG"/>
</category>
<category name="OIMCP.DBUMCOMMON">
  <priority value="DEBUG"/>
</category>
```

After you enable logging, the log information is written to the following file:

JBOSS_HOME\server\default\log\server.log

In case of cluster, the log information is written to the following file:

JBOSS_HOME\server\all\log\server.log

■ Oracle WebLogic Server

To enable logging:

1. Make the following changes in the *OIM_HOME*/xellerate/config/log.properties:

- Search for the following line:

```
log4j.rootLogger=WARN,stdout
```

Make this line a comment and remove the comment the line preceding this line.

- Locate and remove the comment from the following lines:

```
#log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
#log4j.appender.logfile.DatePattern='.'yyyy-MM-dd
#log4j.appender.logfile.File=DIRECTORY_PATH/xel.log
#log4j.appender.logfile.MaxBackupIndex=20
#log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
#log4j.appender.logfile.layout.ConversionPattern=%p %t %c - %m%n
```

2. Specify the name and the location of the file to which the preceding logs have to be written. You can do this by changing the value of the following line:

```
log4j.appender.logfile.File=c:/oracle/xellerate/logs/xel.log
```

Replace *c:/oracle/xellerate/logs* with a valid directory location.

3. Add the following line in the *OIM_HOME*/xellerate/config/log.properties file:

```
log4j.logger.OIMCP.DBUM=log_level
```

4. In this line, replace *log_level* with the log level that you want to set.

For example:

```
log4j.logger.OIMCP.DBUM=DEBUG
```

After you enable logging, the log information is written to the following file:

DIRECTORY_PATH/xel.log

2.3.1.6 Configuring the Connector for Incremental Reconciliation

Note: Perform the procedure described in this section to configure the connector for incremental reconciliation. If you are using Oracle Database as your target system, then you need not perform the procedure described in this section.

During an incremental reconciliation run, the scheduled task fetches only target system records that are added or modified after the time stamp stored in the Last Execution Time attribute of the scheduled task. The connector requires a query to

calculate the time-stamp value. This time-stamp value is used by the query that is used to perform reconciliation.

To configure the connector for incremental reconciliation, you must perform the following steps:

1. In a text editor, open the reconciliation properties file.
2. Enter a SQL query that returns in milliseconds the current date and time of the computer on which your database is running. The value returned by this query is stored as the value of the Last Execution Time attribute of the scheduled task.

The name of this query must be specified as the value of the Recon Time Query Name attribute while performing the procedure described in [Section 3.4.5, "Reconciliation Scheduled Tasks."](#)

For example, in Oracle Database the ORACLE_RECON_TIME query, in the properties file, is used for calculating a value for the Last Execution Time attribute:

```
SELECT (SYSDATE - TO_DATE('01011970', 'DDMMYYYY')) *24*60*60*1000 as ts FROM DUAL
```

The name of this query, ORACLE_RECON_TIME, is specified as the value of the Recon Time Query Name attribute while running the scheduled task.

3. Modify the query that is used to perform reconciliation by including a WHERE clause. The WHERE clause must contain the condition that determines if a target system record was added or modified after the time stamp stored in the Last Execution Time scheduled task attribute.

In the following example, the condition highlighted in bold has been added to the WHERE clause of the ORACLE_TARGET_USER_RECON query:

```
SELECT \
USERNAME, \
DECODE(PASSWORD, 'EXTERNAL', 'EXTERNAL', 'GLOBAL', 'GLOBAL', 'PASSWORD')
PASSWORD, \
EXTERNAL_NAME , \
DEFAULT_TABLESPACE, \
ACCOUNT_STATUS, \
TEMPORARY_TABLESPACE, \
PROFILE, \
SELECT BYTES FROM DBA_TS_QUOTAS WHERE dba.USERNAME = USERNAME AND
TABLESPACE_NAME = dba.DEFAULT_TABLESPACE) AS DEFAULT_TABLESPACE_QUOTA , \
SELECT BYTES FROM DBA_TS_QUOTAS WHERE dba.USERNAME = USERNAME AND
TABLESPACE_NAME = dba.TEMPORARY_TABLESPACE) AS TEMPORARY_TABLESPACE_QUOTA \
FROM DBA_USERS dba \
WHERE ((CREATED - TO_DATE('01011970','ddmmYYYY')) *24*60*60*1000) >
:lastExecutionTime
```

4. Save and close the file.

2.3.2 Creating the Administrator Account on Oracle Database Vault

Note: Perform the procedure described in this section only if you have Oracle Database Vault installed and you want to configure the connector for provisioning and reconciling authorization to Oracle Database Vault realms.

You must create an administrator account on Oracle Database Vault. This account is used by the connector for performing reconciliation and provisioning operations on Oracle Database Vault realms.

To create the administrator account on Oracle Database Vault:

1. Log in to Oracle Database Vault as a user with the DV_ACCTMGR privilege.
2. Create the administrator account by running the following command:

```
CREATE USER USERNAME IDENTIFIED BY PASSWORD;
```

3. Log out and then log in as a user with the DV_OWNER privilege.
4. Grant access to Oracle Database Vault and Data Dictionary realms by running the following commands:

```
exec DVSYS.DBMS_MACADM.ADD_AUTH_TO_REALM('Database Vault Account
Management', 'USERNAME', 'Enabled', 1)
exec DVSYS.DBMS_MACADM.ADD_AUTH_TO_REALM('Oracle Data
Dictionary', 'USERNAME', 'Enabled', 1)
```

5. Grant the DV_ADMIN and DV_SECANALYST privileges.
6. Log in as a user with the DV_ACCTMGR privilege..
7. Grant the DV_SECANALYST privilege.
8. Log in as SYS and grant the following privileges (run the command):

```
GRANT ANY OBJECT PRIVILEGE
GRANT ANY PRIVILEGE
GRANT ANY ROLE
UNLIMITED TABLESPACE
with ADMIN OPTION
to USERNAME
```

2.3.3 Configuring Secure Communication Between the Target System and Oracle Identity Manager

Note: It is recommended that you perform the procedure described in this section to secure communication between the target system and Oracle Identity Manager.

The procedure to secure communication depends on the database that you are using:

- [Section 2.3.3.1, "Configuring Secure Communication Between IBM DB2 UDB and Oracle Identity Manager"](#)
- [Section 2.3.3.2, "Configuring Secure Communication Between Microsoft SQL Server and Oracle Identity Manager"](#)
- [Section 2.3.3.3, "Configuring Secure Communication Between Oracle Database and Oracle Identity Manager"](#)
- [Section 2.3.3.4, "Configuring Secure Communication Between Sybase and Oracle Identity Manager"](#)

2.3.3.1 Configuring Secure Communication Between IBM DB2 UDB and Oracle Identity Manager

Note: IBM DB2 UDB version 9.1 Fix Pack 2 and later support secure communication over SSL.

To configure secure communication between IBM DB2 UDB and Oracle Identity Manager:

1. See IBM DB2 UDB documentation for information about enabling SSL communication between IBM DB2 UDB and a client system. In this context, the client is Oracle Identity Manager.

Export the certificate on the IBM DB2 UDB host computer.

2. Copy the certificate to the Oracle Identity Manager host computer.
3. Import the certificate into the JVM truststore of the application server on which Oracle Identity Manager is running.

To import the certificate into the truststore, run the following command:

```
..\..\bin\keytool -import -file FILE_LOCATION -keystore TRUSTSTORE_LOCATION
-storepass TRUSTSTORE_PASSWORD -trustcacerts -alias ALIAS
```

In this command:

- Replace *FILE_LOCATION* with the full path and name of the certificate file.
- Replace *ALIAS* with an alias for the certificate.
- Replace *TRUSTSTORE_PASSWORD* with a password for the truststore.
- Replace *TRUSTSTORE_LOCATION* with one of the truststore paths from [Table 2–3](#). This table shows the location of the truststore for each of the supported application servers.

Note: For a clustered configuration, you must import the file into the truststore on each node of the cluster.

Table 2–3 Truststore Locations on Supported Application Servers

Application Server	Truststore Location
Oracle WebLogic Server	<i>WEBLOGIC_HOME</i> /java/jre/lib/security/cacerts
IBM WebSphere Application Server	<i>WEBSPHERE_HOME</i> /java/jre/lib/security/cacerts
JBoss Application Server	<i>JAVA_HOME</i> /jre/lib/security/cacerts

4. To enable secure communication between IBM DB2 UDB and Oracle Identity Manager, set the value of the isSecure IT resource parameter to *yes*. You must provide a value for this parameter while performing the procedure described in [Section 2.3.5, "Configuring the IT Resource."](#)

2.3.3.2 Configuring Secure Communication Between Microsoft SQL Server and Oracle Identity Manager

To configure secure communication between Microsoft SQL Server and Oracle Identity Manager:

1. See Microsoft SQL Server documentation for information about enabling SSL communication between Microsoft SQL Server and a client system. In this context, the client is Oracle Identity Manager.

Export the certificate on the Microsoft SQL Server host computer.

2. Copy the certificate to the Oracle Identity Manager host computer.
3. Import the certificate into the JVM truststore of the application server on which Oracle Identity Manager is running.

To import the certificate into the truststore, run the following command:

```
..\..\bin\keytool -import -file FILE_LOCATION -keystore TRUSTSTORE_LOCATION
-storepass TRUSTSTORE_PASSWORD -trustcacerts -alias ALIAS
```

In this command:

- Replace *FILE_LOCATION* with the full path and name of the certificate file.
- Replace *ALIAS* with an alias for the certificate.
- Replace *TRUSTSTORE_PASSWORD* with a password for the truststore.
- Replace *TRUSTSTORE_LOCATION* with one of the truststore paths from [Table 2–4](#). This table shows the location of the truststore for each of the supported application servers.

Note: For a clustered configuration, you must import the file into the truststore on each node of the cluster.

Table 2–4 Truststore Locations on Supported Application Servers

Application Server	Truststore Location
Oracle WebLogic Server	<i>WEBLOGIC_HOME</i> /java/jre/lib/security/cacerts
IBM WebSphere Application Server	<i>WEBSPHERE_HOME</i> /java/jre/lib/security/cacerts
JBoss Application Server	<i>JAVA_HOME</i> /jre/lib/security/cacerts

4. To enable secure communication between Microsoft SQL Server and Oracle Identity Manager, set the value of the isSecure IT resource parameter to yes. You must provide a value for this parameter while performing the procedure described in [Section 2.3.5, "Configuring the IT Resource"](#).

2.3.3.3 Configuring Secure Communication Between Oracle Database and Oracle Identity Manager

To secure communication between Oracle Database and Oracle Identity Manager, you can perform either one or both of the following procedures:

- [Section 2.3.3.3.1, "Configuring Data Encryption and Integrity in Oracle Database"](#)
- [Section 2.3.3.3.2, "Configuring SSL Communication in Oracle Database"](#)

2.3.3.3.1 Configuring Data Encryption and Integrity in Oracle Database Refer to *Oracle Database Advanced Security Administrator's Guide* for information about configuring data encryption and integrity.

2.3.3.3.2 Configuring SSL Communication in Oracle Database

Note: The Database User Management connector does not support SSL communication between an Oracle Database target system and Oracle Identity Manager running on IBM WebSphere Application Server or Oracle Application Server. This is also mentioned in [Chapter 7, "Known Issues"](#) (see Bug 6696248).

To enable SSL communication between Oracle Database and Oracle Identity Manager:

1. See *Oracle Database Advanced Security Administrator's Guide* for information about enabling SSL communication between Oracle Database and Oracle Identity Manager.

Export the certificate on the Oracle Database host computer.

2. Copy the certificate to Oracle Identity Manager.
3. Import the certificate into the JVM truststore of the application server on which Oracle Identity Manager is running.

To import the certificate into the truststore, run the following command:

```
..\..\bin\keytool -import -file FILE_LOCATION -keystore TRUSTSTORE_LOCATION
-storepass TRUSTSTORE_PASSWORD -trustcacerts -alias ALIAS
```

In this command:

- Replace *FILE_LOCATION* with the full path and name of the certificate file.
- Replace *ALIAS* with an alias for the certificate.
- Replace *TRUSTSTORE_PASSWORD* with a password for the truststore.
- Replace *TRUSTSTORE_LOCATION* with one of the truststore paths from [Table 2–5](#). This table shows the location of the truststore for each of the supported application servers.

Note: For a clustered configuration, you must import the file into the truststore on each node of the cluster.

Table 2–5 Truststore Locations on Supported Application Servers

Application Server	Truststore Location
Oracle WebLogic Server	<i>WEBLOGIC_HOME</i> /java/jre/lib/security/cacerts
JBoss Application Server	<i>JAVA_HOME</i> /jre/lib/security/cacerts

4. To enable secure communication between Oracle Database and Oracle Identity Manager, set the value of the isSecure IT resource parameter to *yes*. You must provide a value for this parameter while performing the procedure described in [Section 2.3.5, "Configuring the IT Resource"](#).

2.3.3.4 Configuring Secure Communication Between Sybase and Oracle Identity Manager

To configure secure communication between Sybase and Oracle Identity Manager:

1. See Sybase Adaptive Server Enterprise documentation for information about enabling SSL communication between Sybase and a client system. In this context, the client is Oracle Identity Manager.

Export the certificate on the Sybase host computer.

2. Copy the certificate to the Oracle Identity Manager host computer.
3. Import the certificate into the JVM truststore of the application server on which Oracle Identity Manager is running.

To import the certificate into the truststore, run the following command:

```
..\..\bin\keytool -import -file FILE_LOCATION -keystore TRUSTSTORE_LOCATION
-storepass TRUSTSTORE_PASSWORD -trustcacerts -alias ALIAS
```

In this command:

- Replace *FILE_LOCATION* with the full path and name of the certificate file.
- Replace *ALIAS* with an alias for the certificate.
- Replace *TRUSTSTORE_PASSWORD* with a password for the truststore.
- Replace *TRUSTSTORE_LOCATION* with one of the truststore paths from [Table 2–6](#). This table shows the location of the truststore for each of the supported application servers.

Note: For a clustered configuration, you must import the file into the truststore on each node of the cluster.

Table 2–6 Truststore Locations on Supported Application Servers

Application Server	Truststore Location
Oracle WebLogic Server	<i>WEBLOGIC_HOME</i> /java/jre/lib/security/cacerts
IBM WebSphere Application Server	<i>WEBSHERE_HOME</i> /java/jre/lib/security/cacerts
JBoss Application Server	<i>JAVA_HOME</i> /jre/lib/security/cacerts

4. To enable secure communication between Sybase and Oracle Identity Manager, set the value of the isSecure IT resource parameter to yes. You must provide a value for this parameter while performing the procedure described in [Section 2.3.5, "Configuring the IT Resource"](#).

2.3.4 Determining Values for the JDBC URL and Connection Properties Parameters

This section discusses the JDBC URL and Connection Properties parameters. You apply the information in this section while performing the procedure described in [Section 2.3.5, "Configuring the IT Resource"](#).

The values that you specify for the Database URL and Connection Properties parameters depend on the target system:

- [Section 2.3.4.1, "JDBC URL and Connection Properties for IBM DB2 UDB"](#)
- [Section 2.3.4.2, "JDBC URL and Connection Properties for Microsoft SQL Server"](#)

- [Section 2.3.4.3, "JDBC URL and Connection Properties for Oracle Database"](#)
- [Section 2.3.4.4, "JDBC URL and Connection Properties for Sybase Adaptive Server Enterprise"](#)

2.3.4.1 JDBC URL and Connection Properties for IBM DB2 UDB

The following are guidelines on specifying the JDBC URL and Connection Properties parameters:

- **JDBC URL parameter**

Enter the following component of the connection URL as the value of the JDBC URL provider:

```
jdbc:db2://[SERVER_NAME][:PORT_NUMBER]/[DATABASE_NAME]
```

In this format:

- *SERVER_NAME* is the IP address (not the host name) of the target system host computer.
- *PORT_NUMBER* is the port at which the target system database is listening.
- *DATABASE_NAME* is the name of the database we are connecting.

The following is a sample value for the Database URL parameter:

```
jdbc:db2://192.168.16.76:50000/DBUSER
```

- **Connection Properties parameter**

Enter the following component of the connection URL as the value of the Connection Properties parameter:

```
[, PROPERTY=VALUE[, PROPERTY=VALUE]] . . .
```

In this format:

- *PROPERTY* is the name of one or more database connection properties, such as `applicationName` and `disableStatementPooling`.
- *VALUE* is the value of each database connection property whose name you specify by using the *PROPERTY* placeholder.

Note: Semicolons must be changed to commas in the value that you specify.

The following is a sample value for the Connection Properties parameter:

```
databaseName=sales,port=50000
```

If you enable SSL communication between IBM DB2 UDB and Oracle Identity Manager, then you must include the `javax.net.ssl.trustStore`, and `javax.net.ssl.trustStorePassword` properties in the Decode value that you specify for the SSL Keystore Properties Code Key entry in the `Lookup.DBUM.DB2.Configuration` lookup definition. In other words, the Decode value of the SSL Keystore Properties Code Key must be in the following format:

```
javax.net.ssl.trustStore=STORE_LOCATION~javax.net.ssl.trustStorePassword=STORE_PASSWORD
```

When you specify this value, replace *STORE_LOCATION* with the full path and name of the truststore, and replace *STORE_PASSWORD* with the password of the truststore.

For example:

```
Djavax.net.ssl.trustStore=C:/j2sdk1.4.2_12/jre/lib/security/cacerts~javax.net.s
sl.trustStorePassword=changeit
```

2.3.4.2 JDBC URL and Connection Properties for Microsoft SQL Server

Note: In Microsoft SQL Server documentation, the term "connection URL" is used instead of "JDBC URL."

■ JDBC URL parameter

Enter the following component of the connection URL as the value of the JDBC URL provider:

```
jdbc:sqlserver://[SERVER_NAME][:PORT_NUMBER][;database=DATABASE_NAME]
```

In this format:

- *SERVER_NAME* is the IP address (not the host name) of the target system host computer.
- *PORT_NUMBER* is the port at which the target system database is listening.
- *DATABASE_NAME* is the name of the database we are connecting.

The following is a sample value for the Database URL parameter:

```
jdbc:sqlserver://192.168.16.76:1433;database=model
```

■ Connection Properties parameter

Enter the following component of the connection URL as the value of the Connection Properties parameter:

```
[;PROPERTY=VALUE[;PROPERTY=VALUE]] . . .
```

In this format:

- *PROPERTY* is the name of one or more database connection properties, such as `applicationName` and `disableStatementPooling`.
- *VALUE* is the value of each database connection property whose name you specify by using the *PROPERTY* placeholder.

Note: Semicolons must be changed to commas in the value that you specify.

The following is a sample value for the Connection Properties parameter:

```
databaseName=sales,port=1433
```

If you enable SSL communication between Microsoft SQL Server and Oracle Identity Manager, then you must include the `encrypt` and `hostNameInCertificate` properties in the value that you specify for the

Connection Properties parameter. In other words, the following must be part of the string that you enter as the value of the parameter:

```
encrypt=true,hostNameInCertificate=HOST_NAME
```

Replace *HOST_NAME* with the host name given in the certificate that you use.

In addition, you must specify the location of the truststore if you import the certificate into a truststore other than the JVM truststore of Oracle Identity Manager. To specify the location of the truststore, include the following properties in the value that you specify for the Connection Properties parameter:

```
encrypt=true,hostNameInCertificate=HOST_NAME,trustStore=STORE_LOCATION,trustStorePassword=STORE_PASSWORD
```

When you specify this value, replace *STORE_LOCATION* with the full path and name of the truststore, and replace *STORE_PASSWORD* with the password of the truststore.

2.3.4.3 JDBC URL and Connection Properties for Oracle Database

The values that you specify for the JDBC URL and Connection Properties parameters depend on the security measures that you have implemented:

- [Section 2.3.4.3.1, "Only Data Encryption and Integrity Is Configured"](#)
- [Section 2.3.4.3.2, "Only SSL Communication Is Configured"](#)
- [Section 2.3.4.3.3, "Both Data Encryption and Integrity and SSL Communication Are Configured"](#)

If you are using Oracle Database with RAC implementation as the target system, then enter a value for the JDBC URL property in the format specified in the following section:

[Section 2.3.4.3.4, "JDBC URL and Connection Properties for Oracle RAC"](#)

2.3.4.3.1 Only Data Encryption and Integrity Is Configured If you have configured only data encryption and integrity, then enter the following values:

- **JDBC URL parameter**

While configuring the IT resource, the value that you specify for the JDBC URL parameter must be in the following format:

```
jdbc:oracle:thin:@TARGET_HOST_NAME_or_IP_ADDRESS:PORT_NUM:sid
```

The following is a sample value for the JDBC URL parameter:

```
jdbc:oracle:thin:@ten.mydomain.com:1521:cust_db
```

- **Connection Properties parameter**

After you configure data encryption and integrity, the connection properties are recorded in the `sqlnet.ora` file. The value that you must specify for the Connection Properties parameter is explained by the following sample scenario:

See Also: *Oracle Database Advanced Security Administrator's Guide* for information about the `sqlnet.ora` file

Suppose the following entries are recorded in the `sqlnet.ora` file:

```
SQLNET.ENCRYPTION_SERVER=REQUIRED  
SQLNET.ENCRYPTION_TYPES_SERVER=(3DES168, DES40, DES, 3DES112)
```

```
SQLNET.CRYPTO_CHECKSUM_SERVER=REQUESTED
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER=(SHA1,MD5)
```

While configuring the IT resource, you must specify the following as the value of the Connection Properties parameter:

Note:

- The property-value pairs must be separated by commas.
 - As shown in the following example, for the `encryption_types` and `crypto_checksum_types` properties, you can select any of the values recorded in the `sqlnet.ora` file.
-
-

```
oracle.net.encryption_client=REQUIRED,oracle.net.encryption_types_client=(3DES168),oracle.net.crypto_checksum_client=REQUESTED,oracle.net.crypto_checksum_types_client=(MD5)
```

2.3.4.3.2 Only SSL Communication Is Configured After you configure SSL communication, the JDBC URL is recorded in the `tnsnames.ora` file. See *Oracle Database Net Services Reference* for detailed information about the `tnsnames.ora` file.

The following are sample formats of the contents of the `tnsnames.ora` file. In these formats, `DESCRIPTION` contains the connection descriptor, `ADDRESS` contains the protocol address, and `CONNECT_DATA` contains the database service identification information.

Sample Format 1:

```
NET_SERVICE_NAME=
(DESCRIPTION=
  (ADDRESS= (PROTOCOL_ADDRESS_INFORMATION) )
  (CONNECT_DATA=
    (SERVICE_NAME=SERVICE_NAME) ) )
```

Sample Format 2:

```
NET_SERVICE_NAME=
(DESCRIPTION_LIST=
  (DESCRIPTION=
    (ADDRESS= (PROTOCOL_ADDRESS_INFORMATION) )
    (ADDRESS= (PROTOCOL_ADDRESS_INFORMATION) )
    (ADDRESS= (PROTOCOL_ADDRESS_INFORMATION) )
    (CONNECT_DATA=
      (SERVICE_NAME=SERVICE_NAME) ) )
  (DESCRIPTION=
    (ADDRESS= (PROTOCOL_ADDRESS_INFORMATION) )
    (ADDRESS= (PROTOCOL_ADDRESS_INFORMATION) )
    (ADDRESS= (PROTOCOL_ADDRESS_INFORMATION) )
    (CONNECT_DATA=
      (SERVICE_NAME=SERVICE_NAME) ) ) )
```

Sample Format 3:

```
NET_SERVICE_NAME=
(DESCRIPTION=
  (ADDRESS_LIST=
    (LOAD_BALANCE=on)
    (FAILOVER=off)
    (ADDRESS= (PROTOCOL_ADDRESS_INFORMATION) )
```

```
(ADDRESS=(PROTOCOL_ADDRESS_INFORMATION)) )  
(ADDRESS_LIST=  
(LOAD_BALANCE=off)  
(FAILOVER=on)  
(ADDRESS=(PROTOCOL_ADDRESS_INFORMATION))  
(ADDRESS=(PROTOCOL_ADDRESS_INFORMATION)) )  
(CONNECT_DATA=  
(SERVICE_NAME=SERVICE_NAME)) )
```

If you have configured only SSL communication and imported the certificate that you create on the target system host computer into the JVM truststore of Oracle Identity Manager, then enter the following values:

JDBC URL parameter

While configuring the IT resource, the value that you specify for the JDBC URL parameter must be derived from the value of *NET_SERVICE_NAME* in the *tnsnames.ora* file. For example:

Note: As shown in this example, you must include only the
(ADDRESS=(*PROTOCOL*=TCPS) (*HOST*=*HOST_NAME*) (*PORT*=2484))
element because you are configuring SSL. You need not include other
(ADDRESS=(*PROTOCOL_ADDRESS_INFORMATION*)) elements.

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS) (HOST=myhost)  
(PORT=2484))) (CONNECT_DATA=(SERVER=DEDICATED) (SERVICE_NAME=mysid)))
```

Connection Properties parameter

Whether you need to specify a value for the Connection Properties parameter depends on the truststore into which you import the certificate:

- If you import the certificate into the truststore of the JVM that Oracle Identity Manager is using, then you need not specify a value for the Connection Properties parameter.
- If you import the certificate into any other truststore, then while creating the connector, specify a value for the Connection Properties parameter in the following format:

```
javax.net.ssl.trustStore=STORE_LOCATION, javax.net.ssl.trustStoreType=JKS, javax.  
net.ssl.trustStorePassword=STORE_PASSWORD
```

When you specify this value, replace *STORE_LOCATION* with the full path and name of the truststore, and replace *STORE_PASSWORD* with the password of the truststore.

2.3.4.3.3 Both Data Encryption and Integrity and SSL Communication Are Configured If both data encryption and integrity and SSL communication are configured, then:

JDBC URL parameter

While configuring the IT resource, to specify a value for the JDBC URL parameter, enter a comma-separated combination of the values for the JDBC URL parameter described in [Section 2.3.4.3.1, "Only Data Encryption and Integrity Is Configured"](#) and [Section 2.3.4.3.2, "Only SSL Communication Is Configured"](#). For example:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS) (HOST=myho  
st) (PORT=2484))) (CONNECT_DATA=(SERVER=DEDICATED) (SERVICE_NAME=mysid)))
```

- **Connection Properties parameter**

While configuring the IT resource, , to specify a value for the Connection Properties parameter, enter a comma-separated combination of the values for the Connection Properties parameter described in [Section 2.3.4.3.1, "Only Data Encryption and Integrity Is Configured"](#) and [Section 2.3.4.3.2, "Only SSL Communication Is Configured"](#). For example:

```
oracle.net.encryption_client=REQUIRED,oracle.net.encryption_types_client=(3DES168),oracle.net.crypto_checksum_client=REQUESTED,oracle.net.crypto_checksum_type_s_client=(MD5),javax.net.ssl.trustStore=STORE_LOCATION,javax.net.ssl.trustStoreType=JKS,javax.net.ssl.trustStorePassword=STORE_PASSWORD
```

As shown in the following example, for the `encryption_types` and `crypto_checksum_types` properties, you can select any of the values recorded in the `sqlnet.ora` file. When you specify this value, replace `STORE_LOCATION` with the full path and name of the truststore, and replace `STORE_PASSWORD` with the password of the truststore.

2.3.4.3.4 JDBC URL and Connection Properties for Oracle RAC

The following are guidelines on specifying the JDBC URL and Connection Properties parameters:

- **JDBC URL parameter**

While configuring the IT resource, the value that you specify for the JDBC URL parameter must be in the following format:

Note: The JDBC URL connection string must not exceed 200 characters.

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=HOST1_NAME.DOMAIN)(PORT=PORT1_NUMBER))(ADDRESS=(PROTOCOL=TCP)(HOST=HOST2_NAME.DOMAIN)(PORT=PORT2_NUMBER))(ADDRESS=(PROTOCOL=TCP)(HOST=HOST3_NAME.DOMAIN)(PORT=PORT3_NUMBER))... (ADDRESS=(PROTOCOL=TCP)(HOST=HOSTn_NAME.DOMAIN)(PORT=PORTn_NUMBER))(CONNECT_DATA=(SERVICE_NAME=ORACLE_DATABASE_SERVICE_NAME)))
```

Sample value:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=host1.example.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host2.example.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host3.example.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host4.example.com)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=svce1)))
```

- **Connection Properties parameter**

While configuring the IT resource, do not specify any value for the Connection Properties parameter.

2.3.4.4 JDBC URL and Connection Properties for Sybase Adaptive Server Enterprise

The following are guidelines on specifying the JDBC URL and Connection Properties parameters:

- **JDBC URL parameter**

Enter the following component of the connection URL as the value of the JDBC URL provider:

```
jdbc:sybase:Tds:SERVER_NAME:PORT_NUMBER/DATABASE_NAME
```

In this format:

- *SERVER_NAME* is the IP address (not the host name) of the target system host computer.
- *PORT_NUMBER* is the port at which the target system database is listening.
- *DATABASE_NAME* is the name of the target system database.

The following is a sample value for the JDBC URL parameter:

```
jdbc:sybase:Tds:172.21.109.62:9050/master
```

■ Connection Properties parameter

Enter the following component of the connection URL as the value of the Connection Properties parameter:

```
[, PROPERTY=VALUE[, PROPERTY=VALUE]] . . .
```

In this format:

- *PROPERTY* is the name of one or more database connection properties, such as `applicationName` and `disableStatementPooling`.
- *VALUE* is the value of each database connection property whose name you specify by using the *PROPERTY* placeholder.

The following is a sample value for the Connection Properties parameter:

```
databaseName=sales,port=9000
```

If you enable SSL communication between Sybase Adaptive Server Enterprise and Oracle Identity Manager, then you must include the `SYB SOCKET_FACTORY` property in the value that you specify for the Connection Properties parameter. In other words, the following must be part of the string that you enter as the value of the parameter:

```
SYB SOCKET_FACTORY=VALUE
```

Replace *VALUE* with the of the class that implements `com.sybase.jdbcx.SybSocketFactory`; or `"DEFAULT"`, which instantiates a new `java.net.Socket()`.

2.3.5 Configuring the IT Resource

Note: Perform the procedure described in this section if you are using IBM DB2 UDB, Microsoft SQL Server, Oracle Database, and Sybase as your target system. For all other databases, proceed to [Chapter 5, "Configuring the Connector for a JDBC-Based Database."](#)

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

1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.

3. Click **Manage IT Resources**.
4. In the IT Resource Name field on the Manage IT Resource page, enter the name of one of the following IT resources, and then click **Search**:
 - For IBM DB2 UDB, enter DB2UDB.
 - For Microsoft SQL Server, enter MS SQL Server.
 - For Oracle Database, enter Oracle.
 - For Sybase, enter Sybase.
5. Click the edit icon for the 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. [Table 2–7](#) describes each parameter.

Table 2–7 IT Resource Parameters

Parameter	Description
Admin ID	<p>Enter the user name of the target system account to be used for connector operations.</p> <p>Note: If you are configuring the connector for Oracle Database Vault, then you must enter the user name of the account that you had created in Section 2.3.2, "Creating the Administrator Account on Oracle Database Vault."</p> <p>Sample value: sysadm</p> <p>See the "Target system user account" row in Table 1–1 more information.</p>
Admin Password	<p>Enter the password of the target system account specified by the Admin ID parameter.</p> <p>Note: If you are configuring the connector for Oracle Database Vault, then you must enter the password of the account that you had created in Section 2.3.2, "Creating the Administrator Account on Oracle Database Vault."</p>
Database Driver	<p>Depending on the target system that you are using, enter one of the following values as the JDBC driver class name:</p> <ul style="list-style-type: none"> ■ For IBM DB2 UDB: <code>com.ibm.db2.jcc.DB2Driver</code> ■ For Microsoft SQL Server: <code>com.microsoft.sqlserver.jdbc.SQLServerDriver</code> ■ For Oracle Database: <code>oracle.jdbc.driver.OracleDriver</code> ■ For Sybase: <code>com.sybase.jdbc2.jdbc.SybDriver</code> ■ For other databases, enter the corresponding JDBC driver class name
JDBC URL	<p>Specify the JDBC URL for the target system database.</p> <p>See Section 2.3.4, "Determining Values for the JDBC URL and Connection Properties Parameters" for information about the JDBC URL value that you must enter.</p>

Table 2–7 (Cont.) IT Resource Parameters

Parameter	Description
Configuration Lookup	<p>This parameter holds the name of the lookup definition that stores configuration information for connector operations.</p> <p>If you have configured your target system as a target resource, then enter one of the following values:</p> <ul style="list-style-type: none"> ■ For IBM DB2 UDB: <code>Lookup.DBUM.DB2.Configuration</code> ■ For Microsoft SQL Server: <code>Lookup.DBUM.MSSQL.Configuration</code> ■ For Oracle Database: <code>Lookup.DBUM.Oracle.Configuration</code> ■ For Sybase: <code>Lookup.DBUM.Sybase.Configuration</code> ■ For other databases, enter the corresponding Configuration lookup definition name. <p>If you have configured your target system as a trusted source, then enter one of the following values:</p> <ul style="list-style-type: none"> ■ For IBM DB2 UDB: <code>Lookup.DBUM.DB2.TrustedRecon.Configuration</code> ■ For Microsoft SQL Server: <code>Lookup.DBUM.MSSQL.TrustedRecon.Configuration</code> ■ For Oracle Database: <code>Lookup.DBUM.Oracle.TrustedRecon.Configuration</code> ■ For Sybase: <code>Lookup.DBUM.Sybase.TrustedRecon.Configuration</code> ■ For other databases, enter the corresponding Configuration lookup definition name.
Database Name	<p>If you are using Microsoft SQL Server or Sybase as the target system for creating users, then specify a value for this parameter. Otherwise, do not enter any value.</p> <p>This parameter holds the name of the database as specified in the JDBC URL parameter.</p> <p>Sample value: <code>master</code></p>
isSecure	<p>Enter <code>yes</code> if you plan to configure SSL to secure communication between Oracle Identity Manager and the target system. Otherwise, enter <code>no</code>.</p> <p>Default value: <code>no</code></p>
Connection Properties	<p>Specify the connection properties for the target system database.</p> <p>See Section 2.3.4, "Determining Values for the JDBC URL and Connection Properties Parameters" for information about the connection properties value that you must enter.</p>
Connection Pooling Parameters	
Abandoned connection timeout	<p>Enter the time (in seconds) after which a connection must be automatically closed if it is not returned to the pool.</p> <p>Note: You must set this parameter to a value that is high enough to accommodate processes that take a long time to complete (for example, full reconciliation).</p> <p>Default value: <code>600</code></p>
Connection wait timeout	<p>Enter the maximum time (in seconds) for which the connector must wait for a connection to be available.</p> <p>Default value: <code>60</code></p>
Inactive connection timeout	<p>Enter the time (in seconds) of inactivity after which a connection must be dropped and replaced by a new connection in the pool.</p> <p>Default value: <code>600</code></p>

Table 2–7 (Cont.) IT Resource Parameters

Parameter	Description
Initial pool size	<p>Enter the number of connections that must be established when the connection pool is initialized.</p> <p>The pool is initialized when it receives the first connection request from a connector.</p> <p>Default value: 1</p>
Max pool size	<p>Enter the maximum number of connections that must be established in the pool at any point of time.</p> <p>This number includes the connections that have been borrowed from the pool.</p> <p>Default value: 100</p>
Min pool size	<p>Enter the minimum number of connections that must be in the pool at any point of time.</p> <p>This number includes the connections that have been borrowed from the pool.</p> <p>Default value: 5</p>
Validate connection on borrow	<p>Enter <code>true</code> if you want connections to be validated before they are lent by the pool. Otherwise, enter <code>false</code>.</p> <p>It is recommended that you set the value to <code>true</code>.</p> <p>Default value: <code>false</code></p>
Timeout check interval	<p>Enter the time interval (in seconds) at which the other timeouts specified by the other parameters must be checked.</p> <p>Default value: 30</p>
Pool preference	<p>This parameter holds the preferred connection pooling implementation.</p> <p>Value: <code>Default</code></p> <p>Note: Do not change this value of this parameter.</p>
Connection pooling supported	<p>Enter <code>true</code> if you want to enable connection pooling for this target system installation. Otherwise, enter <code>false</code>.</p> <p>Default value: <code>false</code></p>
Target supports only one connection	<p>This parameter indicates whether the target system can support one or more connections at a time.</p> <p>Value: <code>false</code></p> <p>Note: Do not change the value of this parameter.</p>
ResourceConnection class definition	<p>This parameter holds the implementation of the ResourceConnection class.</p> <p>Value: <code>oracle.iam.connectors.dbum.common.db.util.DBUMResourceConnectionImpl</code></p> <p>Note: Do not change the value of this parameter.</p>
Native connection pool class definition	<p>This parameter holds the name of the wrapper to the native pool mechanism that implements the GenericPool class.</p> <p>Note: Do not specify a value for this parameter.</p>

Table 2–7 (Cont.) IT Resource Parameters

Parameter	Description
Pool excluded fields	<p>This parameter holds a list of comma-separated list of IT parameters whose change must not trigger a refresh of the connector pool</p> <p>Value: Configuration Lookup Name,Manage TCA Record,Enable Revoked User,Statement Timeout,Context User ID,Context Application Name,Context Responsibility Name,TopologyName,SSO Enabled,SSO Identifier,SSO Login Attribute,SSO IT Resource,Manage HR Record</p> <p>Note:</p> <p>Do not change the value of this parameter unless you are adding or deleting a parameter from the IT resource. You must ensure that the total length of the list does not exceed 2000 characters. If you are adding a parameter to the IT resource, then that parameter name must be added to the above list with a comma separator. If you are deleting a parameter from the IT resource, then that parameter must be removed from the list if it exists in the list.</p> <p>You must restart Oracle Identity Manager for changes that you make to this parameter to take effect.</p>
Connection Retries	<p>Enter the number of consecutive attempts to be made at establishing a connection with the target system.</p> <p>Default value: 2</p>
Connection wait timeout	<p>Enter the time in milliseconds within which the target system is expected to respond to a connection attempt.</p> <p>For a particular connection attempt, if the target system does not respond within the time interval specified by the Connection Timeout parameter, then it is assumed that the connection attempt has failed.</p> <p>Default value: 60</p>
Retry Interval	<p>Enter the interval in milliseconds between consecutive attempts at establishing a connection with the target system.</p> <p>Default value: 1000</p>

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

Using the Connector

This chapter is divided into the following sections:

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

- [Section 3.1, "Setting Up Lookup Definitions in Oracle Identity Manager"](#)
- [Section 3.2, "Guidelines on Configuring Reconciliation"](#)
- [Section 3.3, "Scheduled Task for Lookup Field Synchronization"](#)
- [Section 3.4, "Configuring Reconciliation"](#)
- [Section 3.5, "Configuring Scheduled Tasks"](#)
- [Section 3.6, "Guidelines on Performing Provisioning Operations"](#)
- [Section 3.7, "Performing Provisioning Operations"](#)

3.1 Setting Up Lookup Definitions in Oracle Identity Manager

You must provide Decode values for some of the entries of the following lookup definitions.

To set a Decode value for an entry in a lookup definition:

1. On the Design Console, expand **Administration**, and then double-click **Lookup Definition**.
2. Search for and open the lookup definition that you want to modify.
3. Enter the value in the **Decode** column for the Code Key that you want to set.
4. Click the Save icon.

Depending on whether you have configured your target system as a trusted source of target resource, see one of the following sections for information about the entries for which you must specify Decode values:

- [Section 3.1.1, "Setting Up the Configuration Lookup Definition for a Target Resource"](#)
- [Section 3.1.2, "Setting Up the Configuration Lookup Definition for a Trusted Source"](#)
- [Section 3.1.3, "Setting Up the ExclusionList Lookup Definition"](#)

3.1.1 Setting Up the Configuration Lookup Definition for a Target Resource

Depending on the target system that you are using, the following is the list of Configuration lookup definitions:

- For IBM DB2 UDB: Lookup.DBUM.DB2.Configuration
- For Microsoft SQL Server: Lookup.DBUM.MSSQL.Configuration
- For Oracle Database: Lookup.DBUM.Oracle.Configuration
- For Sybase: Lookup.DBUM.Sybase.Configuration

Provide Decode values for the following entries of the Configuration lookup definition:

- Reconciliation Query Property File
Enter the full path and name of the file containing queries that must be run during reconciliation.
- Reconciliation SQL Injection Keywords
Enter the list of SQL keywords that must not be used in the reconciliation query. Use the tilde (~) character as a separator if you want to specify more than one SQL keyword. During target resource reconciliation runs, the connector does not run a query (used for target resource reconciliation) that contains any of the keywords listed in the Decode column.
- Reserved Words List
Enter the list of reserved words that are not supported in the OIM User process form fields during provisioning operations. Use the tilde (~) character as a separator if you want to specify more than one reserved word.
- Target Date Format
Enter the format in which date values are stored on the target system.
- Unsupported Special Characters
Enter the list of special characters that are not supported in the process form fields during provisioning operations.
Sample value: #*~^

3.1.2 Setting Up the Configuration Lookup Definition for a Trusted Source

Depending on the target system that you are using, the following is the list of Configuration lookup definitions:

- For IBM DB2 UDB: Lookup.DBUM.DB2.TrustedRecon.Configuration
- For Microsoft SQL Server: Lookup.DBUM.MSSQL.TrustedRecon.Configuration
- For Oracle Database: Lookup.DBUM.Oracle.TrustedRecon.Configuration
- For Sybase: Lookup.DBUM.Sybase.TrustedRecon.Configuration

Provide Decode values for the following entries of the Configuration lookup definition:

- Reconciliation Query Property File
Enter the full path and name of the file containing queries that must be run during reconciliation.
- Reconciliation SQL Injection Keywords

Enter the list of SQL keywords that must not be used in the reconciliation query. Use the tilde (~) character as a separator if you want to specify more than one SQL keyword. During trusted source reconciliation runs, the connector does not run a query that contains any of the keywords listed in the Decode column.

- **Target Date Format**

Enter the format in which date values are stored on the target system.

3.1.3 Setting Up the ExclusionList Lookup Definition

In the ExclusionList lookup definition, enter the user attributes of the target system accounts for which you do not want to perform target resource reconciliation and provisioning as follows:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Depending on the target system that you are using, search for and open one of the following lookup definitions:
 - Lookup.DBUM.DB2.ExclusionList
 - Lookup.DBUM.MSSQL.ExclusionList
 - Lookup.DBUM.Oracle.ExclusionList
 - Lookup.DBUM.Sybase.ExclusionList
3. Click **Add**.
4. If you want to specify the target system accounts on which you do not want to perform provisioning, then:
 - a. In the Code Key column, enter the name of the process form field.
 - b. In the Decode column, enter tilde-separated list of values for the process form field.

For example, if you are using IBM DB2 UDB as your target system and you do not want to provision users with user names DB2 admin, JDoe, and DFinn, then populate the lookup definition with the following values:

Code Key	Decode
UD_DB_DB2_U_USERNAME	DB2 admin~JDoe~DFinn

5. If you want to specify the target system accounts on which you do not want to perform target resource reconciliation, then:
 - a. In the Code Key column, enter the reconciliation field of the resource object.
 - b. In the Decode column, enter a tilde-separated list of values for the reconciliation field of resource object

For example, if you are using IBM DB2 UDB as your target system and you do not want to reconcile user account data of John, Mary, and Anna, then populate the lookup definition with the following values:

Code Key	Decode
User Name	John~Mark~Anna

6. Click the Save icon.

3.2 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, the scheduled task for lookup field synchronization must be run before user reconciliation runs.
- The scheduled task for user or login reconciliation must be run before the scheduled task for reconciliation of deleted user or login data.
- After you configure batched reconciliation, if reconciliation fails during a batched reconciliation run, then rerun the scheduled task without changing the values of the task attributes.

3.3 Scheduled Task for Lookup Field Synchronization

The DBUM Lookup reconciliation scheduled task is used for lookup field synchronization. [Table 3–1](#) describes the attributes of this scheduled task. The procedure to configure scheduled tasks is described later in the guide.

Table 3–1 Attributes of the DBUM Lookup reconciliation Scheduled Task

Attribute	Description
IT Resource	<p>Enter the name of the IT resource that you configure by performing the procedure described in Section 2.3.5, "Configuring the IT Resource"</p> <p>Sample value: Oracle</p>
Lookup Definition Name	<p>Enter the name of the lookup definition in Oracle Identity Manager that you want to synchronize with the target system. Depending on the target system that you are using, the value can be one of the following:</p> <ul style="list-style-type: none"> ■ For IBM DB2 UDB, the value can be one of the following: <ul style="list-style-type: none"> - Lookup.DBUM.DB2.Tablespace - Lookup.DBUM.DB2.Schema ■ For Microsoft SQL Server, the value can be one of the following: <ul style="list-style-type: none"> - Lookup.DBUM.MSSQL.DBNames - Lookup.DBUM.MSSQL.DBRoles - Lookup.DBUM.MSSQL.DefaultLang ■ For Oracle Database, the value can be one of the following: <ul style="list-style-type: none"> - Lookup.DBUM.Oracle.Profiles - Lookup.DBUM.Oracle.Roles - Lookup.DBUM.Oracle.Privileges - Lookup.DBUM.Oracle.Temp.Tablespace - Lookup.DBUM.Oracle.Tablespace ■ For Sybase, the value can be one of the following: <ul style="list-style-type: none"> - Lookup.DBUM.Sybase.Databases - Lookup.DBUM.Sybase.Roles - Lookup.DBUM.Sybase.DefaultLang - Lookup.DBUM.Sybase.DBGroups <p>Sample value: Lookup.DBUM.Oracle.Roles</p>
Exclusion List	<p>Enter the lookup value in the target system lookup fields that you do not want to synchronize with the corresponding lookup definitions in Oracle Identity Manager.</p> <p>If you want to specify more than one lookup value that must be excluded during lookup field synchronization, then enter a tilde-separated list of lookup values.</p> <p>If you do not want to exclude any lookup value, then leave the default value for this attribute unchanged.</p> <p>The following is an example of a list of role lookup values in Oracle Database that must be excluded during lookup reconciliation:</p> <p>CONNECT~RESOURCE</p>

Table 3–1 (Cont.) Attributes of the DBUM Lookup reconciliation Scheduled Task

Attribute	Description
Task Name	This attribute holds the name of the scheduled task. Value: <code>DBUM Lookup reconciliation</code> Note: You must not change this value.
Ref Data Provider Impl	This attribute holds the name of the class that implements the logic for lookup field synchronization. Default value: <code>MapResultSetProvider</code> Note: You must not change this value.
Query Properties File Path	Enter the full path and name of the file containing the lookup definition synchronization query that you want to run. Sample value: <code>/usr/temp/DBUMLookupQuery.properties</code>

3.4 Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- [Section 3.4.1, "Performing Full Reconciliation"](#)
- [Section 3.4.2, "Reconciliation Time Stamp"](#)
- [Section 3.4.3, "Batched Reconciliation"](#)
- [Section 3.4.4, "Configuring Limited Reconciliation"](#)
- [Section 3.4.5, "Reconciliation Scheduled Tasks"](#)

3.4.1 Performing Full Reconciliation

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

To perform a full reconciliation run, specify values for the following attributes while performing the procedure described in [Section 3.4.5, "Reconciliation Scheduled Tasks"](#):

- **Last Execution Time:** This attribute holds the time stamp at which the last reconciliation run started. You must set the value of this attribute to 0.
- **Custom Query:** This attribute holds the query for filtering records returned during reconciliation. If you need to perform full reconciliation, then accept the default value of `NODATA` for this attribute.
- **Use Custom Query:** Set the value of this attribute to `No`.

For Oracle Database, at the end of the full reconciliation run, the Last Execution Time attribute is automatically set to the time stamp at which the run started. For other target systems, the Last Execution Time attribute is automatically set to the time stamp at which the run started only if you have performed the procedure described in [Section 2.3.1.6, "Configuring the Connector for Incremental Reconciliation"](#). From the next run onward, only records created or modified after this time stamp value are considered for reconciliation.

3.4.2 Reconciliation Time Stamp

This section describes the Last Execution Time attribute of the scheduled task.

The Last Execution Time attribute holds the time stamp at which the last reconciliation run started. This attribute is used in conjunction with the reconciliation query specified by the Query Name attribute. During a reconciliation run, only target system records added or modified after the time stamp value stored in the Last Execution Time attribute are fetched into Oracle Identity Manager for reconciliation.

Apply the following guidelines while deciding on a value for the Last Execution Time attribute:

- If you want to fetch all target system records for reconciliation, then set the value of the attribute to 0.
- If you want to specify a time stamp, then first run the query to convert the time stamp into the required format.

For example, on Oracle Database, you first run the following query:

```
SELECT (TO_DATE('DATE_TO_BE_CONVERTED', 'DD-MON-YYYY') - TO_DATE('01011970', 'DDMMYYYY')) *24*60*60*1000 as ts FROM DUAL
```

In this query, replace *DATE_TO_BE_CONVERTED* with the date that you want to use as the time stamp. For example, if you want to use 5-Dec-2008 as the time stamp, then run the following query:

```
SELECT (TO_DATE('5-Dec-2008', 'DD-MON-YYYY') - TO_DATE('01011970', 'DDMMYYYY')) *24*60*60*1000 as ts FROM DUAL
```

The query returns the following value:

```
1228435200000
```

Specify this value as the value of the Last Execution Time attribute.

- The Last Execution Time attribute is updated during each reconciliation run. For example, the Last Execution Time attribute is set to the time stamp at which the run begins.

3.4.3 Batched Reconciliation

Note: You can configure the connector to perform batched reconciliation only if you are using IBM DB2 UDB or Oracle Database as the target system.

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure batched reconciliation to avoid these problems.

To configure batched reconciliation, you must specify values for the following attributes while performing the procedure described in [Section 3.4.5, "Reconciliation Scheduled Tasks"](#):

- Use Batched Reconciliation: Use this attribute to enable batched reconciliation. Set the value of this attribute to Yes.

- **Batch Reconciliation Query Name:** Use this attribute to specify the name of the batched reconciliation query in the reconciliation query file that you want to run.
- **Batch Size:** Use this attribute to specify the number of records that must be included in each batch. The default value is 100.

3.4.4 Configuring Limited Reconciliation

Note: This section describes an optional procedure. Perform this procedure only if you want to add filter parameters for 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 can configure limited reconciliation by performing the procedures described in one of the following sections:

- [Section 3.4.4.1, "Specifying a Value for the Custom Query Attribute"](#)
- [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#)

3.4.4.1 Specifying a Value for the Custom Query Attribute

If your target system database uses stored procedures to retrieve user records, and your database does not support filtering of records returned by the store procedure, then you can use the Custom Query scheduled task attribute to configure limited reconciliation. You set the value of the Custom Query attribute while performing the procedure described in [Section 3.4.5.1, "Scheduled Tasks for Reconciling Data About Users and Logins"](#).

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

RESOURCE_OBJECT_FIELD_NAME=VALUE

For example, if you specify `Last Name=Doe` as the value of the Custom Query attribute, then only records for persons whose last name is Doe are considered for reconciliation.

You can add multiple query conditions by using a combination of resource object attributes and the following logical operators:

- The AND operator represented by the ampersand (&)
- The OR operator represented by the vertical bar (|)
- The EQUAL operator represented by the equal sign (=)

For example, the following query condition is used to limit reconciliation to records of those persons whose first name is John and last name is Doe:

`First Name=John & Last Name=Doe`

The following query condition can be used to limit reconciliation to the records of those persons whose first name is either John or their User ID is 219786:

`First Name=John | User ID=219786`

You must apply the following guidelines while creating the query condition:

- Use only the equal sign (=), ampersand (&), and vertical bar (|) in the query condition. Do not include any other special characters in the query condition. Any other character that is included is treated as part of the value that you specify.
- Add a space before and after ampersand and vertical bars used in the query condition. For example:

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

This is to ensure to help the system distinguish between ampersands and vertical bars used in the query and the same characters included as part of attribute values specified in the query condition.

- You must not include unnecessary blank spaces between operators and values in the query condition.

A query condition with spaces separating values and operators would yield different results as compared to a query condition that does not contain spaces between values and operators. For example, the output of the following query conditions would be different:

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

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

In the second query condition, the reconciliation engine would look for first name and last name values that contain a space at the start.

3.4.4.2 Adding a Filter Parameter in the Reconciliation Query

If your target system database enables you to add a WHERE clause to the query that you use to retrieve user records, then you can configure limited reconciliation by adding a filter parameter in the reconciliation query and specifying a value for the parameter in the Query Filter lookup definition.

For example, you can add a parameter in the WHERE clause of the ORACLE_TARGET_USER_RECON query so that it returns records of users whose user name is the one that you specify in the lookup definition.

To add a filter parameter in a reconciliation query:

Note: Before you modify a query in the properties file, run the query by using any standard database client to ensure that the query produces the required results when it is run against the target system database.

1. Modify the query as follows:
 - a. Open the properties file in a text editor.
 - b. Add the WHERE clause with the condition to the query that you want to modify.

Note: The parameter name must begin with the colon (:) as a prefix. In addition, there must be no space between the colon and parameter name and within the parameter name.

For example, in the following snippet of the ORACLE_TARGET_USER_RECON query, the variable condition highlighted in bold has been added:

```
WHERE ((CREATED - TO_DATE('01011970','ddmmyyyy')) *24*60*60*1000) >
:lastExecutionTime \
AND USERNAME = :username
```

- c. Save and close the file.
2. Configure the Query Filter lookup definition as follows:
 - a. Log in to the Design Console.
 - b. Expand the **Administration** folder, and then double-click **Lookup Definition**.
 - c. If you have configured the target system as trusted source, then search for and open the appropriate lookup definition:
 - Lookup.DBUM.DB2.TrustedRecon.QueryFilter
 - Lookup.DBUM.MSSQL.TrustedRecon.QueryFilter
 - Lookup.DBUM.Oracle.TrustedRecon.QueryFilter
 - Lookup.DBUM.Sybase.TrustedRecon.QueryFilter
 - d. If you have configured the target system as target resource, then search for and open the appropriate lookup definition:
 - Lookup.DBUM.DB2.TargetRecon.QueryFilter
 - Lookup.DBUM.MSSQL.TargetRecon.QueryFilter
 - Lookup.DBUM.Oracle.TargetRecon.QueryFilter
 - Lookup.DBUM.Sybase.TargetRecon.QueryFilter
 - e. To add a row, click **Add**.
 - f. In the **Code Key** column, enter the variable name that you specified in the properties file. Do not include the colon (:) character. For example, enter username in the Code Key column.
 - g. In the **Decode** column, enter the value that you want to assign to the parameter for subsequent reconciliation runs.
Sample value: jdoe
 - h. Click the Save icon.

When you next run the query that you have modified, the condition that you add is applied as an additional filter during reconciliation.

3.4.5 Reconciliation Scheduled Tasks

This connector supports both trusted source and target resource reconciliation. When you run the connector installer, the following scheduled tasks are automatically created in Oracle Identity Manager:

- [Section 3.4.5.1, "Scheduled Tasks for Reconciling Data About Users and Logins"](#)
- [Section 3.4.5.2, "Scheduled Tasks for Reconciling Data About Deleted Users or Logins"](#)

3.4.5.1 Scheduled Tasks for Reconciling Data About Users and Logins

The following scheduled tasks are used to reconcile user or login data:

- **Scheduled tasks for target resource reconciliation**
 - For IBM DB2 UDB: DBUM DB2 Target Resource User Reconciliation
 - For the Microsoft SQL Server login entity: DBUM MSSQL Target Resource Login Reconciliation
 - For the Microsoft SQL Server user entity: DBUM MSSQL Target Resource User Reconciliation
 - For Oracle Database: DBUM Oracle Target Resource User Reconciliation
 - For the Sybase login entity: DBUM Sybase Target Resource Login Reconciliation
 - For the Sybase user entity: DBUM Sybase Target Resource User Reconciliation
- **Scheduled tasks for trusted source reconciliation**
 - For IBM DB2 UDB: DBUM DB2 Trusted Source User Reconciliation
 - For Microsoft SQL Server: DBUM MSSQL Trusted Source User Reconciliation
 - For Oracle Database: DBUM Oracle Trusted Source User Reconciliation
 - For the Sybase user entity: DBUM Sybase Trusted Source User Reconciliation

[Table 3–2](#) describes the attributes of these scheduled tasks.

Note:

- Values for most attributes 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 would not be performed.
 - The descriptions of some attributes also instruct you not to change the default values. However, if you create a copy of this scheduled task, then you can enter attribute values specific to the target system installation for which you create the copy of scheduled task. See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for more information about creating copies of connector objects.
-
-

Table 3–2 Attributes of Scheduled Tasks for Fetching Data About Users or Logins During Target Resource Reconciliation

Attribute	Description
Batch Reconciliation Query Name	<p>Enter the name of the query that you want the connector to apply during batched reconciliation.</p> <p>Note: This attribute is valid only when the Use Batched Reconciliation attribute is set to Yes. This attribute is discussed later in this table.</p>
Batch Size	<p>Enter the number of records that must be included in each batch fetched from the target system.</p> <p>Default value: 100</p> <p>This attribute is discussed in Section 3.4.3, "Batched Reconciliation."</p>
Custom Query	<p>Enter the query that you want the connector to apply during reconciliation. See Section 3.4.4, "Configuring Limited Reconciliation" for more information.</p> <p>Default value: NODATA</p> <p>Note: This attribute is valid only when the Use Custom Query attribute is set to Yes.</p> <p>If you enter a value for this attribute, then you must not enter a value for the Reconciliation Query Filter Lookup attribute. The Reconciliation Query Filter Lookup attribute is discussed later in this table.</p>
Is Login Recon	<p>Specifies whether or not reconciliation is to be carried out for the login entity of the target system.</p> <p>Enter Yes if you want to reconcile data about the login entity for your target system. Otherwise, enter No.</p>
Is Trusted Recon	<p>If you want reconciliation to be carried out in trusted mode, then enter Yes. Enter No if you want reconciliation to be carried out in target resource mode.</p>
IT Resource Name	<p>Enter the name of the IT resource that you configure by performing the procedure described in Section 2.3.5, "Configuring the IT Resource".</p> <p>Default value:</p> <ul style="list-style-type: none"> ■ Value for IBM DB2 UDB: DB2UDB ■ Value for Microsoft SQL Server: MS SQL Server ■ Value for Oracle Database: Oracle ■ Value for Sybase: Sybase
Last Execution Time	<p>This attribute holds the time stamp at which the last reconciliation run started.</p> <p>Default value: 0</p> <p>See Section 3.4.2, "Reconciliation Time Stamp" for information about setting a value for the Last Execution Time attribute.</p>
Query Name	<p>Enter the name of the query in the reconciliation query file that you want to run.</p> <p>Default value:</p> <ul style="list-style-type: none"> ■ Value for IBM DB2 UDB: DB2_TARGET_USER_RECON ■ Value for Microsoft SQL Server: SQL_SERVER_LOGIN ■ Value for Oracle Database: ORACLE_TARGET_USER_RECON ■ Value for Sybase: SYBASE_LOGIN

Table 3–2 (Cont.) Attributes of Scheduled Tasks for Fetching Data About Users or Logins During Target Resource Reconciliation

Attribute	Description
Reconciliation Attribute Mapping Lookup	<p>This attribute holds the name of the lookup definition that maps resource object attributes with column names or column name aliases used in the reconciliation query.</p> <p>For target resource reconciliation</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>Lookup.DBUM.DB2.TargetRecon.Mapping</code> Value for Microsoft SQL Server login entity: <code>Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping</code> Value for Microsoft SQL Server user entity: <code>Lookup.DBUM.MSSQL.TargetRecon.User.Mapping</code> Value for Oracle Database: <code>Lookup.DBUM.Oracle.TargetRecon.Mapping</code> Value for Sybase login entity: <code>Lookup.DBUM.Sybase.TargetRecon.Login.Mapping</code> Value for Sybase user entity: <code>Lookup.DBUM.Sybase.TargetRecon.User.Mapping</code> <p>For trusted source reconciliation</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>Lookup.DBUM.DB2.TrustedRecon.Mapping</code> Value for Microsoft SQL Server: <code>Lookup.DBUM.MSSQL.TrustedRecon.Mapping</code> Value for Oracle Database: <code>Lookup.DBUM.Oracle.TrustedRecon.Mapping</code> Value for Sybase: <code>Lookup.DBUM.DB2.TrustedRecon.Mapping</code> <p>Note: You must not change this value.</p>
Reconciliation Query Filter Lookup	<p>This attribute holds the name of the lookup definition that contains information about reconciliation filter parameters.</p> <p>For target resource reconciliation</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>Lookup.DBUM.DB2.TargetRecon.QueryFilter</code> Value for Microsoft SQL Server: <code>Lookup.DBUM.MSSQL.TargetRecon.QueryFilter</code> Value for Oracle Database: <code>Lookup.DBUM.Oracle.TargetRecon.QueryFilter</code> Value for Sybase: <code>Lookup.DBUM.Sybase.TargetRecon.QueryFilter</code> <p>For trusted source reconciliation</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>Lookup.DBUM.DB2.TrustedRecon.QueryFilter</code> Value for Microsoft SQL Server: <code>Lookup.DBUM.MSSQL.TrustedRecon.QueryFilter</code> Value for Oracle Database: <code>Lookup.DBUM.Oracle.TrustedRecon.QueryFilter</code> Value for Sybase: <code>Lookup.DBUM.Sybase.TrustedRecon.QueryFilter</code> <p>Note: You must ensure that the filter parameters in this lookup definition can be applied along with the query specified by the Query Name attribute. An error is encountered if this condition is not met.</p>

Table 3–2 (Cont.) Attributes of Scheduled Tasks for Fetching Data About Users or Logins During Target Resource Reconciliation

Attribute	Description
Reconciliation Transformation Lookup	<p>This attribute holds the name of the lookup definition that is used to configure transformation of attribute values fetched from the target system during reconciliation.</p> <p>For target resource reconciliation</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>Lookup.DBUM.DB2.TargetRecon.Transformation</code> Value for Microsoft SQL Server login entity: <code>Lookup.DBUM.MSSQL.TargetRecon.Login.Transformation</code> Value for Microsoft SQL Server user entity: <code>Lookup.DBUM.MSSQL.TargetRecon.User.Transformation</code> Value for Oracle Database: <code>Lookup.DBUM.Oracle.TargetRecon.Transformation</code> Value for Sybase login entity: <code>Lookup.DBUM.Sybase.TargetRecon.Login.Transformation</code> Value for Sybase user entity: <code>Lookup.DBUM.Sybase.TargetRecon.User.Transformation</code> <p>For trusted source reconciliation</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>Lookup.DBUM.DB2.TrustedRecon.Transformation</code> Value for Microsoft SQL Server: <code>Lookup.DBUM.MSSQL.TrustedRecon.Transformation</code> Value for Oracle Database: <code>Lookup.DBUM.Oracle.TrustedRecon.Transformation</code> Value for the Sybase entity: <code>Lookup.DBUM.Sybase.TrustedRecon.Transformation</code> <p>Note: This attribute is valid only when the Use Transformation for Reconciliation attribute is set to Yes. That attribute is discussed later in this table.</p>
Reconciliation Validation Lookup	<p>This attribute 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.</p> <p>For target resource reconciliation</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>Lookup.DBUM.DB2.TargetRecon.Validation</code> Value for Microsoft SQL Server login entity: <code>Lookup.DBUM.MSSQL.TargetRecon.Login.Validation</code> Value for Microsoft SQL Server user entity: <code>Lookup.DBUM.MSSQL.TargetRecon.Login.Transformation</code> Value for Oracle Database: <code>Lookup.DBUM.Oracle.TargetRecon.Validation</code> Value for Sybase login entity: <code>Lookup.DBUM.Sybase.TargetRecon.Login.Validation</code> Value for Sybase user entity: <code>Lookup.DBUM.Sybase.TargetRecon.User.Validation</code> <p>For trusted source reconciliation</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>Lookup.DBUM.DB2.TrustedRecon.Validation</code> Value for Microsoft SQL Server: <code>Lookup.DBUM.MSSQL.TrustedRecon.ValidationValidation</code> Value for Oracle Database: <code>Lookup.DBUM.Oracle.TrustedRecon.Validation</code> Value for the Sybase entity: <code>Lookup.DBUM.Sybase.TrustedRecon.Validation</code> <p>Note: This attribute is valid only when the Use Validation for Reconciliation attribute is set to Yes. That attribute is discussed later in this table.</p>

Table 3–2 (Cont.) Attributes of Scheduled Tasks for Fetching Data About Users or Logins During Target Resource Reconciliation

Attribute	Description
Recon Time Query Name	<p>Enter the name of the query in the reconciliation query file that is used to fetch the current time of the target system for incremental reconciliation.</p> <p>For IBM DB2 UDB, Microsoft SQL Server, and Sybase, enter the name of the query that you create by performing Step 2 of Section 2.3.1.6, "Configuring the Connector for Incremental Reconciliation."</p> <ul style="list-style-type: none"> ■ Value for IBM DB2 UDB: NODATA ■ Value for Microsoft SQL Server: NODATA ■ Value for Oracle Database: ORACLE_RECON_TIME ■ Value for Sybase: NODATA
Resource Object Name	<p>This attribute holds the name of the resource object for the target system.</p> <ul style="list-style-type: none"> ■ Value for IBM DB2 UDB: DB2 DB User ■ Value for Microsoft SQL Server login entity: MSSQL User Login ■ Value for Microsoft SQL Server user entity: MSSQL User ■ Value for Oracle Database: Oracle DB User ■ Value for Sybase login entity: Sybase DB User Login ■ Value for Sybase user entity: Sybase DB User <p>Note: Do not change the default value. However, if you create a copy of the resource object, then you can specify the name of the new resource object as the value of the Resource Object attribute.</p>
Status Reconciliation Primary Key Field	<p>Enter a value for this attribute only if you are writing your own implementation for determining the status of a target system record. While performing the procedure in Section 5.12, "Configuring Status Reconciliation," you provide a value for the Status Reconciliation Class Name entry.</p> <p>If you are writing your own implementation, then enter the name of the primary key resource object attribute. Otherwise, enter NODATA.</p>

Table 3–2 (Cont.) Attributes of Scheduled Tasks for Fetching Data About Users or Logins During Target Resource Reconciliation

Attribute	Description
Task Name	<p>This attribute holds the name of the scheduled task.</p> <p>For target resource reconciliation</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: DBUM DB2 Target Resource User Reconciliation Value for Microsoft SQL Server login entity: DBUM MSSQL Target Resource Login Reconciliation Value for Microsoft SQL Server user entity: DBUM MSSQL Target Resource User Reconciliation Value for Oracle Database: DBUM Oracle Target Resource User Reconciliation Value for Sybase login entity: DBUM Sybase Target Resource Login Reconciliation Value for Sybase user entity: DBUM Sybase Target Resource User Reconciliation <p>For trusted source reconciliation</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: DBUM DB2 Trusted Source User Reconciliation Value for Microsoft SQL Server: DBUM MSSQL Trusted Source User Reconciliation Value for Oracle Database: DBUM Oracle Trusted Source User Reconciliation Value for the Sybase entity: DBUM Sybase Trusted Source User Reconciliation <p>Note: For these scheduled tasks, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that new scheduled task as the value of the Task Name attribute in that scheduled task.</p>
Use Batched Reconciliation	<p>Enter Yes if you want to enable batched reconciliation. Otherwise, enter No.</p> <p>Default value: No</p> <p>Note: If you set the value of this attribute to Yes, then you must specify values for the Batch Reconciliation Query Name and Batch Size attributes.</p>
Use Custom Query	<p>Enter Yes if you want to use the Custom Query attribute to specify the filter parameter. Otherwise, enter No.</p> <p>Default value: No</p>
Use Resource Exclusion List	<p>Enter Yes if you do not want to perform reconciliation on specified target system accounts. Otherwise, enter No.</p> <p>Default value: No</p>
Use Transformation For Reconciliation	<p>Enter Yes if you want to transform attribute values that are fetched from the target system during reconciliation. Otherwise, enter No.</p> <p>Default value: Yes</p>
Use Validation For Reconciliation	<p>Enter Yes if you want to validate attribute values that are fetched from the target system during reconciliation. Otherwise, enter No.</p> <p>Default value: Yes</p>

3.4.5.2 Scheduled Tasks for Reconciling Data About Deleted Users or Logins

Depending on whether you want to run target resource reconciliation or trusted source reconciliation, the following are the scheduled tasks that are used to reconcile data about deleted users or logins:

- Scheduled tasks for target resource reconciliation**

- For IBM DB2 UDB: DBUM DB2 Target Delete Reconciliation
- For the Microsoft SQL Server login entity: DBUM MSSQL Target Delete Login Reconciliation
- For the Microsoft SQL Server user entity: DBUM MSSQL Target Delete User Reconciliation
- For Oracle Database: DBUM Oracle Target Delete Reconciliation
- For the Sybase login entity: DBUM Sybase Target Delete Login Reconciliation
- For the Sybase user entity: DBUM Sybase Target Delete User Reconciliation
- **Scheduled tasks for trusted source reconciliation**
 - For IBM DB2 UDB: DBUM DB2 Trusted Delete Reconciliation
 - For Microsoft SQL Server: DBUM MSSQL Trusted Delete Reconciliation
 - For Oracle Database: DBUM Oracle Trusted Delete Reconciliation
 - For Sybase: DBUM Sybase Trusted Delete Reconciliation

[Table 3–3](#) describes the attributes of these scheduled tasks.

Note:

- Values for most attributes 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 was left empty, then reconciliation would not be performed.
 - The descriptions of some attributes also instruct you not to change the default values. However, if you create a copy of this scheduled task, then you can enter attribute values specific to the target system installation for which you create the copy of scheduled task. See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for more information about creating copies of connector objects.
-

Table 3–3 Attributes of Scheduled Tasks for Fetching Data About Deleted Users or Logins During Target Resource Reconciliation

Attribute	Description
Delete Reconciliation Attribute Mapping Lookup	<p>This attribute holds the name of the lookup definition that holds mappings between the target system and the process form fields.</p> <p>Default value for target resource reconciliation:</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>Lookup.DBUM.DB2.TargetRecon.Delete.Mapping</code> Value for Microsoft SQL Server login entity: <code>Lookup.DBUM.MSSQL.TargetRecon.Delete.Login.Mapping</code> Value for Microsoft SQL Server user entity: <code>Lookup.DBUM.MSSQL.TargetRecon.Delete.User.Mapping</code> Value for Oracle Database: <code>Lookup.DBUM.Oracle.TargetRecon.Delete.Mapping</code> Value for Sybase login entity: <code>Lookup.DBUM.Sybase.TargetRecon.Delete.Login.Mapping</code> Value for Sybase user entity: <code>Lookup.DBUM.Sybase.TargetRecon.Delete.User.Mapping</code> <p>Default value for trusted source reconciliation:</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>Lookup.DBUM.DB2.TrustedRecon.Delete.Mapping</code> Value for Microsoft SQL Server: <code>Lookup.DBUM.MSSQL.TrustedRecon.Delete.Mapping</code> Value for Oracle Database: <code>Lookup.DBUM.Oracle.TrustedRecon.Delete.Mapping</code> Value for Sybase: <code>Lookup.DBUM.Sybase.TrustedRecon.Delete.Mapping</code> <p>Note: You must not change this value.</p>
Is Login Recon	Set the value of this attribute to Yes if you want to reconcile login data. Otherwise, enter No.
IT Resource Name	<p>Enter the name of the IT resource that you configure by performing the procedure described in Section 2.3.5, "Configuring the IT Resource".</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>DB2UDB</code> Value for Microsoft SQL Server: <code>MS SQL Server</code> Value for Oracle Database: <code>Oracle</code> Value for Sybase: <code>Sybase</code>

Table 3–3 (Cont.) Attributes of Scheduled Tasks for Fetching Data About Deleted Users or Logins During Target Resource Reconciliation

Attribute	Description
Query Name	<p>This attribute holds the name of the query for reconciliation of deleted records.</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>DB2_DELETE_USER</code> Value for Microsoft SQL Server: <code>SQL_SERVER_DELETE_USER</code> Value for Oracle Database: <code>ORACLE_DELETE_USER</code> Value for Sybase: <code>SYBASE_LOGIN_DELETE</code>
Resource Object Name	<p>This attribute holds the name of the resource object for the target system.</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>DB2 DB User</code> Value for Microsoft SQL Server login entity: <code>MSSQL User Login</code> Value for Microsoft SQL Server user entity: <code>MSSQL User</code> Value for Oracle Database: <code>Oracle DB User</code> Value for Sybase login entity: <code>Sybase DB User Login</code> Value for Sybase user entity: <code>Sybase DB User</code> <p>Note: Do not change the default value. However, if you create a copy of the resource object, then you can specify the name of the new resource object as the value of the Resource Object attribute.</p>
Task Name	<p>This attribute holds the name of the scheduled task.</p> <p>For target resource reconciliation</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>DBUM DB2 Target Delete Reconciliation</code> Value for Microsoft SQL Server login entity: <code>DBUM MSSQL Target Delete Login Reconciliation</code> Value for Microsoft SQL Server user entity: <code>DBUM MSSQL Target Delete User Reconciliation</code> Value for Oracle Database: <code>DBUM Oracle Target Delete Reconciliation</code> Value for Sybase login entity: <code>DBUM Sybase Target Delete Login Reconciliation</code> Value for Sybase user entity: <code>DBUM Sybase Target Delete User Reconciliation</code> <p>For trusted source reconciliation</p> <ul style="list-style-type: none"> Value for IBM DB2 UDB: <code>DBUM DB2 Trusted Delete Reconciliation</code> Value for Microsoft SQL Server: <code>DBUM MSSQL Trusted Delete Reconciliation</code> Value for Oracle Database: <code>DBUM Oracle Trusted Delete Reconciliation</code> Value for Sybase: <code>DBUM Sybase Trusted Delete Reconciliation</code> <p>Note: For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that new scheduled task as the value of the Task Name attribute in that scheduled task.</p>

3.5 Configuring Scheduled Tasks

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

The following is a list of scheduled tasks that you must configure:

- For lookup field synchronization**
DBUM Lookup reconciliation

- **For target resource user or login data reconciliation**
 - For IBM DB2 UDB: DBUM DB2 Target Resource User Reconciliation
 - For the Microsoft SQL Server login entity: DBUM MSSQL Target Resource Login Reconciliation
 - For the Microsoft SQL Server user entity: DBUM MSSQL Target Resource User Reconciliation
 - For Oracle Database: DBUM Oracle Target Resource User Reconciliation
 - For the Sybase login entity: DBUM Sybase Target Resource Login Reconciliation
 - For the Sybase user entity: DBUM Sybase Target Resource User Reconciliation
- **For target resource reconciliation of deleted users or logins**
 - For IBM DB2 UDB: DBUM DB2 Target Delete Reconciliation
 - For the Microsoft SQL Server login entity: DBUM MSSQL Target Delete Login Reconciliation
 - For the Microsoft SQL Server user entity: DBUM MSSQL Target Delete User Reconciliation
 - For Oracle Database: DBUM Oracle Target Delete Reconciliation
 - For the Sybase login entity: DBUM Sybase Target Delete Login Reconciliation
 - For the Sybase user entity: DBUM Sybase Target Delete User Reconciliation
- **For trusted source reconciliation of deleted users or logins**
 - For IBM DB2 UDB: DBUM DB2 Trusted Delete Reconciliation
 - For Microsoft SQL Server: DBUM MSSQL Trusted Delete Reconciliation
 - For Oracle Database: DBUM Oracle Trusted Delete Reconciliation
 - For the Sybase: DBUM Sybase Trusted Delete Reconciliation

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Manage Scheduled Task**.
4. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.

The following screenshot shows the Scheduled Task Management page:

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

- My Account
- My Resources
- Requests
- To-Do List
- Users
- Organizations
- User Groups
- Access Policies
- Resource Management
 - Manage
 - Create IT Resource
 - Manage IT Resource
 - Create Scheduled Task
 - Manage Scheduled Task
- Deployment Management
- Reports
- Generic Technology Connector
- Help

Scheduled Task Management

Select a scheduled task and the action that you want to perform on it.

Scheduled Task Name

Task State

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

5. In the search results table, click the edit icon in the Edit column for the scheduled task. The following screenshot shows the Scheduled Task Details page:

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

My Account
My Resources
Requests
To-Do List
Users
Organizations
User Groups
Access Policies
Resource Management
 • Manage
 • Create IT Resource
 • Manage IT Resource
 • Create Scheduled Task
 • **Manage Scheduled Task**
Deployment Management
Reports
Generic Technology Connector
Help

Edit Scheduled Task

* Indicates required field

Task Information

Task Name * DBUM Oracle Target Res

Class Name * oracle.iam.connectors.dbu [Clear](#)

Status
☒ Enabled
☐ Disabled

Schedule

Max Retries 10

Next Start December 22, 2009 1:

Frequency
☒ Once
☐ Every Minutes

Last Start n/a

Last Stop n/a

[Cancel](#) [Continue >>](#)

[Back to Search Results](#)

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

6. On the Edit Scheduled Task Details page, you can modify the following details of the scheduled task by clicking **Edit**:
 - **Status:** Specify whether or not you want to leave the task in the enabled state. In the enabled state, the task is ready for use.
 - **Max Retries:** Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 1.
 - **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.
 - **Frequency:** Specify the frequency at which you want the task to run.
7. After modifying the values for the scheduled task details listed in the previous step, click **Continue**.
8. Specify values for the attributes of the scheduled task. To do so, select each attribute from the Attribute list, specify a value in the field provided, and then click **Update**. See [Section 3.4.5, "Reconciliation Scheduled Tasks"](#) for information about attributes of the scheduled task.

Note: Attribute values are predefined in the connector XML file that you import. Specify values only for the attributes that you want to change.

The following screenshot shows the Attributes page. The attributes of the scheduled task that you select for modification are displayed on this page.

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

Attributes

Results 1-10 of 21 First | Previous | Next | Last

Attribute Name	Attribute Value	Delete
Batch Reconciliation Query Name	ORACLE_TARGET_USER_RECON_WITH_BATCH	
Batch Size	0	
Custom Query	NODATA	
Is Login Recon	No	
Is Trusted Recon	No	
IT Resource Name	Oracle	
Last Execution Time	0	
Query Name	ORACLE_TARGET_USER_RECON	
Reconciliation Attribute Mapping Lookup	Lookup.DBUM.Oracle.TargetRecon.Mapping	
Reconciliation Query Filter Lookup	Lookup.DBUM.Oracle.TargetRecon.QueryFilter	

First | Previous | Next | Last

Attribute With

Attribute With

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

9. Click **Save Changes** to commit the changes.

Note: If you want to stop a scheduled task while it is running, then use the Stop Execution feature of the Design Console. See "The Task Scheduler Form" in *Oracle Identity Manager Design Console Guide* for information about this feature.

3.6 Guidelines on Performing Provisioning Operations

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

- [Section 3.6.1, "Guidelines Common to Performing Provisioning Operations on Any Target System"](#)

- [Section 3.6.2, "Guidelines on Performing Provisioning Operations in IBM DB2 UDB"](#)
- [Section 3.6.3, "Guidelines on Performing Provisioning Operations in Microsoft SQL Server"](#)
- [Section 3.6.4, "Guidelines on Performing Provisioning Operations in Oracle Database"](#)
- [Section 3.6.5, "Guidelines on Performing Provisioning Operations in Sybase"](#)

3.6.1 Guidelines Common to Performing Provisioning Operations on Any Target System

The following are guidelines that you must apply while performing provisioning operations on any target system:

- Before you perform provisioning operations, lookup definitions must be synchronized with the lookup fields of the target system. In other words, the scheduled task for lookup field synchronization DBUM Lookup reconciliation must be run before provisioning operations.
- Passwords for user accounts provisioned from Oracle Identity Manager must adhere to the password policy set in the target system.
- The character length of target system fields must be taken into account when specifying values for the corresponding Oracle Identity Manager fields.
- During an updated password provisioning operation, ensure that you clear the existing text in the Password field, and then enter the new password. If you modify the password by appending new characters to the existing value, then the newly added characters are displayed in clear text. This has been mentioned in [Chapter 7, "Known Issues."](#)

3.6.2 Guidelines on Performing Provisioning Operations in IBM DB2 UDB

The following are guidelines that you must apply while performing provisioning operations on IBM DB2 UDB:

- Authentication on IBM DB2 UDB is performed through the operating system. Therefore, the user that you want to provision must exist in the account database of the operating system.

For example, if you want to provision the domain, then the target (IBM DB2 UDB server) must exist on the domain server and the user that you want to provision must exist in the domain.
- IBM DB2 UDB performs authentication externally and authorization internally. Authentication is performed through an accountID and password pair that is passed on to an external certifier. By default, the operating system performs the authentication. However, other programs can be used for this purpose. Authorization is done by mapping the accountID internally to various permissions at the database, index, package, schema, server, table, and/or table space level. When you perform provisioning operations on IBM DB2 UDB, keep in mind the following points:
 - Granting authorization does not automatically authenticate the accountID. You can, for example, authorize nonexistent accounts.
 - Revoking authorization does not remove publicly available authority from an account.

3.6.3 Guidelines on Performing Provisioning Operations in Microsoft SQL Server

The following are guidelines that you must apply while performing provisioning operations on Microsoft SQL Server:

- Before you provision a Microsoft SQL Server account that uses Microsoft Windows authentication, you must ensure that the account you want to provision exists in the account database of the operation system.
- If you are creating users accounts, then you must specify a value for the Database Name parameter of the IT resource. See [Table 2-7](#) for more information about the Database Name parameter.
- If you are provisioning a Microsoft SQL Server login account that uses Microsoft Windows authentication, then you must specify values for the following fields:
 - **Default Database:** Select the name of the default database that the user must connect to.
 - **Default Language:** Select the default language for the login.
 - **Login Name:** Enter the login name in the following format:

DOMAIN_NAME\LOGIN_NAME

In this format:

- * *DOMAIN_NAME* is the name of the domain to which the login account must belong.
- * *LOGIN_NAME* is the name of the login that you are creating in the target system.

The following is a sample value that you can enter in the Login Name field:

MyDomain\jdoe

- If you are provisioning a Microsoft SQL Server login account that uses SQL Server authentication, then you must specify values for the following mandatory fields:
 - **Login Name:** Enter the name of the login account.
 - **Password:** Enter the password for the login account.

3.6.4 Guidelines on Performing Provisioning Operations in Oracle Database

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

- Before you provision an externally-authenticated user account, you must ensure that the account you want to provision must exist in the account database of the operation system.
- For creating password-authenticated database user, you must specify values for the following fields:
 - **IT Resource:** Specify `Oracle` as the value of this lookup field.
 - **Username:** Enter the name of the database user.
 - **Password:** Enter the password for the database user.
 - **Authentication Type:** Specify `PASSWORD` as the value of this lookup field.
- For creating globally-authenticated database users, you must specify a value for the following mandatory fields:

- **IT Resource:** Specify `Oracle` as the value of this lookup field.
- **Username:** Enter the name of the database user.
- **Authentication Type:** Specify `GLOBAL` as the value of this lookup field.
- **Global DN:** Enter the distinguished name (DN) for your organization.

Sample value: `cn=ajones,cn=users,dc=oracle,dc=vm`

After you submit the data required, the adapter runs the following query to create a globally-authenticated database user:

```
CREATE USER :ora_user_id IDENTIFIED GLOBALLY AS :ora_global_dn
```

- For creating externally-authenticated database users, you must specify a value for the following mandatory fields:

- **IT Resource:** Specify `Oracle` as the value of this lookup field.
- **Username:** Enter the name of the database user in the following format:

OS_Authent_PrefixDomain_Name\User_Name

In this format:

- * *OS_Authent_Prefix* is a prefix that Oracle adds to every user's operating system account name.
- * *Domain_Name* is the name of the domain to which the user account being created must belong.
- * *User_Name* is the name of the user account existing in the operating system database.

Sample value: `OPS$my_domain\jdoe`

- **Authentication Type:** Specify `EXTERNAL` as the value of this lookup field.

After you submit the data required, the adapter runs the following query to create an externally-authenticated database user:

```
CREATE USER :ora_user_id_external IDENTIFIED EXTERNALLY
```

- If you specify values for the Default Tablespace Quota (in MB) or Temporary Tablespace Quota (in MB) fields, then enter values in the following format:

TABLESPACE_QUOTA M

In this format, *TABLESPACE_QUOTA* is the tablespace quota allocated to the user and *M* indicates that megabytes is the unit of measurement of quota. The following is a sample value: `300 M`

If you want to allocate to a user unlimited quota on a tablespace, then specify the following as the value of the Default Tablespace Quota (in MB) or Temporary Tablespace Quota (in MB) fields:

`UNLIMITED`

3.6.5 Guidelines on Performing Provisioning Operations in Sybase

If you are using Sybase for creating users accounts, then you must specify a value for the Database Name parameter of the IT resource. See [Table 2-7](#) for more information about the Database Name parameter.

3.7 Performing Provisioning Operations

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

Note: The following procedure is performed using the direct provisioning approach.

1. Log in to the Administrative and User Console.
2. From the Users menu:
 - Select **Create** if you want to first create the OIM User and then provision a database account to the user.
 - Select **Manage** if you want to provision a database account to an existing OIM User.
3. If you select Create, on the Create User page, enter values for the OIM User fields, and then click **Create User**.

Create User
You may create a new user from this page.

* Indicates Required Field

User ID * RICHARD

First Name * RICHARD

Middle Name

Last Name * ROE

Status

Organization * Xellerate Users [Clear](#)

User Type * End-User

Employee Type * Full-Time Employee

Manager ID [Clear](#)

Email

User Disabled ☐

Password *

Confirm Password *

User Locked ☐

Start Date

End Date

Provisioning Date

Provisioned Date

Deprovisioning Date

Deprovisioned Date

Change Password at next logon ☒

[Create User](#) [Cancel](#)

4. If you select Manage, then search for the OIM User and select the link for the user from list of users displayed in the search results.

My Account

My Resources

Requests

To-Do List

Users

- Create
- Manage

Organizations

User Groups

Access Policies

Resource Management

Deployment Management

Reports

Generic Technology Connector

Help

Manage User

Type in search criteria to search for users.

Employee Type

Status

Results 1-1 of 1

First | Previous | Next | Last

User ID	First Name	Last Name	Status	Enable	Disable	Unlock	Delete
RICHARD	RICHARD	ROE	Active	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Unlock"/>	<input type="button" value="Delete"/>

First | Previous | Next | Last

- On the User Detail page, select **Resource Profile** from the list at the top of the page.

My Account

My Resources

Requests

To-Do List

Users

- Create
- Manage

Organizations

User Groups

Access Policies

Resource Management

Deployment Management

Reports

Generic Technology Connector

Help

User Detail

This is information about the user.

You can view additional details about this user:

User ID

RICHARD

First Name

RICHARD

Middle Name

Last Name

ROE

Status

Active

Organization

Xellerate Users

User Type

End-User

Employee Type

Full-Time Employee

Manager ID

Email

Start Date

End Date

Provisioning Date

Provisioned Date

December 21, 2009

Deprovisioning Date

Deprovisioned Date

Change Password at next logon

☒

- On the Resource Profile page, click **Provision New Resource**.

- My Account
- My Resources
- Requests
- To-Do List
- Users
 - Create
 - Manage
- Organizations
- User Groups
- Access Policies
- Resource Management
- Deployment Management

Resources Not Found
There are no resources for this user

[User Detail](#) >> [Resource Profile](#)

User Name : [RICHARD](#)
First Name : RICHARD
Last Name : ROE

[Provision New Resource](#)

7. On the Step 1: Select a Resource page, depending on the target system that you are using, select the appropriate resource from the list, and then click **Continue**.

- My Account
- My Resources
- Requests
- To-Do List
- Users
 - Create
 - Manage
- Organizations
- User Groups
- Access Policies
- Resource Management
- Deployment Management
- Reports
- Generic Technology Connector
- Help

Provision Resource to User
You are provisioning to RICHARD ROE [RICHARD].

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#)

Step 1: Select a Resource

Select a resource to provision.

Filter By

Results 1-6 of 6 [First](#) | [Previous](#) | [Next](#)

	Resource Name	Resource Type	Resource Form
<input type="radio"/>	DB2 DB User	Application	No
<input checked="" type="radio"/>	Oracle DB User	Application	No
<input type="radio"/>	MSSQL DB User Login	Application	No
<input type="radio"/>	MSSQL DB User	Application	No
<input type="radio"/>	Sybase DB User Login	Application	No
<input type="radio"/>	Sybase DB User	Application	No

[First](#) | [Previous](#) | [Next](#)

8. On the Verify Resource Selection page, click **Continue**.

Provision Resource to User
You are provisioning to RICHARD ROE [RICHARD].

Step 2: Verify Resource Selection

You have selected to provision Oracle DB User to RICHARD ROE [RICHARD]

9. On the Provide Process Data page, enter the details of the account that you want to create on the target system and then click **Continue**.

Provision Resource to User
You are provisioning to RICHARD ROE [RICHARD].

Step 5: Provide Process Data

DBUM Provisioning form for Oracle User

* Indicates required field

IT Resource	* Oracle	<input type="button" value="Clear"/>
Username	* RICHARD	<input type="button" value="Clear"/>
Password	*****	
Authentication Type	* PASSWORD	<input type="button" value="Clear"/>
Global DN		
Default Tablespace		<input type="button" value="Clear"/>
Default Tablespace Quota (in MB)		
Temporary Tablespace		<input type="button" value="Clear"/>
Temporary tablespace Quota (in MB)		
Profile Name		<input type="button" value="Clear"/>
Account Status		

10. On the Step 2: Verify Process Data page, verify the data that you entered and then click **Continue**.

Provision Resource to User
You are provisioning to RICHARD ROE [RICHARD].

1 2 3 4 5 6

Step 6: Verify Process Data

You have selected to provision Oracle DB User to RICHARD ROE [RICHARD].

DBUM Provisioning form for Oracle User

IT Resource	Oracle
Username	RICHARD
Password	*****
Authentication Type	PASSWORD
Global DN	
Default Tablespace	
Default Tablespace Quota (in MB)	
Temporary Tablespace	
Temporary tablespace Quota (in MB)	
Profile Name	
Account Status	

11. On Step 5: Provide Process Data page, for process data, enter the details of the account that you want to create on the target system and then click **Continue**.
12. If you want to provide child data, then on the Step 5: Provide Process Data page for child data, search for and select the child data for the user on the target system and then click **Continue**. Repeat the same step if you have more than one child data and you want to provision them.

Provision Resource to User
You are provisioning to RICHARD ROE [RICHARD].

1 2 3 4 5 6

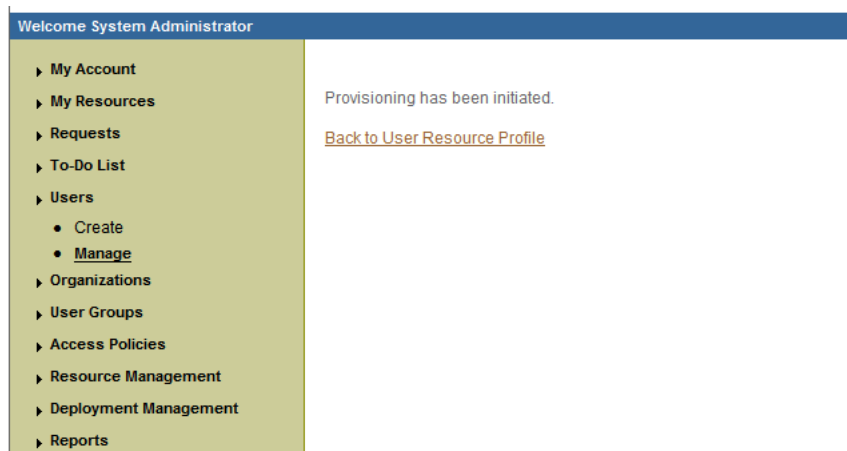
Step 5: Provide Process Data

DBUM Grant/Revoke Roles

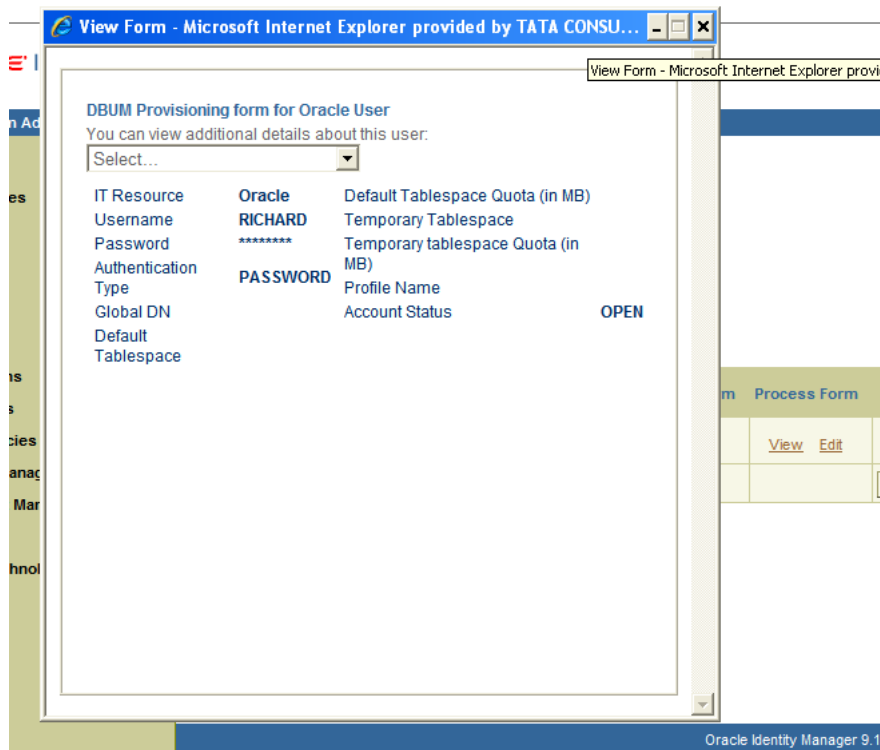
Roles

Role Admin Option

13. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
14. The "Provisioning has been initiated" message is displayed. Click **Back to User Resource Profile**. The Resource Profile page shows that the resource has been provisioned to the user.



15. If you click the View link in the Process Form column, then the process form is displayed.



16. If you click the resource, then the Resource Provisioning Details page is displayed.




- My Account
- My Resources
- Requests
- To-Do List
- Users
 - Create
 - Manage
- Organizations
- User Groups
- Access Policies
- Resource Management
- Deployment Management
- Reports
- Generic Technology Connector
- Help

[User Detail](#) >> [Resource Profile](#) >> [Resource Provisioning Details](#)

The following are the provisioning tasks for the resource. You can also enable, disable, or revoke this resource from the us

Oracle DB User provisioning details for RICHARD ROE[RICHARD]

Results 1-3 of 3 [First](#) | [Previous](#) |

Task Name	Task Status	Date Assigned	Assigned To
System Validation	Completed	December 21, 2009	 System Administrator [XELSYSADM]
Create User	Completed	December 21, 2009	 System Administrator [XELSYSADM]
Add Role or Grant	Completed	December 21, 2009	 System Administrator [XELSYSADM]

[First](#) | [Previous](#) |

[Enable](#) [Disable](#) [Revoke](#) [Add Task](#)

See Also: [Section 1.7, "Connector Objects Used During Provisioning"](#) for more information about the provisioning functions supported by this connector and the process form fields used for provisioning

Extending the Functionality of the Connector

The following section describes procedures that you can perform to extend the functionality of the connector for addressing your specific business requirements:

- [Section 4.1, "Guidelines on Extending the Functionality of the Connector"](#)
- [Section 4.2, "Adding or Removing Attributes for Reconciliation"](#)
- [Section 4.3, "Adding or Removing Attribute Mappings for Provisioning"](#)
- [Section 4.4, "Modifying Field Lengths on the Process Form"](#)
- [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#)
- [Section 4.6, "Configuring the Connector for Multiple Trusted Source Reconciliation"](#)
- [Section 4.7, "Configuring Reconciliation Queries"](#)
- [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#)
- [Section 4.9, "Configuring Transformation of Data During Reconciliation"](#)
- [Section 4.10, "Configuring the Connector for Reconciling and Provisioning Object-Level Privileges"](#)
- [Section 4.11, "Configuring the Connector for Reconciling and Provisioning Authorization to Oracle Database Vault Realms"](#)

4.1 Guidelines on Extending the Functionality of the Connector

As mentioned earlier in this guide, predefined queries are provided to reconcile target system user records and synchronize lookup field values with Oracle Identity Manager. These predefined queries are in the `DBUMReconQuery.properties` and `DBUMLookUpQuery.properties` files, respectively.

You can modify the predefined queries. In addition, you can add your own queries in the same file or in a different properties file. The query whose name you specify in the scheduled task is applied during reconciliation or lookup field synchronization.

The following sections discuss guidelines that you must apply while modifying the predefined queries or creating new queries:

- [Section 4.1.1, "Guidelines for Configuring Queries Used in Lookup Field Synchronization"](#)
- [Section 4.1.2, "Guidelines for Configuring Queries Used in Reconciliation"](#)

- [Section 4.1.3, "Guidelines Common to Configuring Both Types of Queries"](#)

The following section discusses guidelines that you must apply while modifying the predefined attribute mappings for provisioning:

- [Section 4.1.4, "Guidelines on Modifying Predefined Attribute Mappings for Provisioning"](#)

4.1.1 Guidelines for Configuring Queries Used in Lookup Field Synchronization

The following are guidelines that you must apply while modifying or creating queries for lookup field synchronization:

- You must not change the SELECT clause of the predefined query. In other words, the set of target system attributes from which values are fetched for synchronization cannot be modified.
- If you create a query, then you must mention the name of the query, which is the lookup definition name, as the value of the Lookup Definition Name attribute in the scheduled task.
- If you want to use a new properties file instead of the predefined DBUMLookUpQuery.properties file, then specify the full path and name of that file as the value of the Query Properties File Path attribute in the reconciliation scheduled task. See [Section 3.3, "Scheduled Task for Lookup Field Synchronization"](#) for information about this scheduled task.

4.1.2 Guidelines for Configuring Queries Used in Reconciliation

The following are examples of scenarios in which you might want to modify a reconciliation query:

- You want to add a column in the SELECT clause of the reconciliation query.
- You want to remove a column from the SELECT clause of the reconciliation query. For example, if you are using Oracle Database as the target system, then you might want to remove the PROFILE column.
- You want to add conditions to the WHERE clause of the reconciliation query so that only a specified subset of the target system records are considered for reconciliation.

The following are guidelines that you must apply while modifying or creating queries for reconciliation:

- By adding or removing a column from the SELECT clause of a reconciliation query, you add or remove an attribute from the list of target system attributes for reconciliation. To enable the connector to process a change (addition or removal) in the list of reconciled attributes, you must make corresponding changes in the provisioning part of the connector. The procedures are described later in this guide.
- In the query properties file, you must not change the names of the following predefined queries because these names have been included in the connector code:

SYBASE_DATABASE

SYBASE_LOGIN_DETAILS

SYBASE_USER_DETAILS

SQL_SERVER_DATABASE

SQL_SERVER_LOGIN_DETAILS

SQL_SERVER_USER_DETAILS

SQL_SERVER_STATUS_AUTH_TYPE:

- Some of the predefined queries use inner queries. If you add or remove a column from the outer query, you must make corresponding changes in the inner queries.
- You cannot remove columns corresponding to the following resource object attributes that are marked as mandatory attributes:
 - For IBM DB2 UDB: User Name
 - For Microsoft SQL Server login entity: Login Name
 - For Microsoft SQL Server user entity: Login Name, User Name
 - For Oracle Database: User Name
 - For Sybase login entity: Login Name
 - For Sybase user entity: Login Name, User Name
- If you are using Oracle Database as the target system, then you must ensure that the following condition included in the WHERE clause of the inner query is not removed:

```
WHERE ((CREATED - TO_DATE('01011970','ddmmyyyy')) *24*60*60*1000) >
:lastExecutionTime
```

This condition is used to determine if a target system record was added or updated after the time stamp stored in the Last Execution Time scheduled task attribute.

- For Oracle Database, in the WHERE clause, you must ensure that formats for date literals are specified by the use of the TO_DATE function. For example, instead of specifying a date value as '31-Dec-4712' use
TO_DATE('31-Dec-4712','DD-Mon-YYYY').
- When you add or remove columns from the SELECT clause of the child queries in the properties file, then you must update the attribute mapping lookup definition that holds mappings between child attributes and the target system column names. In addition, you must update other OIM objects. The procedure is described later in this guide.
- Before you modify or add a query in the properties file, you must run the query by using any standard database client to ensure that the query produces the required results when it is run against the target system database.
- If you want to use a new properties file instead of the predefined DBUMReconQuery.properties file, then specify the name of the file as the value of the Query Properties File attribute in the Configuration lookup definition for your target system database. See [Appendix A, "Preconfigured Lookup Definitions"](#) for information about Configuration lookup definition.

4.1.3 Guidelines Common to Configuring Both Types of Queries

The following are guidelines that you must apply while modifying or creating queries for either reconciliation or lookup field synchronization:

- The name of the query must not be the same as the name of any other query in the properties file.

- The name of the query must not contain spaces.
- Before you modify or add a query in the properties file, you must run the query by using any standard database client to ensure that it produces the required results.
- Use the number sign (#) to begin each comment line in the properties file.
Add comments to describe changes that you make in existing queries and also to describe new queries that you add in the file.
See existing comments in the properties file for an example.
- If you want to introduce line breaks in the query (to improve readability), then add a backslash (\) at the end of each line.
- You must not change existing conditions in the WHERE clause of the predefined query.
- You can add conditions to the WHERE clause of the predefined query.

4.1.4 Guidelines on Modifying Predefined Attribute Mappings for Provisioning

You must not remove attributes that are marked as mandatory in [Section 1.7.2, "Attributes for Provisioning."](#)

4.2 Adding or Removing Attributes for Reconciliation

This section is divided into the following topics:

- [Section 4.2.1, "Adding New Standard and Custom Attributes for Reconciliation"](#)
- [Section 4.2.2, "Adding New Standard and Custom Multivalued Attributes for Target Resource Reconciliation"](#)
- [Section 4.2.3, "Removing Attributes Used for Reconciliation"](#)

4.2.1 Adding New Standard and Custom Attributes for Reconciliation

Note: The procedure described in this section applies to both standard target system attributes and custom attributes that you create on the target system.

If you want to add a multivalued field for reconciliation, then see [Section 4.2.2, "Adding New Standard and Custom Multivalued Attributes for Target Resource Reconciliation."](#)

By default, the attributes listed in [Section 1.6.2, "Target System Columns Used in Reconciliation"](#) are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for target resource reconciliation or trusted source reconciliation.

To add a new standard or custom attribute for reconciliation:

See Also: *Oracle Identity Manager Design Console Guide* for detailed information about these steps

1. Open the reconciliation properties file in a text editor. In the section corresponding to the target system database that you are using, add to the query, the target system column name that you want to include for reconciliation.

See Also:

[Section 1.6.1, "Reconciliation Queries"](#)

[Section 4.1.2, "Guidelines for Configuring Queries Used in Reconciliation"](#)

[Section 4.1.3, "Guidelines Common to Configuring Both Types of Queries"](#)

2. Save the changes to the file.
3. Log in to the Design Console.
4. In the resource object definition, add the reconciliation field corresponding to the attribute as follows:
 - a. Expand the **Resource Management** folder, and then double-click **Resource Objects**.
 - b. If you have configured the target system as a trusted source, then search for and open the **DBUM Trusted Source** resource object.
 - c. If you have configured the target system as a target resource, then search for and open one of the following resource objects:
 - For IBM DB2 UDB: DB2 DB User
 - For Microsoft SQL Server login entity: MSSQL User Login
 - For Microsoft SQL Server user entity: MSSQL User
 - For Oracle Database: Oracle DB User
 - For Sybase login entity: Sybase DB User Login
 - For Sybase user entity: Sybase DB User
 - d. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box.
 - e. Specify a value for the field name.
 - f. From the **Field Type** list, select a data type for the field. In addition, if you want to designate the attribute as a mandatory attribute, then select the check box.
 - g. Click the Save icon, and then close the dialog box.
5. Add an entry for the attribute in the lookup definition for reconciliation attribute mapping as follows:
 - a. Expand the **Administration** folder, and then double-click **Lookup Definition**.
 - b. If you have configured the target system as a trusted source, then search for and open one of the following lookup definitions:
 - For IBM DB2 UDB: Lookup.DBUM.DB2.TrustedRecon.Mapping
 - For Microsoft SQL Server: Lookup.DBUM.MSSQL.TrustedRecon.Mapping
 - For Oracle Database: Lookup.DBUM.Oracle.TrustedRecon.Mapping
 - For Sybase: Lookup.DBUM.Sybase.TrustedRecon.Mapping
 - c. If you have configured the target system as a target source, then search for and open one of the following lookup definitions:

- For IBM DB2 UDB: Lookup.DBUM.DB2.TargetRecon.Mapping
 - For Microsoft SQL Server login entity: Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping
 - For Microsoft SQL Server user entity: Lookup.DBUM.MSSQL.TargetRecon.User.Mapping
 - For Oracle Database: Lookup.DBUM.Oracle.TargetRecon.Mapping
 - For Sybase login entity: Lookup.DBUM.Sybase.TargetRecon.Login.Mapping
 - For Sybase user entity: Lookup.DBUM.Sybase.TargetRecon.User.Mapping
- d. To add a row, click **Add**.
- e. In the **Code Key** column, enter the name that you have set for the attribute in the resource object.
- f. In the **Decode** column, enter one of the following values:
- If your target system contains a column corresponding to the resource object attribute that you added, then enter the target system column name in the reconciliation query of the properties file as the Decode value. If you have set an alias for the column in the query, then enter the alias in the Decode column.
 - If you want to set a constant value, then enter the value in the `CONSTANT~CONSTANT_VALUE` format.

In this format, `CONSTANT` specifies that the data in this column is a constant or literal. `CONSTANT_VALUE` is value to be displayed in the corresponding field of the OIM User form.
 - If you want to specify values fetched from the target system in a format that is accepted by Oracle Identity Manager, then enter the value in the `COLUMN_NAME~LOOKUP_NAME` format.

In this format, `COLUMN_NAME` is the target system column name from which the value is fetched. `LOOKUP_NAME` is the name of the lookup definition that maps values fetched from the target system with values that must be displayed in the OIM User form field.
 - If the process form field corresponding to the Code Key value is a lookup type field, then enter the value in the `LOOKUP~COL_NAME` format.

In this format, `LOOKUP` specifies that the data retrieved from the target system is lookup data. `COL_NAME` is the corresponding column name or column name alias used in the reconciliation query
- g. Click the Save icon.
6. Add the attribute as a field on the process form as follows:
- a. Expand the **Development Tools** folder, and then double-click **Form Designer**.
 - b. Search for and open the process form for the connector that you are using:

See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process forms for each connector.
 - c. Click **Create New Version** to create a version of the process form. Then, enter a version name and click the Save icon.
 - d. Click **Add**.

- e. Specify the properties of the attribute according to your requirement.
- f. Click the Save icon.
- g. Click **Make Version Active** to activate the new version of the process form.
7. Create a reconciliation field mapping in the process definition as follows:
 - a. Expand the **Process Management** folder, and then double-click **Process Definition**.
 - b. If you have configured the target system as a trusted source, then search for and open the **DBUM Trusted User** process definition.
 - c. If you have configured the target system as a target resource, then search for and open one of the following process definitions:
 - For IBM DB2 UDB: DB2 DB User
 - For Microsoft SQL Server login entity: MSSQL DB User Login
 - For Microsoft SQL Server user entity: MSSQL DB User
 - For Oracle Database: Oracle DB User
 - For Sybase login entity: Sybase DB User Login
 - For Sybase user entity: Sybase DB User
 - d. On the Reconciliation Field Mapping tab, click **Add Field Map**.
 - e. From the Field name list in the Add Reconciliation Field Mapping dialog box, select the name that you have assigned to the attribute created in the resource object.
 - f. Double-click the Process Data Field. The entries in the dialog box that is displayed correspond to the process form fields.
 - g. Select the corresponding newly added field from the dialog box.
 - h. If the field mapping is a key field for matching the process data, check the key Field for Reconciliation matching check box.
 - i. Click the Save icon.
8. Add the attribute for provisioning. [Section 4.3, "Adding or Removing Attribute Mappings for Provisioning"](#) for detailed information about the procedure.

4.2.2 Adding New Standard and Custom Multivalued Attributes for Target Resource Reconciliation

By default, the attributes listed in [Section 1.6.2, "Target System Columns Used in Reconciliation"](#) are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new multivalued attributes for target resource reconciliation.

To add a new standard or custom multivalued attribute for reconciliation:

See Also: *Oracle Identity Manager Design Console Guide* for detailed information about these steps

1. Open the reconciliation properties file in a text editor. In the section corresponding to the target system database that you are using, add to the query, the target system column name that you want to include for reconciliation.

See Also:

[Section 1.6.1, "Reconciliation Queries"](#)

[Section 4.1.2, "Guidelines for Configuring Queries Used in Reconciliation"](#)

[Section 4.1.3, "Guidelines Common to Configuring Both Types of Queries"](#)

2. Save the changes to the file.
3. Log in to the Design Console.
4. In the resource object definition, add the reconciliation field corresponding to the attribute as follows:
 - a. Expand the **Resource Management** folder, and then double-click **Resource Objects**.
 - b. Search for and open one of the following resource objects:
 - For IBM DB2 UDB: DB2 DB User
 - For Microsoft SQL Server login entity: MSSQL User Login
 - For Microsoft SQL Server user entity: MSSQL User
 - For Oracle Database: Oracle DB User
 - For Sybase login entity: Sybase DB User Login
 - For Sybase user entity: Sybase DB User
 - c. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box.
 - d. Specify a value for the field name.
 - e. From the **Field Type** list, select **Multi-Valued**. In addition, if you want to designate the attribute as a mandatory attribute, then select the check box.
 - f. Click the Save icon, and then close the dialog box.
 - g. Right-click the field that you added as a multivalued attribute in Step 4.c, and then select **Define Property Fields** to open the Add Reconciliation Field dialog box.
 - h. In the **Field Name** field, enter the name of the field that you want to add to the multivalued attribute.
 - i. From the **Field Type** list, select **String**.
 - j. Click the Save icon and close the dialog box.
 - k. Repeat Steps 4.g through 4.j for every field that you want to add to the multivalued attribute.
5. Create a lookup definition with the entries listed in [Table 4–1](#). This lookup definition contains configurable entries for a multivalued attribute.

Table 4–1 Entries in the Configuration Lookup Definition for a Multivalued Attribute

Code Key	Decode
Child Attribute Mapping Lookup	<p>Enter the name of the lookup definition that maps the fields of the multivalued attribute with the column name used in the reconciliation query.</p> <p>Sample value: Lookup.DBUM.DB2.TargetRecon.Schema.Configuration</p> <p>See Appendix A, "Preconfigured Lookup Definitions" for more information about this lookup definition.</p>
Child Query Name	<p>Enter the name of the query in the reconciliation query file that you want to run for reconciling data about the child attribute.</p> <p>Sample value: DB2_TARGET_USER_SCHEMA</p>
Child Reconciliation Query Filter Lookup	<p>Enter the name of the lookup definition that contains information about reconciliation filter parameters for the child attribute.</p> <p>Sample value: Lookup.DBUM.DB2.TargetRecon.Schema.QueryFilter</p> <p>See Appendix A, "Preconfigured Lookup Definitions" for more information about this lookup definition.</p>
Parent Attribute	<p>This entry holds the primary key column of the query used for running target resource user reconciliation.</p>

6. Add an entry for the attribute in the lookup definition for reconciliation attribute mapping as follows:
 - a. Expand the **Administration** folder, and then double-click **Lookup Definition**.
 - b. Search for and open one of the following lookup definitions:
 - For IBM DB2 UDB: Lookup.DBUM.DB2.TargetRecon.Mapping
 - For Microsoft SQL Server login entity: Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping
 - For Microsoft SQL Server user entity: Lookup.DBUM.MSSQL.TargetRecon.User.Mapping
 - For Oracle Database: Lookup.DBUM.Oracle.TargetRecon.Mapping
 - For Sybase login entity: Lookup.DBUM.Sybase.TargetRecon.Login.Mapping
 - For Sybase user entity: Lookup.DBUM.Sybase.TargetRecon.User.Mapping
 - c. To add a row, click **Add**.
 - d. In the **Code Key** column, enter the name that you have set for the attribute in the resource object.
 - e. In the **Decode** column, enter a value in the following format:


```
Child~CONFIG_LOOKUP_NAME
```

In this format:

 - Child specifies that the data in this column is the child attribute data

- *CONFIG_LOOKUP_NAME* is name of the lookup definition that holds configurable entries for the multivalued attribute. This is the lookup definition that you created in Step 5.
- f. Click the Save icon.
- 7. Create a child form. See [Section 5.4, "Creating a Process Form"](#) for information about creating a child form.
- 8. Add the child attribute as a field on the child form.
See [Section 4.3, "Adding or Removing Attribute Mappings for Provisioning"](#) for information about adding child attributes to the child form.
- 9. Assign to the parent form the child table, which is represented by the child form as follows:
 - a. Expand **Development Tools**, and then double-click **Form Designer**.
 - b. Search for and open the parent process form for the target system that you are using:
See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.
 - c. Click **Create New Version** to create a version of the form. Then, enter a version name and click the Save icon.
 - d. On the Child Tables(s) tab, click **Assign**.
The Assignment window is displayed.
 - e. From this window, select the child table, and assign it to the form.
 - f. Click **OK**.
The selected child table is assigned to the form.
- 10. Create a reconciliation field mapping in the process definition as follows:
 - a. Expand the **Process Management** folder, and then double-click **Process Definition**.
 - b. Search for and open one of the following process definitions:
 - For IBM DB2 UDB: DB2 DB User
 - For Microsoft SQL Server login entity: MSSQL DB User Login
 - For Microsoft SQL Server user entity: MSSQL DB User
 - For Oracle Database: Oracle DB User
 - For Sybase login entity: Sybase DB User Login
 - For Sybase user entity: Sybase DB User
 - c. On the Reconciliation Field Mapping tab, click **Add Field Map**.
 - d. From the Field Name list in the Add Reconciliation Field Mapping dialog box, select the name that you have assigned to the multivalued attribute created in the resource object.
 - e. Double-click the Process Data Field, a new pop-up will appear. The entries in the pop-up correspond to the process form fields.
 - f. Select the corresponding newly added field from the pop-up.

- g. If the field mapping is a key field for matching the process data, check the Key Field for Reconciliation matching check box.
 - h. Click the Save icon.
11. Add the attribute for provisioning. [Section 4.3, "Adding or Removing Attribute Mappings for Provisioning"](#) for detailed information about the procedure.

4.2.3 Removing Attributes Used for Reconciliation

By default, the attributes listed in [Section 1.6.2, "Target System Columns Used in Reconciliation"](#) are mapped for reconciliation between Oracle Identity Manager and the target system. From that list of attributes, you must ensure that mappings for the following attributes and the corresponding columns in the SQL query are not modified or removed:

- For IBM DB2 UDB: User Name
- For Microsoft SQL Server login entity: Login Name
- For Microsoft SQL Server user entity: Login Name, User Name
- For Oracle Database: User Name
- For Sybase login entity: Login Name
- For Sybase user entity: Login Name, User Name

To remove an attribute from the list of attributes for reconciliation:

See Also: *Oracle Identity Manager Design Console Guide* for detailed information about these steps

1. Open the properties file in a text editor, and remove the column from the query corresponding to the target system that you are using. Then, save and close the file.

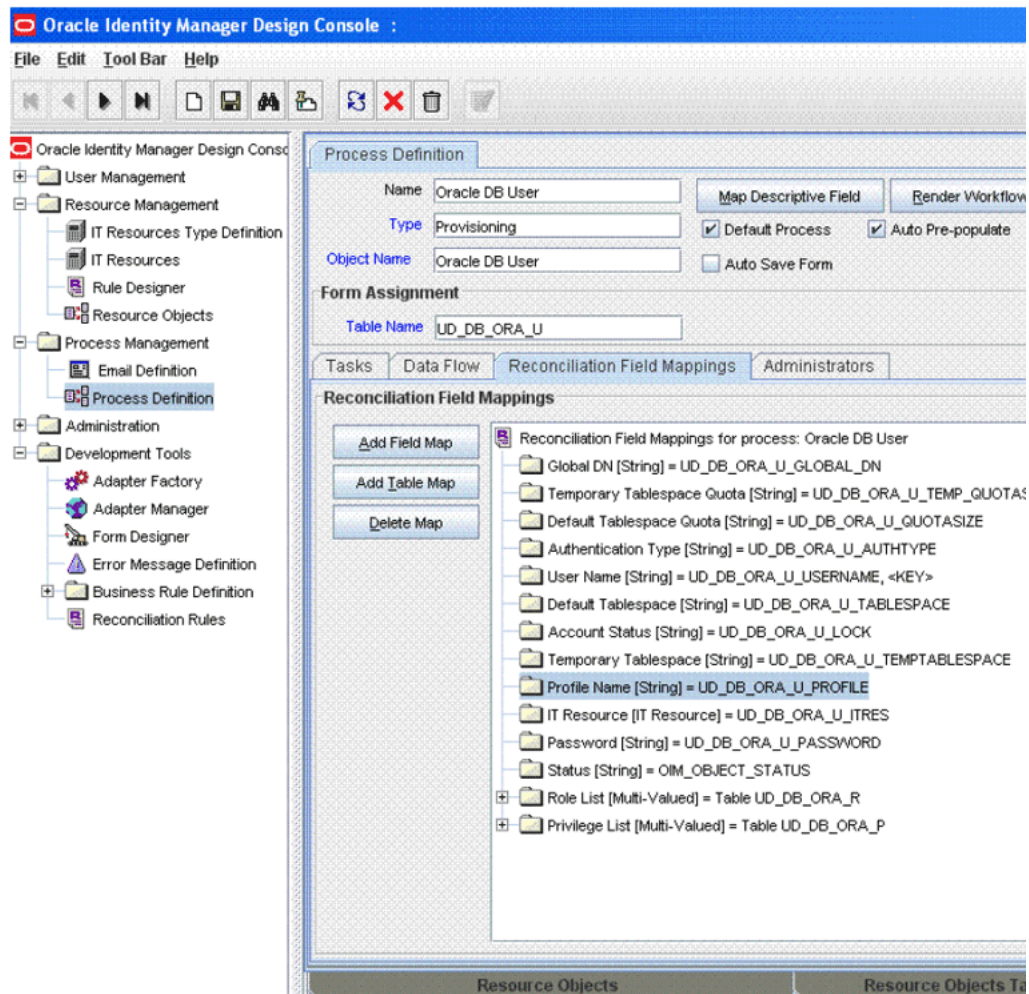
See Also:

Section 1.5.1, "Reconciliation Queries"

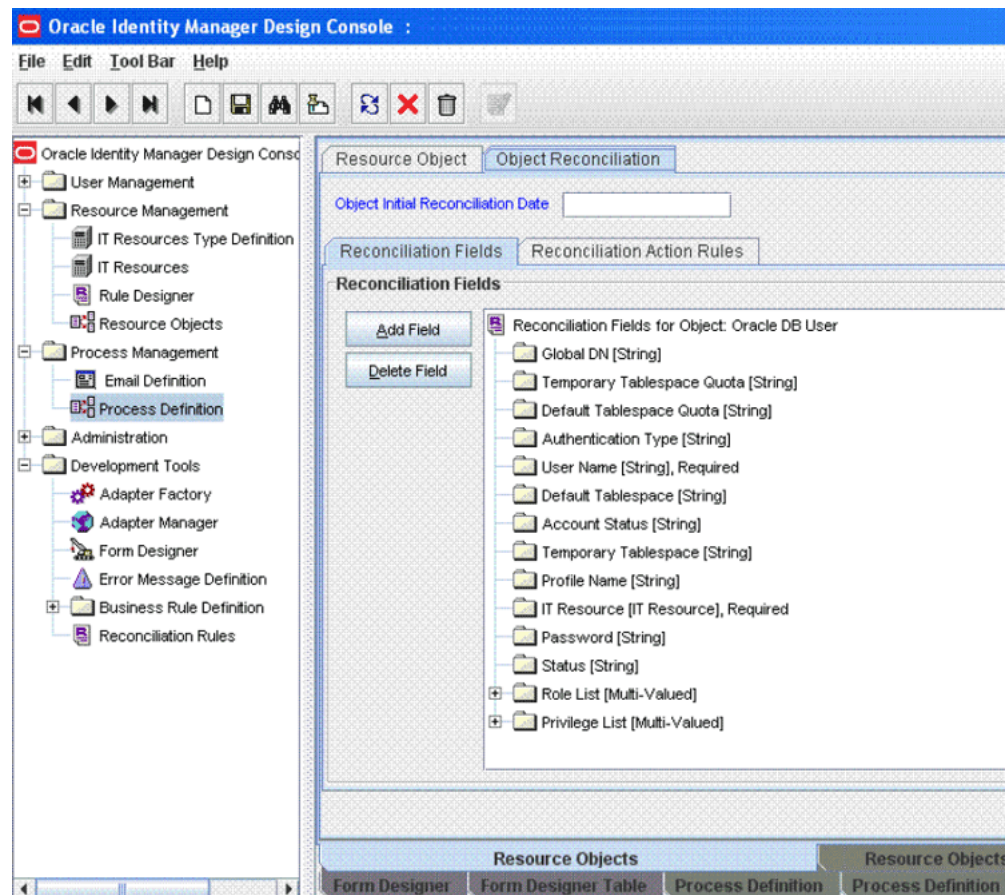
Section 5.1.2, "Guidelines for Configuring Queries Used in Reconciliation"

Section 5.1.3, "Guidelines Common to Configuring Both Types of Queries"

2. Log in to the Design Console.
3. Remove the reconciliation field mapping in the process definition as follows:
 - a. Expand the **Process Management** folder, and then double-click **Process Definition**.
 - b. Search for and open the process definition for the connector that you are using:
 See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.
 - c. On the Reconciliation Field Mapping tab, select the mapping that you want to remove and then click **Delete Map**. The following screenshot shows this page:



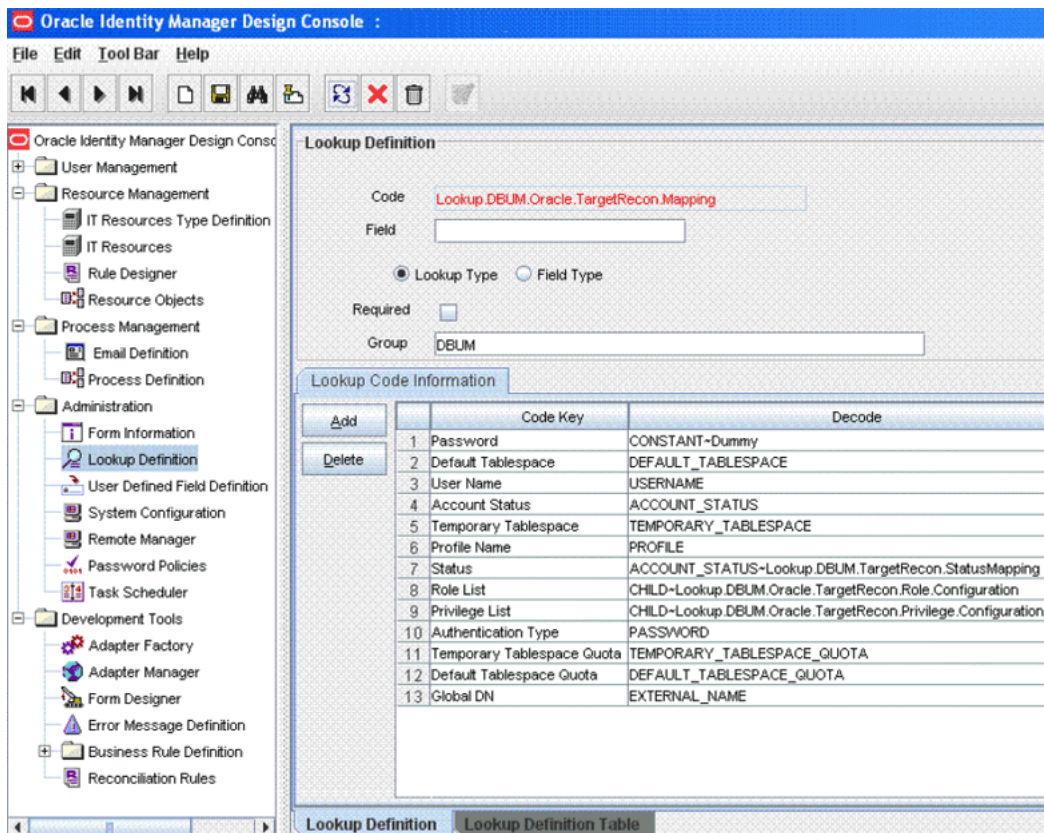
- d. Click the Save icon.
4. In the resource object definition, remove the reconciliation field corresponding to the attribute as follows:
 - a. Expand the **Resource Management** folder, and then double-click **Resource Objects**.
 - b. If you have configured the target system as a trusted source, then search for and open the **DBUM Trusted Source** resource object.
 - c. If you have configured the target system as a target resource, then search for and open one of the following resource objects:
 - For IBM DB2 UDB: DB2 DB User
 - For Microsoft SQL Server login entity: MSSQL User Login
 - For Microsoft SQL Server user entity: MSSQL User
 - For Oracle Database: Oracle DB User
 - For Sybase login entity: Sybase DB User Login
 - For Sybase user entity: Sybase DB User
 - d. On the Object Reconciliation tab, select the attribute that you want to remove and then click **Delete Field**. The following screenshot shows this page:



- e. Click the Save icon, and then close the dialog box.
5. Remove the entry for the attribute in the lookup definition for reconciliation attribute mapping as follows:
 - a. Expand the **Administration** folder, and then double-click **Lookup Definition**.
 - b. If you have configured the target system as a trusted source, then search for and open one of the following lookup definitions:
 - For IBM DB2 UDB: Lookup.DBUM.DB2.TrustedRecon.Mapping
 - For Microsoft SQL Server: Lookup.DBUM.DB2.TrustedRecon.Mapping
 - For Oracle Database: Lookup.DBUM.Oracle.TrustedRecon.Mapping
 - For Sybase: Lookup.DBUM.Sybase.TrustedRecon.Mapping
 - c. If you have configured the target system as a target resource, then search for and open one of the following lookup definitions:
 - For IBM DB2 UDB: Lookup.DBUM.DB2.TargetRecon.Mapping
 - For Microsoft SQL Server login entity: Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping
 - For Microsoft SQL Server user entity: Lookup.DBUM.MSSQL.TargetRecon.User.Mapping

- For Oracle Database: Lookup.DBUM.Oracle.TargetRecon.Mapping
- For Sybase login entity:
Lookup.DBUM.Sybase.TargetRecon.Login.Mapping
- For Sybase user entity: Lookup.DBUM.Sybase.TargetRecon.User.Mapping

The following screenshot shows this page for Oracle Database:



- d. Select the row for the attribute that you want to remove, and then click **Delete**.
- e. Click the Save icon.
6. Remove the attribute from the process form as follows:
 - a. Expand the **Development Tools** folder, and then double-click **Form Designer**.
 - b. Search for and open the process form for the connector that you are using:
See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.
 - c. Click **Create New Version** to create a version of the process form. Then, enter a version name and click the Save icon.
 - d. Select the field that you want to remove, and then click **Delete**.

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order
1	UD_DB_ORA_U_TEMP_QUOTASIZE	String	10	Temporary Tablespace	TextField		9
2	UD_DB_ORA_U_USERNAME	String	50	Username	TextField		2
3	UD_DB_ORA_U_GLOBAL_DN	String	50	Global DN	TextField		5
4	UD_DB_ORA_U_ITRES	long		IT Resource	ITResourceLookupField		1
5	UD_DB_ORA_U_TEMPTABLESPACE	String	50	Temporary Tablespace	LookupField		8
6	UD_DB_ORA_U_PASSWORD	String	50	Password	PasswordField		3
7	UD_DB_ORA_U_TABLESPACE	String	50	Default Tablespace	LookupField		6
8	UD_DB_ORA_U_PROFILE	String	50	Profile Name	LookupField		10
9	UD_DB_ORA_U_LOCK	String	100	Account Status	DOField		11
10	UD_DB_ORA_U_AUTHTYPE	String	50	Authentication Type	LookupField	PASSWORD	4
11	UD_DB_ORA_U_QUOTASIZE	String	10	Default Tablespace	TextField		7
12							

- e. Click the Save icon.
- f. Click **Make Version Active** to activate the new version of the process form.
7. Remove the attribute from the list used for provisioning. [Section 4.3.3, "Removing Attributes for Provisioning"](#) for detailed information about the procedure.

4.3 Adding or Removing Attribute Mappings for Provisioning

By default, the attributes listed in [Section 1.7.2, "Attributes for Provisioning"](#) are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can add new attributes for provisioning.

Note: Attributes marked as mandatory in [Section 1.7.2, "Attributes for Provisioning"](#) cannot be modified or removed.

As mentioned earlier in this guide, SQL statements are used for performing provisioning operations. These SQL statements are stored in the Query Configuration lookup definition. The input parameters required to run the SQL statements are retrieved from the Parameter Configuration lookup definition. The Parameter Configuration lookup definition maps identifiers used in the SQL statements and the attributes for provisioning, defined on the process form. Therefore, if you add an attribute for provisioning, then this attribute must be mapped to an identifier, which becomes the actual input parameter required to run the SQL statements. This guideline forms the basis of two of the steps that you perform while adding or removing attributes for provisioning.

The section describes the following procedures:

- [Section 4.3.1, "Adding New Standard and Custom Attributes for Provisioning"](#)
- [Section 4.3.2, "Adding New Standard and Custom Multivalued Attributes for Provisioning"](#)

- [Section 4.3.3, "Removing Attributes for Provisioning"](#)

4.3.1 Adding New Standard and Custom Attributes for Provisioning

Note: Perform the procedure described in this section only if you want to map standard or custom target system attributes for provisioning. If you want to add a standard or custom multivalued attribute for provisioning, then see [Section 4.3.2, "Adding New Standard and Custom Multivalued Attributes for Provisioning."](#)

To add a new standard or custom attribute for provisioning:

1. Add the attribute as a field on the process form as follows:

Note: Directly proceed to the next step if you have already added the field to the process form while performing the procedure described in [Section 4.2.1, "Adding New Standard and Custom Attributes for Reconciliation."](#)

- a. Expand **Development Tools**, and then double-click **Form Designer**.
- b. Search for and open the process form for the target system that you are using:
See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process form for each target system.
- c. Click **Create New Version** to create a version of the form. Then, enter a version name and click the Save icon.
- d. Click **Add**. The following screenshot shows this page:

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Applicability
1	UD_DB_ORA_U_TEMP_QUOTASIZE	String	10	Temporary Tablespace	TextField		9	
2	UD_DB_ORA_U_USERNAME	String	50	Username	TextField		2	
3	UD_DB_ORA_U_GLOBAL_DN	String	50	Global DN	TextField		5	
4	UD_DB_ORA_U_ITRES	long		IT Resource	ITResourceLookupField		1	
5	UD_DB_ORA_U_TEMP_TABLESPACE	String	50	Temporary Tablespace	LookupField		8	
6	UD_DB_ORA_U_PASSWORD	String	50	Password	PasswordField		3	
7	UD_DB_ORA_U_TABLESPACE	String	50	Default Tablespace	LookupField		6	
8	UD_DB_ORA_U_PROFILE	String	50	Profile Name	LookupField		10	
9	UD_DB_ORA_U_LOCK	String	100	Account Status	DOField		11	
10	UD_DB_ORA_U_AUTHTYPE	String	50	Authentication Type	LookupField	PASSWORD	4	
11	UD_DB_ORA_U_QUOTASIZE	String	10	Default Tablespace	TextField		7	

- e. Specify the properties of the attribute according to your requirement.

- f. Click the Save icon.
- g. Click **Make Version Active** to activate the new version of the process form.
2. Modify the Query Configuration lookup definition as follows:
 - a. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
 - b. Search for and open one of the following lookup definitions:
 - Lookup.DBUM.DB2.Query.Configuration
 - Lookup.DBUM.MSSQL.Query.Configuration
 - Lookup.DBUM.Oracle.Query.Configuration
 - Lookup.DBUM.Sybase.Query.Configuration
 - c. If you want to modify a SQL statement or stored procedure, then:
 - i. Search for the entry containing the SQL statement or stored procedure that you want to modify.
 - ii. In the **Decode** column, enter the SQL statement or stored procedure.

Note: Each identifier in the SQL statement of the Decode column must be prefixed with a colon (:). For example, REVOKE :role_name FROM :user_id.

- iii. Click the Save icon.
- d. If you want to add a SQL statement, then:
 - i. Click **Add**, to add a new row. The following screenshot shows this page:
 - ii. In the **Code Key** column, enter the name of the SQL statement that you want to add.
 - iii. In the **Decode** column, enter the SQL statement.

Note: Each identifier in the SQL statement of the Decode column must be prefixed with a colon (:). For example, REVOKE :role_name FROM :user_id.

- iv. Click the Save icon.
3. In the Parameter Configuration lookup definition, add an entry for the attribute that you added on the process form in Step 1 as follows:
 - a. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
 - b. Search for and open one of the following lookup definitions:
 - Lookup.DBUM.DB2.Parameter.Configuration
 - Lookup.DBUM.MSSQL.Parameter.Configuration
 - Lookup.DBUM.Oracle.Parameter.Configuration
 - Lookup.DBUM.Sybase.Parameter.Configuration
 - c. Click **Add**, to add a new row.

- d. In the **Code Key** column, enter the identifier (prefixed with a colon (:)) of the SQL statement that was entered in the Decode column of the Query Configuration lookup definition in Step 2.
 - e. In the **Decode** column, enter the decode value. See [Appendix A, "Preconfigured Lookup Definitions"](#) for information about the Parameter Configuration lookup definition and the format of values to be entered in the Decode column.
 - f. Click the Save icon.
 4. Add the attribute as a reconciliation field in the resource object:
 - a. On the Design Console, expand **Resource Management**, and then double-click **Resource Objects**.
 - b. Search for and open the resource object for the connector that you are using. See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the resource object for each target system.
 - c. Click **Add Field**.
 - d. Enter the field name and field type.
 - e. If you want make this a mandatory field for reconciliation, then select the Required check box.
 - f. Click the Save icon.
 5. Adding the attribute for reconciliation.

When you add an attribute on the process form, you must also enable reconciliation of values for that attribute from the target system. See [Section 4.2, "Adding or Removing Attributes for Reconciliation"](#) for more information.

4.3.2 Adding New Standard and Custom Multivalued Attributes for Provisioning

Note: This section describes the procedure to add standard or custom multivalued attributes of the target system for provisioning.

By default, the multivalued attributes listed in [Section 1.7.2, "Attributes for Provisioning"](#) are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can add new multivalued fields for provisioning.

To add a new standard or custom multivalued attribute for provisioning:

Note:

See *Oracle Identity Manager Design Console Guide* for detailed information about the steps of this procedure.

If you have already added a multivalued attribute for reconciliation, then you need not repeat steps performed as part of that procedure.

See Also: [Section 4.10, "Configuring the Connector for Reconciling and Provisioning Object-Level Privileges"](#)

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

2. Create a child form for the new multivalued attribute as follows:
 - a. Expand **Development Tools**, and then double-click **Form Designer**.
 - b. In the **Table Name** field, enter a name for the child table.
 - c. In the **Description** field, enter a description for the child form.
 - d. In the Form Type region, select **Process**.
 - e. Click the Save icon.
 - f. On the Additional Columns tab, click **Add**.
 - g. In the Name column, enter a name for the attribute.
 - h. Enter values in the remaining columns, and then click the Save icon.
 - i. If you want to add more fields, then click **Add** and enter values for each field.
3. Associate the child form with the process form as follows:

Note: Only the most basic instructions to create a child form are given in this section. See *Oracle Identity Manager Design Console Guide* for detailed instructions.

- a. Search for and open the parent process form for the target system that you are using. See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process forms for each target system.
 - b. Click **Create New Version**.
 - c. Enter a version name, and then click the Save icon.
 - d. From the **Current Version** list, select the version that you created.
 - e. On the Child Tables tab, click **Assign**.
 - f. From the list on the left, select the child table and then move it to the list on the right. Then, click **OK**.
 - g. Click **Make Version Active**.
4. Create an entry for the attribute in the Query Configuration lookup definition for multivalued attribute provisioning as follows:
 - a. Expand **Administration**, and double-click **Lookup Definition**.
 - b. Search for and open one of the following lookup definitions:
 - Lookup.DBUM.DB2.Query.Configuration
 - Lookup.DBUM.MSSQL.Query.Configuration
 - Lookup.DBUM.Oracle.Query.Configuration
 - Lookup.DBUM.Sybase.Query.Configuration
 - c. If you want to modify a SQL statement or a stored procedure, then:
 - i. Search for the entry containing the SQL statement or stored procedure that you want to modify.
 - ii. In the **Decode** column, enter the SQL statement. or stored procedure

Note: Each identifier in the SQL statement of the Decode column must be prefixed with a colon (:). For example, REVOKE :role_name FROM :user_id.

iii. Click the Save icon.

- d. If you want to add a SQL statement, then:
 - i. Click **Add**, to add a new row.
 - ii. In the **Code Key** column, enter the name of the SQL statement that you want to add.
 - iii. In the **Decode** column, enter the SQL statement.

Note: Each identifier in the SQL statement of the Decode column must be prefixed with a colon (:). For example, REVOKE :role_name FROM :user_id.

iv. Click the Save icon.

5. Create an entry for the attribute in the Parameter Configuration lookup definition for multivalued attribute provisioning as follows:
 - a. Search for and open one of the following lookup definitions:
 - Lookup.DBUM.DB2.Parameter.Configuration
 - Lookup.DBUM.MSSQL.Parameter.Configuration
 - Lookup.DBUM.Oracle.Parameter.Configuration
 - Lookup.DBUM.Sybase.Parameter.Configuration
 - b. Click **Add**, to add a new row.
 - c. In the **Code Key** column, enter the identifier (prefixed with a colon (:)) of the SQL statement that was entered in the Decode column of the Query Configuration lookup definition in Step 2.
 - d. In the **Decode** column, enter the decode value. See [Appendix A, "Preconfigured Lookup Definitions"](#) for information about the Parameter Configuration lookup definition and the format of values to be entered in the Decode column.
 - e. Click the Save icon.
6. Expand **Process Management**, and double-click **Process Definition**.
7. Search for and open the process definition. See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each target system.
8. In the process definition, create a process task for adding values in the attribute:
 - a. Click **Add**.
 - b. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:
 - Conditional
 - Required for Completion

Allow Cancellation while Pending

Allow Multiple Instances

- c. From the **Child Table** list, select the child table name.
- d. From the **Trigger Type** list, select **Insert**.
- e. Click the Save icon.
- f. On the Integration tab of the Creating New Task dialog box, click **Add**.
- g. In the Handler Selection dialog box, select **Adapter**, click the adapter, and then click the Save icon. See [Table 5–1](#) for information about adapters that you can use.

The list of adapter variables is displayed on the Integration tab.

- h. To create the mapping for the adapter variables:

Double-click the number of the first row.

In the Edit Data Mapping for Variable dialog box, enter values for the **Variable Name**, **Data Type**, and **Map To** fields, and then click the Save icon.

Repeat this step for each adapter variable that you must map. See [Table 5–2](#) for information about the adapter variables that you can map.

- i. Click the Save icon in the Editing Task dialog box, and then close the dialog box.
 - j. Click the Save icon to save changes to the process definition.
9. To enable updates of the multivalued attribute during provisioning operations, create a process task in the process definition as follows:

- a. Click **Add**.

- b. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

Conditional

Required for Completion

Allow Cancellation while Pending

Allow Multiple Instances

- c. From the **Child Table** list, select the child table name.
- d. From the **Trigger Type** list, select **Update**.
- e. Click **the Save icon**.
- f. On the Integration tab of the Creating New Task dialog box, click **Add**.
- g. In the Handler Selection dialog box, select **Adapter**, click the adapter that is used to delete the child data, and then click the Save icon. See [Table 5–1](#) for information about adapters that you can use.

The list of adapter variables is displayed on the Integration tab.

- h. To create the mapping for the first adapter variable:

Double-click the number of the first row.

In the Edit Data Mapping for Variable dialog box, enter values for the **Variable Name**, **Data Type**, and **Map To** fields, and then click the Save icon.

Repeat this step for each adapter variable that you must map. See [Table 5–2](#) for information about the adapter variables that you can map.

- i. Click the Save icon in the Editing Task dialog box, and then close the dialog box.
 - j. Click the Save icon to save changes to the process definition.
 - k. Repeat Steps 9.a and 9.b, and 9.e through 9.h to create an adapter task for adding child data.
 - l. To add the tasks to be generated when the SUCCESS response is received:
 - In the Responses section, select the row with the SUCCESS response.
 - In the Tasks To Generate section, click **Assign**.
 - In the dialog box that appears, from the left pane, select the task name created in Step 9.i
10. In the process definition, create a process task to delete values in the attribute:
 - a. Click **Add**.
 - b. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:
 - Conditional
 - Required for Completion
 - Allow Cancellation while Pending
 - Allow Multiple Instances
 - c. From the **Child Table** list, select the child table name.
 - d. From the **Trigger Type** list, select **Delete**.
 - e. Click the Save icon.
 - f. On the Integration tab of the Creating New Task dialog box, click **Add**.
 - g. In the Handler Selection dialog box, select **Adapter**, click the adapter that is used to delete the child data, and then click the Save icon. See [Table 5–1](#) for information about adapters that you can use.

The list of adapter variables is displayed on the Integration tab.
 - h. To create the mapping for the first adapter variable:
 - Double-click the number of the first row.
 - In the Edit Data Mapping for Variable dialog box, enter values for the **Variable Name**, **Data Type**, and **Map To** fields, and then click the Save icon.
 - Repeat this step for each adapter variable that you must map. See [Table 5–2](#) for information about the adapter variables that you can map.
 - i. Click the Save icon in the Editing Task dialog box, and then close the dialog box.
 - j. Click the Save icon to save changes to the process definition.
11. Save the changes to the process definition.

4.3.3 Removing Attributes for Provisioning

By default, the attributes listed in [Section 1.7.2, "Attributes for Provisioning"](#) are mapped for provisioning between Oracle Identity Manager and the target system. From that list of attributes, you must ensure that mappings for the following attributes are not modified or removed:

For IBM DB2 UDB

- IT Resource
- Username
- User Type

For Microsoft SQL Server

Attributes of the login entity:

- IT Resource
- Login Name
- Password (If creating a login based on SQL server authentication)
- Authentication Type
- Default Database (If creating a login based on Windows authentication)
- Default Language (If creating a login based on Windows authentication)

Attributes of the user entity:

- IT Resource
- Login Name
- Username
- Authentication Type
- Database Name

For Oracle Database

- IT Resource
- Username
- Password (If creating a local user by using the *BY password* clause)
- Authentication Type
- Global DN (If creating a global user by using the *GLOBALLY* clause)
- Account Status (Read-only field)

For Sybase

Attributes of the login entity:

- IT Resource
- Login Name
- Password

Attributes of the user entity:

- IT Resource
- Login Name

- Username
- Database Name (Read-only field)

To remove the attribute (field) from the process form:

Note: When you remove an attribute from the process form, you must also remove any pre-populate adapter that is associated with the attribute.

To remove an attribute for provisioning:

1. Remove the attribute as a field on the process form as follows:

Note: Directly proceed to the next step if you have already removed the field from the process form while performing the procedure described in [Section 4.2.3, "Removing Attributes Used for Reconciliation."](#)

- a. Expand **Development Tools**, and then double-click **Form Designer**.
 - b. Search for and open the process form for the connector that you are using:
See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process forms for each target system.
 - c. Click **Create New Version** to create a version of the form. Then, enter a version name and click the Save icon.
 - d. Select the attribute to be deleted, and then click **Delete**.
 - e. Click the Save icon.
 - f. Click **Make Version Active** to activate the new version of the process form.
2. In the Parameter Configuration lookup definition, remove the entry for the attribute that you removed from the process form in Step 1 as follows:
 - a. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
 - b. Search for and open one of the following lookup definitions:
 - Lookup.DBUM.DB2.Parameter.Configuration
 - Lookup.DBUM.MSSQL.Parameter.Configuration
 - Lookup.DBUM.Oracle.Parameter.Configuration
 - Lookup.DBUM.Sybase.Parameter.Configuration
 - c. Select the row containing the process form field name that you removed (in Step 1), and then click **Delete**.
 - d. Click the Save icon.
 3. To remove from the Query Configuration lookup definition, the SQL clauses that contain identifiers corresponding to the entry that you removed from the Parameter Configuration lookup definition (in Step 2):

Note: After you modify the entries in the Query Configuration lookup definition, you must run the statement by using any standard database client to ensure that the statement produces the required results when it is run against the target system database.

- a. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
 - b. Search for and open one of the following lookup definitions:
 - Lookup.DBUM.DB2.Query.Configuration
 - Lookup.DBUM.MSSQL.Query.Configuration
 - Lookup.DBUM.Oracle.Query.Configuration
 - Lookup.DBUM.Sybase.Query.Configuration
 - Lookup.DBUM.ExampleDatabase.Query.Configuration
 - c. Search for the entry that contains the SQL fragment that you want to remove.
 - d. In the Decode column, remove the SQL fragment and its corresponding identifier along with its colon (:) prefix.
 - e. Click the Save icon.
4. Remove the attribute (reconciliation field) from the resource object:
 - a. On the Design Console, expand **Resource Management**, and then double-click **Resource Objects**.
 - b. Search for and open the resource object for the connector that you are using.
See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the resource objects for each target system.
 - c. Select the field that you want to remove, and then click **Delete Field**.
 - d. Click the Save icon.
 5. From the appropriate provisioning process definition, delete the process task corresponding to the attribute that you deleted (in Step 1) as follows:
 - a. On the Design Console, expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the process definition corresponding to the process form that you used in Step 1. See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each target system.
 - c. On the Tasks tab, select the process task to be deleted and then click **Delete**.
 - d. Click the Save icon.
 6. Remove the attribute for reconciliation as follows:
See [Section 4.2.3, "Removing Attributes Used for Reconciliation"](#) for more information.

4.4 Modifying Field Lengths on the Process Form

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

If you want to modify the length of field on the process form, then:

1. Log in to the Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the process form.

See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of process forms for each connector.

4. Click **Create New Version**.
5. Modify the length of the required field.
6. Save the form and make the version active
7. Click the Save icon.

4.5 Configuring the Connector for Multiple Installations of the Target System

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

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

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

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

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

All connector objects are linked. For example, a scheduled task holds the name of the IT resource. Similarly, the IT resource for a target system such as Oracle Database holds the name of the configuration lookup definition, Lookup.DBUM.Oracle.Configuration. If you create a copy of an object, then you must specify the name of the copy in associated connector objects.

[Table 4–2](#) lists associations between connector objects whose copies can be created and the other objects that reference these objects. When you create a copy of a connector object, use this information to change the associations of that object with other objects.

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

Table 4–2 Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
For IBM DB2 UDB			
IT resource	DB2UDB	<ul style="list-style-type: none"> UD_DB_DB2_U (process form) <p>Scheduled Tasks:</p> <ul style="list-style-type: none"> DBUM DB2 Target Resource User Reconciliation DBUM DB2 Target Delete Reconciliation DBUM DB2 Trusted Resource User Reconciliation DBUM DB2 Trusted Delete Reconciliation 	You need to create a copy of IT resource with a different name.
Resource object	DB2 DB User	<p>Scheduled Tasks:</p> <ul style="list-style-type: none"> DBUM DB2 Target Resource User Reconciliation DBUM DB2 Target Delete Reconciliation DBUM DB2 Trusted Resource User Reconciliation DBUM DB2 Trusted Delete Reconciliation 	<p>It is optional to create a copy of the resource object. If you are reconciling the same set of attributes from all installations of the target system, then you need not create a copy of the resource object.</p> <p>Note: Create copies of the resource object only if there are differences in attributes between the various installations of the target system.</p>
Process definition	DB2 DB User	NA	<p>It is optional to create a copy of the process definition. If you are reconciling or provisioning the same set of attributes from all installations of the target system, then you need not create a copy of the process definition.</p> <p>Note: Create copies of the process form only if there are differences in attributes between the various installations of the target system.</p>
Process form	UD_DB_DB2_U	DB2 DB User (Process definition)	<p>It is optional to create a copy of the process form. If you are provisioning the same set of attributes from all installations of the target system, then you need not create a copy of the process definition.</p> <p>Note: Create copies of the process form only if there are differences in attributes between the various installations of the target system.</p>
Child process form	<ul style="list-style-type: none"> UD_DB_DB2_T UD_DB_DB2_S 	<ul style="list-style-type: none"> DB2 DB User (Process definition) UD_DB_DB2_U (Process form) 	It is optional to create a copy of the child process form. If you are provisioning a new set of child data, then you need to create a copy of the child and parent process forms. Then, assign the newly created child process form to the newly created parent process form.

Table 4–2 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Configuration lookup definition for a target system configured as a target resource	Lookup.DBUM.DB2.Configuration	DB2UDB (IT resource)	<p>It is optional to create a copy of the configuration lookup definition. If you are provisioning and reconciling the same set of attributes in all installations of the target system (configured as a target resource), then you need not create a copy of the configuration lookup definition.</p> <p>Note: Create copies of the configuration lookup definition only if there are differences in attributes between the various installations of the target system and you have created a new process form.</p>
Configuration lookup definition for a target system configured as a trusted source	Lookup.DBUM.DB2.TrustedRecon.Configuration	DB2UDB (IT resource)	<p>It is optional to create a copy of the configuration lookup definition. If you are reconciling the same set of attributes in all installations of the target system (configured as a trusted source), then you need not create a copy of the configuration lookup definition.</p> <p>Note: Create copies of the configuration lookup definition for trusted source only if there are differences in attributes between the various installations of the target system and you have created a new process form.</p>
Query configuration lookup definition	Lookup.DBUM.DB2.Query.Configuration	Lookup.DBUM.DB2.Configuration (Configuration lookup definition)	<p>It is optional to create a copy of the query configuration lookup definition. If you are provisioning the same set of attributes in all installations of the target system and using the same configuration lookup definition, then you need not create a copy of query configuration lookup definition.</p> <p>Note: Create copies of the query configuration lookup only if all the following statements are true:</p> <ul style="list-style-type: none"> ■ There are differences in attributes between the various installations of the target system. ■ You have created a copy of the process form. ■ You have created a copy of the configuration lookup definition.

Table 4–2 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Parameter configuration lookup definition	Lookup.DBUM.DB2.Parameter.Configuration	Lookup.DBUM.DB2.Configuration (Configuration lookup definition)	<p>It is optional to create a copy of the parameter configuration lookup. If you are provisioning the same set of attributes in all installations of the target system and using the same configuration lookup definition, then you need not create a copy of configuration lookup.</p> <p>Note: Create copies of the parameter configuration lookup definition only if all the following statements are true:</p> <ul style="list-style-type: none"> ■ There are differences in attributes between the various installations of the target system. ■ You have created a copy of the process form ■ You have created a copy of the query configuration lookup definition.
Resource object attributes mapping lookup definition (for target resource)	Lookup.DBUM.DB2.TargetRecon.Mapping	NA	<p>It is optional to create a copy of the resource object attribute mapping lookup definition. If you are reconciling the same set of attributes in all installations of the target system (configured as a target resource), then you need not to create a copy of resource object attribute mapping lookup.</p> <p>Note: Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.</p>
Resource object attributes mapping lookup definition (for trusted source)	Lookup.DBUM.DB2.TrustedRecon.Mapping	NA	<p>It is optional to create a copy of resource object attribute mapping lookup. If you are reconciling the same set of attributes in all installations of the target system (configured as a trusted source), then you need not to create a copy of resource object attribute mapping lookup.</p> <p>Note: Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.</p>
For Microsoft SQL Server			

Table 4–2 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
IT resource	MS SQLServer	Process forms: <ul style="list-style-type: none"> ■ UD_DB_SQL_L ■ UD_DB_SQL_U Scheduled Tasks: <ul style="list-style-type: none"> ■ DBUM MSSQL Trusted Resource Login Reconciliation ■ DBUM MSSQL Trusted Delete Reconciliation ■ DBUM MSSQL Target Resource Login Reconciliation ■ DBUM MSSQL Target Resource User Reconciliation ■ DBUM MSSQL Target Delete User Reconciliation ■ DBUM MSSQL Target Delete Login Reconciliation 	You need to create a copy of IT resource with a different name.
Resource object	<ul style="list-style-type: none"> ■ MSSQL DB User Login ■ MSSQL DB User 	Scheduled Tasks: <ul style="list-style-type: none"> ■ DBUM MSSQL Trusted Resource Login Reconciliation ■ DBUM MSSQL Trusted Delete Reconciliation ■ DBUM MSSQL Target Resource Login Reconciliation ■ DBUM MSSQL Target Resource User Reconciliation ■ DBUM MSSQL Target Delete User Reconciliation ■ DBUM MSSQL Target Delete Login Reconciliation 	It is optional to create a copy of the resource object. If you are reconciling the same set of attributes from all installations of the target system, then you need not create a copy of the resource object. Note: Create copies of the resource object only if there are differences in attributes between the various installations of the target system.
Process definition	<ul style="list-style-type: none"> ■ MSSQL DB User Login ■ MSSQL DB User 	NA	It is optional to create a copy of the process definition. If you are reconciling or provisioning the same set of attributes from all installations of the target system, then you need not create a copy of the process definition. Note: Create copies of the process form only if there are differences in attributes between the various installations of the target system.

Table 4–2 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Process form	<ul style="list-style-type: none"> UD_DB_SQL_L UD_DB_SQL_U 	Process definitions: <ul style="list-style-type: none"> MSSQL DB User Login MSSQL DB User 	<p>It is optional to create a copy of the process form. If you are provisioning the same set of attributes from all installations of the target system, then you need not create a copy of the process definition.</p> <p>Note: Create copies of the process form only if there are differences in attributes between the various installations of the target system.</p>
Child process form	UD_DB_SQL_R	<ul style="list-style-type: none"> MSSQL DB User (Process definition) UD_DB_SQL_U (Process form) 	<p>It is optional to create a copy of the child process form. If you are provisioning a new set of child data, then you need to create a copy of the child and parent process form. Then, assign the newly created child process form to the newly created parent process form.</p>
Configuration lookup definition for a target system configured as a target resource	Lookup.DBUM.MSSQL.Configuration	MS SQLServer (IT resource)	<p>It is optional to create a copy of the configuration lookup definition. If you are provisioning and reconciling the same set of attributes in all installations of the target system (configured as a target resource), then you need not create a copy of the configuration lookup definition.</p> <p>Note: Create copies of the configuration lookup definition only if there are differences in attributes between the various installations of the target system and you have created a new process form.</p>
Configuration lookup definition for a target system configured as a trusted source	Lookup.DBUM.MSSQL.TrustedRecon.Configuration	MS SQLServer (IT resource)	<p>It is optional to create a copy of the configuration lookup definition. If you are reconciling the same set of attributes in all installations of the target system (configured as a trusted source), then you need not create a copy of the configuration lookup definition.</p> <p>Note: Create copies of the configuration lookup definition for trusted source only if there are differences in attributes between the various installations of the target system and you have created a new process form.</p>

Table 4–2 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Query configuration lookup definition	Lookup.DBUM.MSSQL.Query.Configuration	Lookup.DBUM.MSSQL.Configuration (Configuration lookup definition)	<p>It is optional to create a copy of the query configuration lookup definition. If you are provisioning the same set of attributes in all installations of the target system and using the same configuration lookup definition, then you need not create a copy of query configuration lookup definition.</p> <p>Note: Create copies of the query configuration lookup only if all the following statements are true:</p> <ul style="list-style-type: none"> ■ There are differences in attributes between the various installations of the target system. ■ You have created a copy of the process form. ■ You have created a copy of the configuration lookup definition.
Parameter configuration lookup definition	Lookup.DBUM.MSSQL.Parameter.Configuration	<ul style="list-style-type: none"> ■ Lookup.DBUM.MSSQL.Configuration (Configuration lookup definition) 	<p>It is optional to create a copy of the parameter configuration lookup. If you are provisioning the same set of attributes in all installations of the target system and using the same configuration lookup definition, then you need not create a copy of configuration lookup.</p> <p>Note: Create copies of the parameter configuration lookup definition only if all the following statements are true:</p> <ul style="list-style-type: none"> ■ There are differences in attributes between the various installations of the target system. ■ You have created a copy of the process form ■ You have created a copy of the query configuration lookup definition.
Resource object attributes mapping lookup definition (for target resource)	<ul style="list-style-type: none"> ■ Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping ■ Lookup.DBUM.MSSQL.TargetRecon.User.Mapping 	NA	<p>It is optional to create a copy of resource object attribute mapping lookup. If you are reconciling the same set of attributes in all installations of the target system, then you need not to create a copy of resource object attribute mapping lookup.</p> <p>Note: Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.</p>

Table 4–2 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Resource object attributes mapping lookup definition (for trusted source)	Lookup.DBUM.MSSQL.TrustedRecon.Login.Mapping		<p>It is optional to create a copy of resource object attribute mapping lookup. If you are reconciling the same set of attributes in all installations of the target system (configured as a trusted source), then you need not to create a copy of resource object attribute mapping lookup.</p> <p>Note: Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.</p>
For Oracle Database			
IT resource	Oracle	<ul style="list-style-type: none"> UD_DB_ORA_U (process form) <p>Scheduled tasks:</p> <ul style="list-style-type: none"> DBUM Oracle Target Resource User Reconciliation DBUM Oracle Target Delete Reconciliation DBUM Oracle Trusted Resource User Reconciliation DBUM Oracle Trusted Delete Reconciliation 	Create a copy of the IT resource with a different name.
Resource object	Oracle DB User	<p>Scheduled Tasks:</p> <ul style="list-style-type: none"> DBUM DB2 Target Resource User Reconciliation DBUM DB2 Target Delete Reconciliation DBUM DB2 Trusted Resource User Reconciliation DBUM DB2 Trusted Delete Reconciliation 	<p>It is optional to create a copy of the resource object. If you are reconciling the same set of attributes from all installations of the target system, then you need not create a copy of the resource object.</p> <p>Note: Create copies of the resource object only if there are differences in attributes between the various installations of the target system.</p>
Process definition	Oracle DB User	NA	<p>It is optional to create a copy of the process definition. If you are reconciling or provisioning the same set of attributes from all installations of the target system, then you need not create a copy of the process definition.</p> <p>Note: Create copies of the process form only if there are differences in attributes between the various installations of the target system.</p>

Table 4–2 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Process form	UD_DB_ORA_U	Oracle DB User (Process definition)	<p>It is optional to create a copy of the process form. If you are provisioning the same set of attributes from all installations of the target system, then you need not create a copy of the process definition.</p> <p>Note: Create copies of the process form only if there are differences in attributes between the various installations of the target system.</p>
Child process form	<ul style="list-style-type: none"> ■ UD_DB_ORA_R ■ UD_DB_ORA_P 	<ul style="list-style-type: none"> ■ Oracle DB User (Process definition) ■ UD_DB_ORA_U (Process form) 	<p>It is optional to create a copy of the child process form. If you are provisioning a new set of child data, then you need to create a copy of the child and parent process forms. Then, assign the newly created child process form to the newly created parent process form.</p>
Configuration lookup definition for a target system configured as a target resource	Lookup.DBUM. Oracle.Configuration	Oracle (IT resource)	<p>It is optional to create a copy of the configuration lookup definition. If you are provisioning and reconciling the same set of attributes in all installations of the target system (configured as a target resource), then you need not create a copy of the configuration lookup definition.</p> <p>Note: Create copies of the configuration lookup definition only if there are differences in attributes between the various installations of the target system and you have created a new process form.</p>
Configuration lookup definition for a target system configured as a trusted source	Lookup.DBUM. Oracle.TrustedRe con.Configuration	Oracle (IT resource)	<p>It is optional to create a copy of the configuration lookup definition. If you are reconciling the same set of attributes in all installations of the target system (configured as a trusted source), then you need not create a copy of the configuration lookup definition.</p> <p>Note: Create copies of the configuration lookup definition for trusted source only if there are differences in attributes between the various installations of the target system and you have created a new process form.</p>

Table 4–2 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Query configuration lookup definition	Lookup.DBUM. Oracle.Query.Co nfiguration	Lookup.DBUM.Oracle.Configurat ion (Configuration lookup definition)	<p>It is optional to create a copy of the query configuration lookup definition. If you are provisioning the same set of attributes in all installations of the target system and using the same configuration lookup definition, then you need not create a copy of query configuration lookup definition.</p> <p>Note: Create copies of the query configuration lookup only if all the following statements are true:</p> <ul style="list-style-type: none"> ■ There are differences in attributes between the various installations of the target system. ■ You have created a copy of the process form. ■ You have created a copy of the configuration lookup definition.
Parameter configuration lookup definition	Lookup.DBUM. Oracle.Parameter Configuration	Lookup.DBUM.Oracle.Configurat ion (Configuration lookup definition)	<p>It is optional to create a copy of the parameter configuration lookup. If you are provisioning the same set of attributes in all installations of the target system and using the same configuration lookup definition, then you need not create a copy of configuration lookup.</p> <p>Note: Create copies of the parameter configuration lookup definition only if all the following statements are true:</p> <ul style="list-style-type: none"> ■ There are differences in attributes between the various installations of the target system. ■ You have created a copy of the process form ■ You have created a copy of the query configuration lookup definition.
Resource object attributes mapping lookup definition (for target resource)	Lookup.DBUM. Oracle.TargetRec on.Mapping	NA	<p>It is optional to create a copy of resource object attribute mapping lookup definition. If you are reconciling the same set of attributes in all installations of the target system, then you need not to create a copy of resource object attribute mapping lookup.</p> <p>Note: Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.</p>

Table 4–2 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Resource object attributes mapping lookup definition (for trusted source)	Lookup.DBUM. Oracle.TrustedRe con.Mapping	NA	<p>It is optional to create a copy of resource object attribute mapping lookup definition. If you are reconciling the same set of attributes in all installations of the target system, then you need not to create a copy of resource object attribute mapping lookup.</p> <p>Note: Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.</p>
For Sybase			
IT resource	Sybase	Process forms: <ul style="list-style-type: none"> UD_DB_SYB_L UD_DB_SYB_U Scheduled tasks: <ul style="list-style-type: none"> DBUM Sybase Trusted Resource Login Reconciliation DBUM Sybase Trusted Delete Reconciliation DBUM Sybase Target Resource Login Reconciliation DBUM Sybase Target Resource User Reconciliation DBUM Sybase Target Delete User Reconciliation DBUM Sybase Target Delete Login Reconciliation 	Create a copy of the IT resource with a different name.
Resource object	<ul style="list-style-type: none"> Sybase DB User Login Sybase DB User 	Scheduled Tasks: <ul style="list-style-type: none"> DBUM Sybase Trusted Resource Login Reconciliation DBUM Sybase Trusted Delete Reconciliation DBUM Sybase Target Resource User Reconciliation DBUM Sybase Target Delete User Reconciliation DBUM Sybase Target Delete Login Reconciliation 	<p>It is optional to create a copy of the resource object. If you are reconciling the same set of attributes from all installations of the target system, then you need not create a copy of the resource object.</p> <p>Note: Create copies of the resource object only if there are differences in attributes between the various installations of the target system.</p>

Table 4–2 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Process definition	<ul style="list-style-type: none"> ■ Sybase DB User Login ■ Sybase DB User 	NA	<p>It is optional to create a copy of the process definition. If you are reconciling or provisioning the same set of attributes from all installations of the target system, then you need not create a copy of the process definition.</p> <p>Note: Create copies of the process form only if there are differences in attributes between the various installations of the target system.</p>
Process form	<ul style="list-style-type: none"> ■ UD_DB_SYB_L ■ UD_DB_SYB_U 	<p>Process definitions:</p> <ul style="list-style-type: none"> ■ Sybase DB User Login ■ Sybase DB User 	<p>It is optional to create a copy of the process form. If you are provisioning the same set of attributes from all installations of the target system, then you need not create a copy of the process definition.</p> <p>Note: Create copies of the process form only if there are differences in attributes between the various installations of the target system.</p>
Child process form	UD_DB_SYB_R	<ul style="list-style-type: none"> ■ Sybase DB User Login (Process form) ■ Sybase DB User Login (Process definition) 	<p>It is optional to create a copy of the child process form. If you are provisioning a new set of child data, then you need to create a copy of the child and parent process forms. Then, assign the newly created child process form to the newly created parent process form.</p>
Configuration lookup definition for a target system configured as a target resource	Lookup.DBUM.Sybase.Configuration	Oracle (IT resource)	<p>It is optional to create a copy of the configuration lookup definition. If you are provisioning the same set of attributes in all installations of the target system, then you need not create a copy of configuration lookup.</p> <p>Note: Create copies of the configuration lookup definition only if there are differences in attributes between the various installations of the target system and you have created a new process form.</p>
Configuration lookup definition for a target system configured as a trusted source	Lookup.DBUM.Oracle.TrustedResource.Configuration	Oracle (IT resource)	<p>It is optional to create a copy of the configuration lookup definition. If you are reconciling the same set of attributes in all installations of the target system (configured as a trusted source), then you need not create a copy of the configuration lookup definition.</p> <p>Note: Create copies of the configuration lookup definition for trusted source only if there are differences in attributes between the various installations of the target system and you have created a new process form.</p>

Table 4–2 (Cont.) Connector Objects and Their Associations

Connector Object	Name	Referenced By	Comments on Creating a Copy
Query configuration lookup definition	Lookup.DBUM.Sybase.Query.Configuration	Lookup.DBUM.Sybase.Configuration (Configuration lookup definition)	<p>It is optional to create a copy of the query configuration lookup definition. If you are provisioning the same set of attributes in all installations of the target system and using the same configuration lookup definition, then you need not create a copy of query configuration lookup definition.</p> <p>Note: Create copies of the query configuration lookup only if all the following statements are true:</p> <ul style="list-style-type: none"> ■ There are differences in attributes between the various installations of the target system. ■ You have created a copy of the process form. ■ You have created a copy of the configuration lookup definition.
Parameter configuration lookup definition	Lookup.DBUM.Sybase.Parameter Configuration	Lookup.DBUM.Sybase.Configuration (Configuration lookup definition)	<p>It is optional to create a copy of the parameter configuration lookup. If you are provisioning the same set of attributes in all installations of the target system and using the same configuration lookup definition, then you need not create a copy of configuration lookup.</p> <p>Note: Create copies of the parameter configuration lookup definition only if all the following statements are true:</p> <ul style="list-style-type: none"> ■ There are differences in attributes between the various installations of the target system. ■ You have created a copy of the process form ■ You have created a copy of the query configuration lookup definition.
Resource object attributes mapping lookup definition	<p>For target resource:</p> <ul style="list-style-type: none"> ■ Lookup.DBUM.Sybase.TargetRecon.Login.Mapping ■ Lookup.DBUM.Sybase.TargetRecon.User.Mapping <p>For trusted source:</p> <ul style="list-style-type: none"> ■ Lookup.DBUM.Sybase.TrustedRecon.Login.Mapping 	NA	<p>It is optional to create a copy of resource object attribute mapping lookup definition. If you are reconciling the same set of attributes in all installations of the target system, then you need not to create a copy of resource object attribute mapping lookup.</p> <p>Note: Create copies of this lookup definition only if there are differences in attributes between the two installations of the target system.</p>

When you configure reconciliation:

To reconcile data from a particular target system installation, specify the name of the IT resource for that target system installation as the value of the scheduled task attribute that holds the IT resource name. For example, if you are using Oracle Database as the target system, then you enter the name of the IT resource as the value of the IT resource attribute of the scheduled task that you run.

When you perform provisioning operations:

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

4.5.1 Enabling the Dependent Lookup Fields Feature

When you perform a provisioning operation, lookup fields on the Administrative and User Console allow you to select values from lists. Some of these lookup fields are populated with values copied from the target system.

For release 9.1.0 of the connector, the Dependent Lookup Fields feature is disabled by default. If you have multiple installations of the target system, then you can enable this feature after you deploy the Oracle Identity Manager release 9.1.0.2 bundle patch that addresses Bug 9181280.

If you enable the Dependent Lookup Fields feature, then entries in the lookup field are linked with the target system installation from which the entries are copied. This allows you to select lookup field values that are specific to the target system installation on which the provisioning operation is to be performed.

Note: The bundle patch that addressed Bug 9181280 had not been released at the time of release of this connector.

To enable the Dependent Lookup Fields feature after you deploy the bundle patch that addresses Bug 9181280, you must make changes in the forms listed in [Table 4-3](#). This table lists the forms, the lookup fields on the forms, and the lookup query that you must use for each lookup field. The procedure is described after the table.

Table 4–3 Queries for Lookup Field Synchronization

Process Form	Lookup Field	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
For IBM DB2 UDB			
UD_DB_DB2_T Note: This is a child form.	Tablespace	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.DB2.Table spaces' AND lkv_encoded like CONCAT('\$Form data. UD_DB_DB2_U_ITRES \$',~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key=lku.lku_key AND lku_type_string_key='Lookup.DBUM.DB2.Tablespace' AND lkv_encoded like '\$Formdata. UD_DB_DB2_U_ITRES\$' + '~%'
UD_DB_DB2_S Note: This is a child form.	Schema	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.DB2.Sche ma' AND lkv_encoded like CONCAT('\$Form data. UD_DB_DB2_U_ITRES \$',~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key=lku.lku_key AND lku_type_string_key='Lookup.DBUM.DB2.Schema' AND lkv_encoded like '\$Formdata. UD_DB_DB2_U_ITRES\$' + '~%'
For Microsoft SQL Server			
UD_DB_SQL_R Note: This is a child form.	Role	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.MSSQL.D BRoles' AND lkv_encoded like CONCAT('\$Form data. UD_DB_SQL_U_ITRES \$',~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key=lku.lku_key AND lku_type_string_key='Lookup.DBUM.MSSQL.DBRoles' AND lkv_encoded like '\$Formdata. UD_DB_SQL_U_ITRES\$' + '~%'
UD_DB_SQL_L	Default DataBase	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.MSSQL.D BNames' AND lkv_encoded like CONCAT('\$Form data. UD_DB_SQL_L_ITRES\$', ~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key=lku.lku_key AND lku_type_string_key='Lookup.DBUM.MSSQL.DBNames' AND lkv_encoded like '\$Formdata. UD_DB_SQL_L_ITRES\$' + '~%'

Table 4–3 (Cont.) Queries for Lookup Field Synchronization

Process Form	Lookup Field	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
UD_DB_SQL_L	Default Language	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.MSSQL.D efaultLang' AND lkv_encoded like CONCAT('\$Form data. UD_DB_SQL_L_ITRES\$', ~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key=lku.lku_key AND lku_type_string_key='Lookup.DBU M.MSSQL.DefaultLang' AND lkv_encoded like'\$Formdata. UD_DB_SQL_L_ITRES\$' + '~%'
For Oracle Database			
UD_DB_ORA_P Note: This is a child form.	Privilege	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.Oracle.Pri vileges' AND lkv_encoded like CONCAT('\$Form data. UD_DB_ORA_U_ITRES\$', ~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key=lku.lku_key AND lku_type_string_key='Lookup.DBU M.Oracle.Privileges' AND lkv_encoded like'\$Formdata. UD_DB_ORA_U_ITRES\$' + '~%'
UD_DB_ORA_U	Default Tablespace	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.Oracle.Ta blespaces' AND lkv_encoded like CONCAT('\$Form data. UD_DB_ORA_U_ITRES\$', ~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key=lku.lku_key AND lku_type_string_key='Lookup.DBU M.Oracle.Tablespace' AND lkv_encoded like'\$Formdata. UD_DB_ORA_U_ITRES\$' + '~%'
UD_DB_ORA_U	Temporary Tablespace	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.Oracle.Te mp.Tablespace' AND lkv_encoded like CONCAT('\$Form data. UD_DB_ORA_U_ITRES\$', ~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key=lku.lku_key AND lku_type_string_key='Lookup.DBU M.Oracle.Temp.Tablespace' AND lkv_encoded like'\$Formdata. UD_DB_ORA_U_ITRES\$' + '~%'

Table 4–3 (Cont.) Queries for Lookup Field Synchronization

Process Form	Lookup Field	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
UD_DB_ORA_U	Profile Name	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.Oracle.Pr ofiles' AND lkv_encoded like CONCAT('\$Form data. UD_DB_ORA_U_ITRES\$', ~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key=lku.lku_key AND lku_type_string_key='Lookup.DBU M.Oracle.Profiles' AND lkv_encoded like '\$Formdata. UD_DB_ORA_U_ITRES\$' + '~%'
UD_DB_ORA_R Note: This is a child form.	Role	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.Oracle.Ro les' AND lkv_encoded like CONCAT('\$Form data. UD_DB_ORA_U_ITRES\$', ~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key=lku.lku_key AND lku_type_string_key='Lookup.DBU M.Oracle.Roles' AND lkv_encoded like '\$Formdata. UD_DB_ORA_U_ITRES\$' + '~%'
For Sybase			
UD_DB_SYB_R Note: This is a child form.	Role	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.Sybase.Ro les' AND lkv_encoded like CONCAT('\$Form data. UD_DB_SYB_L_ITRES \$',~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key =lku.lku_key AND lku_type_string_key='Lookup.DBU M.Sybase.Roles' AND lkv_encoded like '\$Formdata. UD_DB_SYB_L_ITRES\$' + '~%'

Table 4–3 (Cont.) Queries for Lookup Field Synchronization

Process Form	Lookup Field	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
UD_DB_SYB_U	Database Group	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.Sybase.D BGroups' AND lkv_encoded like CONCAT('\$Form data. UD_DB_SYB_U_ITRES \$',~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key =lku.lku_key AND lku_type_string_key='Lookup.DBU M.Sybase.DBGroups' AND lkv_encoded like'\$Formdata. UD_DB_SYB_U_ITRES\$' + '~%'
UD_DB_SYB_L	Default Database	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.Sybase.Da tabases' AND lkv_encoded like CONCAT('\$Form data. UD_DB_SYB_L_ITRES \$',~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key =lku.lku_key AND lku_type_string_key='Lookup.DBU M.Sybase.Databases' AND lkv_encoded like'\$Formdata. UD_DB_SYB_L_ITRES\$' + '~%'
UD_DB_SYB_L	Default Language	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key = lku.lku_key AND lku_type_string_key = 'Lookup.DBUM.Sybase.De faultLang' AND lkv_encoded like CONCAT('\$Form data. UD_DB_SYB_L_ITRES \$',~%')	SELECT lkv_encoded,lkv_decoded FROM lkv lkv,lku lku WHERE lkv.lku_key =lku.lku_key AND lku_type_string_key='Lookup.DBU M.Sybase.DefaultLang' AND lkv_encoded like'\$Formdata. UD_DB_SYB_L_ITRES\$' + '~%'

To enable lookup fields on each form:

Note: You must enable lookup fields in the order given in Table 5–3.

1. On the Design Console, expand **Development Tools** and double-click **Form Designer**.
2. Search for and open the form for the target system that you are using. See [Section 4.5, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process forms for each target system.
3. Click **Create New Version**, enter a new version number, and then save the version.
4. From the **Current Version** list, select the version that you created.
5. Open the **Properties** tab, and expand **Components**.
6. Add properties for each lookup field on the form as follows:
 - a. Select the **Lookup Code** property, and then click **Delete Property**.

- b. Select the first lookup field on the form, and then click **Add Property**. For example, if you are using Oracle Database as the target system, then select Privilege on the the UD_DB_ORA_P form.
 - c. In the Add Property dialog box:
 From the Property Name list, select **Lookup Column Name**.
 In the **Property Value** field, enter `1kv_encoded`.
 Click the Save icon, and then close the dialog box.
 - d. Select the lookup field, and then click **Add Property**.
 - e. In the Add Property dialog box:
 From the Property Name list, select **Column Names**.
 In the **Property Value** field, enter `1kv_encoded`.
 Click the Save icon, and then close the dialog box.
 - f. Select the lookup field, and then click **Add Property**.
 - g. In the Add Property dialog box:
 From the Property Name list, select **Column Widths**.
 In the **Property Value** field, enter `234`.
 - h. Select the lookup field, and then click **Add Property**.
 - i. In the Add Property dialog box:
 From the Property Name list, select **Column Captions**.
 In the **Property Value** field, enter `1kv_encoded`.
 Click the Save icon, and then close the dialog box.
 - j. Select the lookup field, and then click **Add Property**.
 - k. In the Add Property dialog box:
 From the Property Name list, select **Lookup Query**.
 In the Property Value field, enter the query given in [Table 4-3](#).
 Click the Save icon, and then close the dialog box.
7. Repeat Step 6 for each lookup field on the form.
8. Click the Save icon to save the changes to the form.
9. Click **Make Version Active**.
10. If you have performed Steps 2 through 9 on a child form, then:
 - a. Expand **Development Tools** and double-click **Form Designer**.
 - b. Search for and open the parent form with which the child form is associated form.
 - c. Click **Create New Version**, enter a new version number, and then save the version.
 - d. Click **Make Version Active**.

4.6 Configuring the Connector for Multiple Trusted Source Reconciliation

Note:

This connector supports multiple trusted source reconciliation.

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 users. 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 person data in your organization.

See *Oracle Identity Manager Design Console Guide* for detailed information about multiple trusted source reconciliation.

4.7 Configuring Reconciliation Queries

Note: This section describes an optional procedure. Perform this procedure only if you want to modify one of the predefined reconciliation queries or create your own query.

You can modify existing queries in the properties file. In addition, you can add your own queries in the file. The query whose name you specify as the value of the Query Name scheduled task attribute is applied during reconciliation.

To modify an existing query or to add a query in the properties file:

Caution: You must not modify the Delete Users query in the reconciliation properties file. If you add a WHERE clause to this query, then only a subset of the actual set of users is brought to Oracle Identity Manager for comparison. OIM Users whose user IDs do not match any of these users are deleted from Oracle Identity Manager.

1. Open the properties file in a text editor. If you are creating your own properties file, then ensure that the extension is .properties. You can place this properties file in any directory on the target system host computer.
2. Apply the following guidelines while modifying or adding a query:

Note: Before you modify or add a query in the properties file, you must run the query by using any standard database client to ensure that the query produces the required results when it is run against the target system database.

- Query Name

Do not include spaces in the query name.

Ensure that the query name is not the same as the name of any other query in the properties file.

- SELECT clause

Add or modify the column list in the SELECT clause. Note that changes that you make in the SELECT clause must be duplicated in the lookup definition that holds mappings between resource object fields and target system column names and, if required, on the process form. See Section 5.2.1, "Adding New Single-Valued Attributes for Reconciliation" for more information.

- Comments

Use the number sign to begin each comment line in the properties file.

Add comments to describe changes that you make in existing queries and also to describe new queries that you add in the file.

See existing comments in the file for an example.

- Line breaks

If you want to introduce line breaks in the query (to improve readability), then add a backslash (\) at the end of each line.

- SQL keywords

You must ensure that the query does not contain any clause or keyword that modifies or can be used to modify data in the database.

3. Save and close the properties file.

4.8 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the 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.

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

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

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

To configure validation of data:

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

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

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

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

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

2. Create a JAR file to hold the Java class.
3. Copy the JAR file into the JavaTasks or ScheduleTask directory.
4. If you created the Java class for validating a process form field for reconciliation, then:
 - a. Log in to the Design Console.
 - b. If you have configured your target system as a target resource, then search for and open one of the following lookup definitions:
 - Lookup.DBUM.DB2.TargetRecon.Validation
 - Lookup.DBUM.MSSQL.TargetRecon.Validation
 - Lookup.DBUM.Oracle.TargetRecon.Validation
 - Lookup.DBUM.Sybase.TargetRecon.Validation
 - c. If you have configured your target system as a trusted source, then search for and open one of the following lookup definitions:
 - Lookup.DBUM.DB2.TrustedRecon.Validation
 - Lookup.DBUM.MSSQL.TrustedRecon.Validation

- Lookup.DBUM.Oracle.TrustedRecon.Validation
- Lookup.DBUM.Sybase.TrustedRecon.Validation
- d. In the **Code Key**, enter the resource object attribute name. In the **Decode**, enter the class name that is implementing the validation logic.

For example, if you want to perform validation of the First Name attribute, then you must enter the following values in the Code Key and Decode columns:

Code Key: First Name

Decode: oracle.iam.connectors.recon.validation

Here, the Code Key specifies the name of the resource object attribute that you want to validate and Decode is the complete package name of the Implementation class.
- e. Save the changes to the lookup definition.
- f. To enable validation, in the scheduled task for your database, set the value of the **Use Validation For Reconciliation** entry to *yes*, and then save your changes.
- 5. If you created the Java class for validating a process form field for provisioning, then:
 - a. Log in to the Design Console.
 - b. Search for and open one of the following lookup definitions:
 - Lookup.DBUM.DB2.Provisioning.Validation
 - Lookup.DBUM.MSSQL.Provisioning.Validation
 - Lookup.DBUM.Oracle.Provisioning.Validation
 - Lookup.DBUM.Sybase.Provisioning.Validation
 - c. In the **Code Key**, enter the process form field name. In the **Decode**, enter the class name that is implementing the validation logic.

For example, if you want to perform validation of the User Name process form field, then you must enter the following values in the Code Key and Decode columns:

Code Key: UD_DB_DB2_U_USERNAME

Decode: DataValidator.java

Here, the Code Key specifies the name of the resource object attribute that you want to validate and Decode is the name of the class that is implementing the validation logic.
 - d. Save the changes to the lookup definition.
 - e. To enable validation for provisioning:
 - Search for and open one of the following lookup definitions:
 - Lookup.DBUM.DB2.Configuration
 - Lookup.DBUM.MSSQL.Configuration
 - Lookup.DBUM.Oracle.Configuration
 - Lookup.DBUM.Sybase.Configuration

- Provide values for the following lookup entries:
 - i. **Use Validation For Provisioning:** Enter `yes` to specify that you want to enable validation.
 - ii. **Provisioning Validation Lookup:** Ensure that the value of this entry is

4.9 Configuring Transformation of Data During Reconciliation

You can configure transformation of reconciled single-valued 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.

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

To configure transformation of data:

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

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

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

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

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

import java.util.HashMap;

public class TransformAttribute implements Transformation {

    /**
     Description:Abstract method for transforming the attributes

     param hmUserDetails<String,Object>

     HashMap containing parent data details

     param hmEntitlementDetails <String,Object>

     HashMap containing child data details

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

2. Create a JAR file to hold the Java class.
3. Copy the JAR file into the `JavaTasks` or `ScheduleTask` directory.
4. Log in to the Design Console.
5. If you have configured your target system as a target resource, then search for and open one of the following lookup definitions:
 - `Lookup.DBUM.DB2.TargetRecon.Transformation`
 - `Lookup.DBUM.MSSQL.TargetRecon.Transformation`
 - `Lookup.DBUM.Oracle.TargetRecon.Transformation`
 - `Lookup.DBUM.Sybase.TargetRecon.Transformation`
6. If you have configured your target system as a trusted source, then search for and open one of the following lookup definitions:
 - `Lookup.DBUM.DB2.TrustedRecon.Transformation`
 - `Lookup.DBUM.MSSQL.TrustedRecon.Transformation`
 - `Lookup.DBUM.Oracle.TrustedRecon.Transformation`
 - `Lookup.DBUM.Sybase.TrustedRecon.Transformation`
7. In the **Code Key**, enter the resource object attribute name. In the **Decode**, enter the class name that implements the validation logic.
8. Save the changes to the lookup definition.
9. In the scheduled task for your database, set the value of the **Use Validation For Reconciliation** entry to `yes`.
10. Save the changes to the scheduled task.

4.10 Configuring the Connector for Reconciling and Provisioning Object-Level Privileges

Note: Perform the procedure described in this section only if both the conditions are true:

- Your target system is Oracle Database and it has been configured as a target resource.
 - You want configure the connector for provisioning and reconciling object-level privileges.
-

This section provides information about the following topics:

- [Section 4.10.1, "Configuring the Connector for Provisioning Object-Level Privileges"](#)

- [Section 4.10.2, "Configuring the Connector for Reconciling Object-Level Privileges"](#)

4.10.1 Configuring the Connector for Provisioning Object-Level Privileges

To configure the connector for provisioning object-level privileges:

Note: A sample scenario in which you provision object-level privileges for the table database object in Oracle Database has been used to illustrate the procedure.

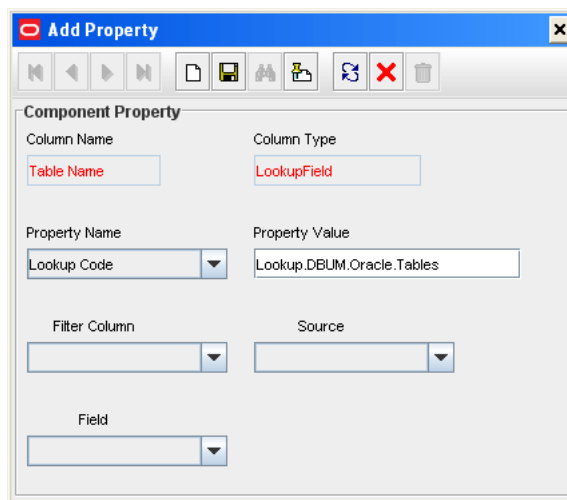
1. Create the Lookup.DBUM.Oracle.Tables and Lookup.DBUM.Oracle.Tables.Privileges lookup definitions for table objects and object privileges, respectively. Note that you do not add any entries to these lookup definitions. The entries in these lookup definitions will be populated after you perform lookup field synchronization.
See [Section 5.6, "Creating Lookup Definitions Used During Connector Operations"](#) for information about creating a lookup definition.
2. Update the properties file that contains queries to perform lookup field synchronization as follows:
 - a. Open the properties file in a text editor.
 - b. Add the following queries for reconciling table objects and table object privileges:
 - Lookup.DBUM.Oracle.Tables = SELECT OBJECT_NAME FROM USER_OBJECTS WHERE OBJECT_TYPE='TABLE'
 - Lookup.DBUM.Oracle.Tables.Privileges = SELECT DISTINCT PRIVILEGE from USR_TAB_PRIVS
3. Run the DBUM Lookup Reconciliation scheduled task to reconcile into the lookup definitions (created in Step 1) existing table objects and table object privileges in Oracle Database.

See [Section 3.3, "Scheduled Task for Lookup Field Synchronization"](#) for more information about the attributes of the DBUM Lookup Reconciliation scheduled task.

4. Create a child form that contains attributes for table object and object privilege as follows:
 - a. Expand **Developement Tools**, and then double-click **Form Designer**.
 - b. In the **Table Name** field, enter UD_DB_ORA_T.
 - c. In the Description field, enter DBUM Manage Object Level Privileges.
 - d. On the Additional Columns tab, click **Add**.
A blank row is displayed in the Additional Columns tab.
 - e. Enter values for the following columns on the blank row that you added:
 - **Name:** UD_DB_ORA_T_TABLE
 - **Variant Type:** String
 - **Length:** 100
 - **Field Label:** Table Name

- **Field Type:** LookupField
- **Order:** 1
- f. Click **Add**.
A blank row is displayed in the Additional Columns tab.
- g. Enter values for the following columns on the blank row that you added:
 - **Name:** UD_DB_ORA_T_PRIVILEGE
 - **Variant Type:** String
 - **Length:** 100
 - **Field Label:** Privilege
 - **Field Type:** LookupField
 - **Order:** 2
- h. Click the Save icon.
- i. On the Properties tab expand **Components**.
- j. Select **Table Name**, and then click **Add Property** to add properties for the Table Name lookup field.
- k. In the Add Property dialog box:
 - From the Property Name list, select **Lookup Code**.
 - In the **Property Value** field, enter `Lookup.DBUM.Oracle.Tables`.
 - Click the Save icon, and then close the dialog box.

The following screenshot shows the Add Property dialog box:



- l. Select **Privilege**, and then click **Add Property** to add properties for the Privilege lookup field.
- m. In the Add Property dialog box:
 - From the Property Name list, select **Lookup Code**.
 - In the **Property Value** field, enter `Lookup.DBUM.Oracle.Tables.Privileges`.
 - Click the Save icon, and then close the dialog box.

5. Assign to the parent form the child table, which is represented by the child form created in the preceding step as follows:
 - a. Expand **Development Tools**, and then double-click **Form Designer**.
 - b. Search for and open the **UD_DB_ORA_P** process form, which is the parent process form.
 - c. Click **Create New Version** to create a version of the form. Then, enter a version name and click the Save icon.
 - d. On the Child Tables(s) tab, click **Assign**.
 - e. In the Assign Child Table(s) dialog box, select the child table **UD_DB_ORA_T**, click the right arrow, and then click OK. The following screenshot shows the Assign Child Table(s) dialog box:
 - f. Click **OK**.
The selected child table is assigned to the form.
 - g. Click **Make Version Active**.
6. Update the Parameter configuration lookup definition by adding lookup entries corresponding to the child attributes as follows:
 - a. Expand **Administration**, and double-click **Lookup Definition**.
 - b. Search for and open the **Lookup.DBUM.Oracle.Parameter.Configuration** lookup definition.
 - c. Click **Add**.
 - d. In the **Code Key** column, enter, for example, `ora_table_privilege`.
 - e. In the **Decode** column, enter (for example)
`UD_DB_ORA_T_PRIVILEGE~varchar2~IN~EXCLUDE_VALIDATION`.
 - f. Click **Add**.
 - g. In the **Code Key** column, enter, for example, `ora_tablename`.
 - h. In the **Decode** column, enter (for example)
`UD_DB_ORA_T_TABLE~varchar2~IN~EXCLUDE_VALIDATION`.

The following screenshot shows the
Lookup.DBUM.Oracle.Parameter.Configuration lookup definition:

Lookup Code Information		
	Code Key	Decode
Add	1 ora_table_privilege	UD_DB_ORA_T_PRIVILEGE~varchar2~IN~EXCLUDE_VALIDATION
Delete	2 ora_tablename	UD_DB_ORA_T_TABLE~varchar2~IN~EXCLUDE_VALIDATION
	3 ora_default_tablespace	UD_DB_ORA_U_TABLESPACE~varchar2~IN~EXCLUDE_VALIDATION
	4 ora_user_id_external	UD_DB_ORA_U_USERNAME~varchar2~IN~DOUBLE_QUOTE~EXCLUDE_V

7. Update the Query configuration lookup definition by adding lookup entries corresponding to the child attributes as follows:
 - a. Expand **Administration**, and double-click **Lookup Definition**.
 - b. Search for and open the **Lookup.DBUM.Oracle.Query.Configuration** lookup definition.
 - c. Click **Add**.
 - d. In the **Code Key** column, enter, for example, `ORA_ADD_TABLE_PRIVILEGE`.

- e. In the **Decode** column, enter (for example) `GRANT :ora_table_privilege ON :ora_tablename TO :ora_user_id_external.`
- f. Click **Add**.
- g. In the **Code Key** column, enter, for example, `ORA_REVOKE_TABLE_PRIVILEGE.`
- h. In the **Decode** column, enter (for example) `REVOKE :ora_table_privilege ON :ora_tablename FROM :ora_user_id_external.`

The following screenshot shows the Lookup.DBUM.Oracle.Query.Configuration lookup definition:

Lookup Code Information		
	Code Key	Decode
Add	1 ORA_ADD_TABLE_PRIVILEGE	GRANT :ora_table_privilege ON :ora_tablename TO :ora_user_id_external
Delete	2 ORA_REVOKE_TABLE_PRIVILEGE	REVOKE :ora_table_privilege ON :ora_tablename FROM :ora_user_id_external
	3 ORA_DELETE_USER	DROP USER :ora_user_id_external CASCADE
	4 ORA_DISABLE_USER	ALTER USER :ora_user_id_external ACCOUNT LOCK

8. Update the Oracle DB User process definition task by adding a process task that is used for granting object-level privileges as follows:
 - a. Expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the **Oracle DB User** process definition.
 - c. On the Tasks tab, click **Add**.
The Creating New Task dialog box is displayed.
 - d. In the **Task Name** field, enter the name of the process task, for example, `Grant object privileges`.
 - e. In the Task Properties section:
 - From the Child Table list, select **UD_DB_ORA_T**.
 - From the Trigger Type list, select **Insert**.
 - f. Click the Save icon, and then close the dialog box.
 - g. On the Tasks tab, double-click the process task that you added.
The Editing Task window is displayed.
 - h. On the Integration tab, click **Add**.
 - i. In the Handler Selection dialog box, to add an adapter to the process task, select the **Adapter** option.
A list of adapters that you can assign to the process task is displayed in the Handler Name region.
 - j. From the list of adapters, select **adpDBUMExecuteQuery**.
 - k. To map the adapter variables listed in this table, select the adapter, click **Map**, and then specify the data given in the following table:

Variable Name	Data Type	Map To	Qualifier	Literal Value
Column Name	String	Literal	String	NA
Adapter Return Value	Object	Response Code	NA	NA
processInstanceKey	Long	Process Data	Process Instance	NA

Variable Name	Data Type	Map To	Qualifier	Literal Value
itResourceColumnName	string	Literal	String	UD_DB_ORA_U_ITRES
lookupCodeKey	String	Literal	String	ORA_ADD_TABLE_PRIVILEGE
value	String	Literal	String	NA
setFlag	String	Literal	String	NA

- I. To add responses listed in this table, on the Responses tab, click **Add**, and then specify the data given in the following table:

Response	Description	Status
INVALID_SQL	Invalid SQL Statement	R
ERROR	Error occurred while performing the operation. Please check the log.	R
INCOMPLETE_LOOKUP_DEFINITION	Incomplete or invalid lookup definition	R
INSUFFICIENT_PRIVILEGE	Insufficient Privilege to execute the query	R
SUCCESS	Object Level Privilege added successfully	C
INVALID_SYNTAX	Incorrect Query format	R
PERMISSION_DENIED	User doesn't have permission to perform this action	R
INVALID_IT_RESOURCE_NAME	Invalid IT Resource name in process task mapping	R
ERROR_UTIL_INIT	Error occurred while initializing parameters	R

9. Update the Oracle DB User process definition task by adding a process task that is used for updating table privileges as follows:
 - a. Expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the **Oracle DB User** process definition.
 - c. On the Tasks tab, click **Add**.
The Creating New Task dialog box is displayed.
 - d. In the **Task Name** field, enter the name of the process task, for example, Update Table Object.
 - e. In the Task Properties section:
 - From the Child Table list, select **UD_DB_ORA_T**.
 - From the Trigger Type list, select **Update**.

The following is a screenshot of the Creating New Task dialog box displaying the Task Properties section:

Creating New Task

Task Name: Update Table Object

Task Description: Updates privileges on table object.

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 ☐

Task Effect: No Effect

Child Table: UD_DB_ORA_T Trigger Type: update

- f. Click the Save icon, and then close the dialog box.
- g. On the Tasks tab, double-click the process task that you added.
The Editing Task dialog box is displayed.
- h. On the Integration tab, click **Add**.
- i. In the Handler Selection dialog box, to add an adapter to the process task, select the **Adapter** option.
A list of adapters that you can assign to the process task is displayed in the Handler Name region.
- j. From the list of adapters, select **adpDBUMExecuteOldDataQuery**.
- k. To map the adapter variables listed in this table, select the adapter, click **Map**, and then specify the data given in the following table:

Variable Name	Data Type	Map To	Qualifier	Literal Value
Column Name	String	Literal	String	NA
Adapter Return Value	Object	Response Code	NA	NA
processInstanceKey	Long	Process Data	Process Instance	NA
itResourceColumnName	string	Literal	String	UD_DB_ORA_U_ITRES
lookupCodeKey	String	Literal	String	ORA_ADD_TABLE_PRIVILEGE
value	String	Literal	String	NA
setFlag	String	Literal	String	NA

- l. To add responses listed in this table, on the Responses tab, click **Add**, and then specify the data given in the following table:

Response	Description	Status
INVALID_SQL	Invalid SQL Statement	R

Response	Description	Status
ERROR	Error occurred while performing the operation. Please check the log.	R
INCOMPLETE_LOOKUP_DEFINITION	Incomplete or invalid lookup definition	R
INSUFFICIENT_PRIVILEGE	Insufficient Privilege to execute the query	R
SUCCESS	Object Level Privilege added successfully	C
INVALID_SYNTAX	Incorrect Query format	R
PERMISSION_DENIED	User doesn't have permission to perform this action	R
INVALID_IT_RESOURCE_NAME	Invalid IT Resource name in process task mapping	R
ERROR_UTIL_INIT	Error occurred while initializing parameters	R

m. To add the task to be generated on receiving the SUCCESS response:

- In the Responses section, select the row with the SUCCESS response.
- In the Tasks To Generate section, click **Assign**.
- In the dialog box that appears, from the left pane, select Grant object privileges, which is the task name created in Step 8.d.
- Click the right arrow and click **OK**.
- Click the Save icon, and then close the form.

10. Update the Oracle DB User process definition task by adding a process task that is used for revoking table privileges by performing the procedure in Step 9.

4.10.2 Configuring the Connector for Reconciling Object-Level Privileges

To configure the connector for reconciling object-level privileges:

Note: A sample scenario in which you reconcile object-level privileges for the table database object in Oracle Database has been used to illustrate the procedure.

1. Add the query that is used to reconcile object-level privileges to the reconciliation query properties file as follows:

- a. Open the properties file in a text editor.
- b. Add the following query for reconciling table objects and table object privileges for a particular user:

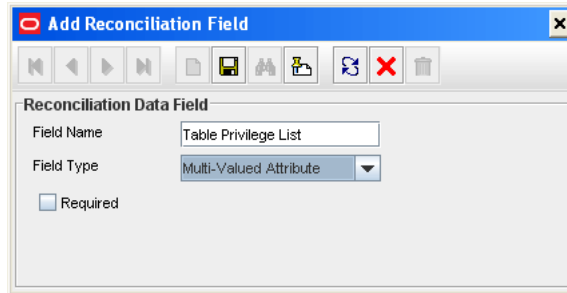
```
ORACLE_TARGET_USER_TABLE_PRIVILEGE=SELECT TABLE_NAME,
PRIVILEGE FROM USER_TAB_PRIVS_MADE WHERE
GRANTEE=:GRANTEE
```

2. In the resource object definition, add a multivalued reconciliation field as follows:

- a. Expand the **Resource Management** folder, and then double-click **Resource Objects**.
- b. Search for and open the **Oracle DB User** resource object.

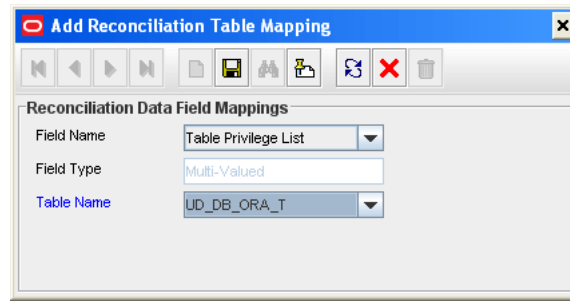
- c. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box.
- d. In the **Field Name** field, enter `Table Privilege List` as the name of the field.
- e. From the **Field Type** list, select **Multi-Valued**.

The following screenshot shows the Add Reconciliation Field dialog box:



- f. Click the Save icon, and then close the dialog box.
- The following screenshot shows the Add Reconciliation Field dialog box:
- g. Right-click the `Table Privilege List` reconciliation field, and then select **Define Property Fields** to open the Add Reconciliation Field dialog box.
 - h. In the **Field Name** field, enter `Table Name`.
 - i. From the **Field Type** list, select **String**.
 - j. Click the Save icon and close the dialog box.
 - k. Right-click the `Table Privilege List` reconciliation field, and then select **Define Property Fields** to open the Add Reconciliation Field dialog box.
 - l. In the **Field Name** field, enter `Privilege`.
 - m. From the **Field Type** list, select **String**.
 - n. Click the Save icon and close the dialog box.
3. Create a reconciliation field mapping for the multivalued attribute as follows:
 - a. Expand the **Process Management** folder, and then double-click **Process Definition**.
 - b. Search for and open the **Oracle DB User** form.
 - c. On the Reconciliation Field Mappings tab of the process definition, click **Add Table Map**.
 - d. In the Add Reconciliation Table Mapping dialog box:
 - From the Field Name list, select **Table Privilege List**.
 - From the Table Name list, select **UD_DB_ORA_T**.

The following is a screenshot of the Add Reconciliation Table Mapping dialog box:



- Click the Save icon and close the dialog box.
- e. Right-click the newly created attribute, Table Privilege List (for example), and then select **Define Property Field Map**.
- f. In the **Field Name** field, select **Table Name**.
- g. Double-click the **Process Data Field** field, and then select **UD_DB_ORA_T_TABLE_NAME**.
- h. Click the save icon and then close the dialog box.
- i. Right-click the newly created attribute, Table Privilege List (for example), and then select **Define Property Field Map**.
- j. In the **Field Name** field, select **Privilege**.
- k. Double-click the **Process Data Field** field, and then select **UD_DB_ORA_T_PRIVILEGE**.
- l. Click the save icon.
- 4. Create a lookup definition that maps fields of the Table Privilege List resource object attribute with the column names used in the reconciliation query (that you added in Step 1.b) as follows:
 - a. Expand the **Administration** folder, and then double-click **Lookup Definition**.
 - b. In the **Code** field, enter `Lookup.DBUM.Oracle.TargetRecon.TablePrivilege.Mapping` as the name of the lookup definition.
 - c. In the **Field** field, enter `DBUM`.
 - d. Select the **Lookup Type** option.
 - e. In the **Group** field, enter `DBUM`.
 - f. Click the Save icon.

The lookup definition is created.

 - g. Add the following entries to this lookup definition by clicking **Add** and specifying values for the Code Key and Decode columns:

Code Key	Decode
Table Name	TABLE_NAME
Privilege	PRIVILEGE

- 5. Create a lookup definition, which contains configurable entries for the multivalued attribute, as follows:

Perform the procedure describes in Step 4 with the following differences:

- While performing Step 4.b, in the **Code** field, enter
`Lookup.DBUM.Oracle.TargetRecon.TablePrivilege.Configuration`.
- While performing Step 4.g, add the following entries to the lookup definition:

Code Key	Decode
Child Attribute Mapping Lookup	Lookup.DBUM.Oracle.TargetRecon.TablePrivilege.Mapping
Child Query Name	ORACLE_TARGET_USER_TABLE_PRIVILEGE
Child Reconciliation Query Filter Lookup	Lookup.DBUM.Oracle.TargetRecon.TablePrivilege.QueryFilter
Parent Attribute	USERNAME

6. Update the `Lookup.DBUM.Oracle.TargetRecon.Mapping` lookup definition by adding a lookup entry corresponding to the multivalued attribute (added to the resource object in Step 2) as follows:
 - a. Expand **Administration**, and double-click **Lookup Definition**.
 - b. Search for and open the `Lookup.DBUM.Oracle.TargetRecon.Mapping` lookup definition.
 - c. Click **Add**.
 - d. In the **Code Key** column, enter `Table Privilege List`.
 - e. In the **Decode** column, enter
`Child~Lookup.DBUM.Oracle.TargetRecon.TablePrivilege.Configuration`.
 - f. Click the Save icon.

4.11 Configuring the Connector for Reconciling and Provisioning Authorization to Oracle Database Vault Realms

Note: Perform the procedure described in this section only if both the conditions are true:

- Your target system is Oracle Database and it has been configured as a target resource.
 - You want configure the connector for provisioning and reconciling authorization to Oracle Database Vault realms.
-

This section provides information about the following topics:

- [Section 4.11.1, "Configuring the Connector for Provisioning Authorization to Oracle Database Vault Realms"](#)
- [Section 4.11.2, "Configuring the Connector for Reconciling Authorization to Oracle Database Vault Realms"](#)

4.11.1 Configuring the Connector for Provisioning Authorization to Oracle Database Vault Realms

To configure the connector for provisioning authorization to Oracle Database Vault realms:

1. Create the Lookup.DBUM.Oracle.DBVault.Realms and Lookup.DBUM.Oracle.DBVault.AuthType lookup definitions for realm name and authorization type, respectively. Note that you do not add any entries to these lookup definitions. The entries in these lookup definitions will be populated after you perform lookup field synchronization.

See [Section 5.6, "Creating Lookup Definitions Used During Connector Operations"](#) for information about creating a lookup definition.

2. Update the properties file that contains queries to perform lookup field synchronization as follows:

- a. Open the properties file in a text editor.

- b. Add the following query for reconciling realm names:

```
Lookup.DBUM.Oracle.DBVault.Realms = SELECT REALM_NAME FROM
FROM DVSYS.DBA_DV_REALM_AUTH
```

3. Run the DBUM Lookup Reconciliation scheduled task to reconcile into the lookup definitions (created in Step 1) names of existing realms in Oracle Database.

See [Section 3.3, "Scheduled Task for Lookup Field Synchronization"](#) for more information about the attributes of the DBUM Lookup Reconciliation scheduled task.

4. Update the Lookup.DBUM.Oracle.DBVault.AuthType lookup definition as follows:

- a. Expand **Administration**, and then double-click **Lookup Definition**.

- b. Search for and open the **Lookup.DBUM.Oracle.DBVault.AuthType** lookup definition.

- c. Add the following entries to this lookup definition by clicking Add and then specifying values for the Code Key and Decode columns:

Code Key	Decode
0	Participant
1	Other

5. Create a child form that contains attributes for realm names and authorization types as follows:

- a. Expand **Development Tools**, and then double-click **Form Designer**.

- b. In the **Table Name** field, enter UD_DB_ORA_V.

- c. In the Description field, enter DBUM Manage DB Vault Authorization.

- d. On the Additional Columns tab, click **Add**.

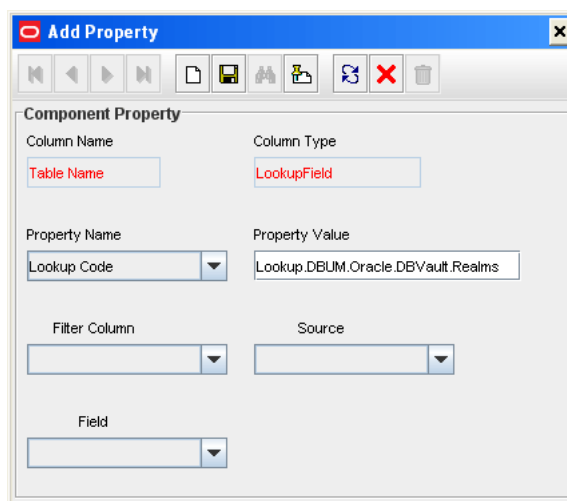
A blank row is displayed in the Additional Columns tab.

- e. Enter values for the following columns on the blank row that you added:

- **Name:** UD_DB_ORA_T_REALM

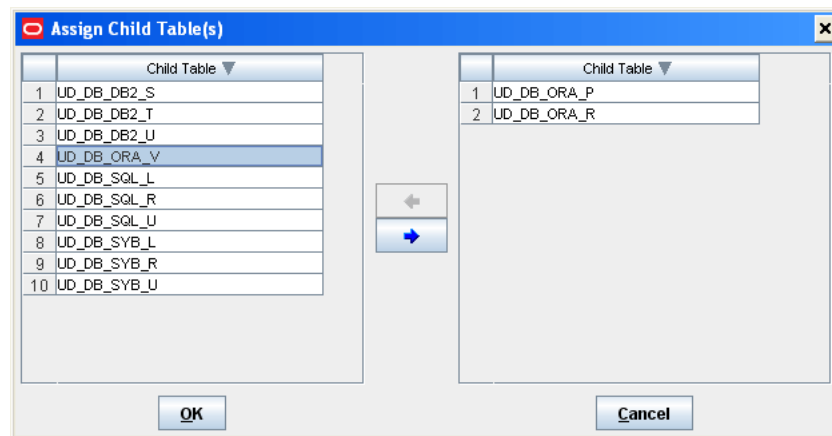
- **Variant Type:** String
 - **Length:** 100
 - **Field Label:** Realm Name
 - **Field Type:** LookupField
 - **Order:** 1
- f. Click **Add**.
- A blank row is displayed in the Additional Columns tab.
- g. Enter values for the following columns on the blank row that you added:
- **Name:** UD_DB_ORA_T_AUTHTYPE
 - **Variant Type:** String
 - **Length:** 100
 - **Field Label:** Authorization Type
 - **Field Type:** LookupField
 - **Order:** 2
- h. Click the Save icon.
- i. On the Properties tab expand **Components**.
- j. Select **Realm Name**, and then click **Add Property** to add properties for the Table Name lookup field.
- k. In the Add Property dialog box:
- From the Property Name list, select **Lookup Code**.
 - In the **Property Value** field, enter `Lookup.DBUM.Oracle.DBVault.Realms`.
 - Click the Save icon, and then close the dialog box.

The following screenshot shows the Add Property dialog box:



- l. Select **Authorization Type**, and then click **Add Property** to add properties for the Privilege lookup field.
- m. In the Add Property dialog box:

- From the Property Name list, select **Lookup Code**.
 - In the **Property Value** field, enter
Lookup.DBUM.Oracle.DBVault.AuthType.
 - Click the Save icon, and then close the dialog box.
6. Assign to the parent form the child table, which is represented by the child form created in the preceding step as follows:
- a. Expand **Development Tools**, and then double-click **Form Designer**.
 - b. Search for and open the **UD_DB_ORA_P** process form, which is the parent process form.
 - c. Click **Create New Version** to create a version of the form. Then, enter a version name and click the Save icon.
 - d. On the Child Tables(s) tab, click **Assign**.
 - e. In the Assign Child Table(s) dialog box, select the child table **UD_DB_ORA_V**, click the right arrow, and then click **OK**. The following screenshot shows the Assign Child Table(s) dialog box:



- f. Click **OK**.
The selected child table is assigned to the form.
 - g. Click **Make Version Active**.
7. Update the Parameter configuration lookup definition by adding lookup entries corresponding to the child attributes as follows:
- a. Expand **Administration**, and double-click **Lookup Definition**.
 - b. Search for and open the **Lookup.DBUM.Oracle.Parameter.Configuration** lookup definition.
 - c. Click **Add**.
 - d. In the **Code Key** column, enter, for example, `realm_name`.
 - e. In the **Decode** column, enter (for example)
`UD_DB_ORA_V_REALM~varchar2~IN~EXCLUDE_VALIDATION`.
 - f. Click **Add**.
 - g. In the **Code Key** column, enter, for example, `auth_options`.

- h. In the **Decode** column, enter (for example)
UD_DB_ORA_V_AUTHTYPE~varchar2~IN~EXCLUDE_VALIDATION.

The following screenshot shows the
Lookup.DBUM.Oracle.Parameter.Configuration lookup definition:

Lookup Code Information		
	Code Key	Decode
Add		
Delete		
	1 ora_default_tablespace	UD_DB_ORA_U_TABLESPACE~varchar2~IN~EXCLUDE_VALIDATION
	2 ora_user_id_external	UD_DB_ORA_U_USERNAME~varchar2~IN~DOUBLE_QUOTE~EXCLUDE_VALIDATION
	3 ora_global_dn	UD_DB_ORA_U_GLOBAL_DN~varchar2~IN~SINGLE_QUOTE
	4 ora_profile	UD_DB_ORA_U_PROFILE~varchar2~IN~EXCLUDE_VALIDATION
	5 ora_temp_tablespace	UD_DB_ORA_U_TEMP_TABLESPACE~varchar2~IN~EXCLUDE_VALIDATION
	6 ora_defaults_quota_size	UD_DB_ORA_U_QUOTASIZE~varchar2~IN
	7 ora_tempts_quota_size	UD_DB_ORA_U_TEMP_QUOTASIZE~varchar2~IN
	8 ora_privilege_admin_option	UD_DB_ORA_P_ADMIN_OPTION~varchar2~IN~EXCLUDE_VALIDATION
	9 ora_role_admin_option	UD_DB_ORA_R_ADMIN_OPTION~varchar2~IN~EXCLUDE_VALIDATION
	10 ora_role_name	UD_DB_ORA_R_ROLE~varchar2~IN~EXCLUDE_VALIDATION
	11 ora_user_id	UD_DB_ORA_U_USERNAME~varchar2~IN
	12 ora_password	UD_DB_ORA_U_PASSWORD~varchar2~IN
	13 ora_privilege_name	UD_DB_ORA_P_PRIVILEGE~varchar2~IN~EXCLUDE_VALIDATION
	14 realm_name	UD_DB_ORA_V_REALM_NAME~varchar2~IN~EXCLUDE_VALIDATION
	15 auth_options	UD_DB_ORA_V_AUTH_TYPE~number~IN~EXCLUDE_VALIDATION

8. Update the Query configuration lookup definition by adding lookup entries corresponding to the child attributes as follows:
- Expand **Administration**, and double-click **Lookup Definition**.
 - Search for and open the **Lookup.DBUM.Oracle.Query.Configuration** lookup definition.
 - Click **Add**.
 - In the **Code Key** column, enter, for example,
ORA_ADD_DBVAULT_AUTHORIZATION.
 - In the **Decode** column, enter (for example) {CALL
DVSYS.DBMS_MACADM.ADD_AUTH_TO_REALM(:realm_name,:ora_user_
id_external,:auth_options)}.
 - Click **Add**.
 - In the **Code Key** column, enter, for example,
ORA_REVOKE_DBVAULT_AUTHORIZATION.
 - In the **Decode** column, enter (for example) {CALL
DVSYS.DBMS_MACADM.DELETE_AUTH_FROM_REALM(:realm_name,:ora_
user_id)}.

The following screenshot shows the
Lookup.DBUM.Oracle.Query.Configuration lookup definition:

Lookup Code Information		
	Code Key	Decode
Add		
Delete		
	1 ADD_REALM_AUTHORIZATION	{CALL DVSYS.DBMS_MACADM.ADD_AUTH_TO_REALM(:realm_name,:ora_user_id,:auth_options)}
	2 DEFAULTTS_QUOTA_QUERY	QUOTA :ora_defaults_quota_size ON :ora_default_tablespace
	3 ORA_ADD_PRIVILEGE	GRANT :ora_privilege_name TO :ora_user_id_external~PRIVILEGE_WITH_ADMIN_OPTION
	4 ORA_ADD_ROLE	GRANT :ora_role_name TO :ora_user_id_external~ROLE_WITH_ADMIN_OPTION
	5 ORA_CREATE_EXTERNAL_USER	CREATE USER :ora_user_id_external IDENTIFIED EXTERNALLY ACCOUNT UNLOCK~TABLESPACE_QI

9. Update the Oracle DB User process definition task by adding a process task that is used for updating authorization to Oracle Database Vault realms as follows:
- Expand **Process Management**, and then double-click **Process Definition**.
 - Search for and open the **Oracle DB User** process definition.
 - On the **Tasks** tab, click **Add**.

The Creating New Task dialog box is displayed.

- d. In the **Task Name** field, enter the name of the process task, for example, `Grant DBVault Authorization`.
- e. In the Task Properties section:
 - From the Child Table list, select **UD_DB_ORA_V**.
 - From the Trigger Type list, select **Insert**.
- f. Click the Save icon, and then close the dialog box.
- g. On the Tasks tab, double-click the process task that you added.
The Editing Task window is displayed.
- h. On the Integration tab, click **Add**.
- i. In the Handler Selection dialog box, to add an adapter to the process task, select the **Adapter** option.
A list of adapters that you can assign to the process task is displayed in the Handler Name region.
- j. From the list of adapters, select **adpDBUMExecuteStoredProc**.
- k. To map the adapter variables listed in this table, select the adapter, click **Map**, and then specify the data given in the following table:

Variable Name	Data Type	Map To	Qualifier	Literal Value
Column Name	String	Literal	String	NA
Adapter Return Value	Object	Response Code	NA	NA
processInstanceKey	Long	Process Data	Process Instance	NA
itResourceColumnName	string	Literal	String	UD_DB_ORA_U_ITRES
lookupCodeKey	String	Literal	String	ORA_REVOKE_DBVAULT_AUTHORIZATION
value	String	Literal	String	NA
setFlag	String	Literal	String	NA

- l. To add responses listed in this table, on the Responses tab, click **Add**, and then specify the data given in the following table:

Response	Description	Status
INVALID_SQL	Invalid SQL Statement	R
ERROR	Error occurred while performing the operation. Please check the log.	R
INCOMPLETE_LOOKUP_DEFINITION	Incomplete or invalid lookup definition	R
INSUFFICIENT_PRIVILEGE	Insufficient Privilege to execute the query	R
SUCCESS	Object Level Privilege added successfully	C
INVALID_SYNTAX	Incorrect Query format	R
PERMISSION_DENIED	User doesn't have permission to perform this action	R

Response	Description	Status
INVALID_IT_RESOURCE_NAME	Invalid IT Resource name in process task mapping	R
ERROR_UTIL_INIT	Error occurred while initializing parameters	R

- m. To add the task to be generated on receiving the SUCCESS response:
 - In the Responses section, select the row with the SUCCESS response.
 - In the Tasks To Generate section, click **Assign**.
 - In the dialog box that appears, from the left pane, select Grant DBVault Authorization, which is the task name created in Step 9.d.
 - Click the right arrow and click **OK**.
 - Click the Save icon, and then close the form.
10. Update the Oracle DB User process definition task by adding a process task that is used for revoking authorization to Oracle Database Vault realms by performing the procedure in Step 9.a to 9.l.

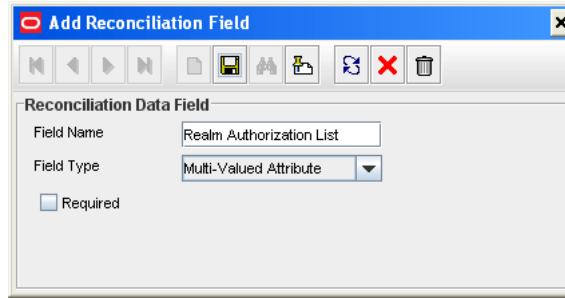
4.11.2 Configuring the Connector for Reconciling Authorization to Oracle Database Vault Realms

To configure the connector for reconciling authorization to Oracle Database Vault realms:

1. Add the query that is used to reconcile authorization to Oracle Database Vault realms to the reconciliation query properties file as follows:
 - a. Open the properties file in a text editor.
 - b. Add the following query for reconciling authorization to Oracle Database Vault realms for a particular user:


```
ORACLE_TARGET_USER_DBVAULT_AUTHORIZATION = SELECT
REALM_NAME,AUTH_OPTIONS FROM DVSYS.DBA_DV_REALM_AUTH
WHERE GRANTEE = :USERNAME
```
2. In the resource object definition, add a multivalued reconciliation field as follows:
 - a. Expand the **Resource Management** folder, and then double-click **Resource Objects**.
 - b. Search for and open the **Oracle DB User** resource object.
 - c. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box.
 - d. In the **Field Name** field, enter Realm Authorization List as the name of the field.
 - e. From the **Field Type** list, select **Multi-Valued**.

The following screenshot shows the Add Reconciliation Field dialog box:



- f. Click the Save icon, and then close the dialog box.
- The following screenshot shows the Add Reconciliation Field dialog box:
- g. Right-click the DBVault Authorization reconciliation field, and then select **Define Property Fields** to open the Add Reconciliation Field dialog box.
- h. In the **Field Name** field, enter `Realm Name`.
- i. From the **Field Type** list, select **String**.
- j. Click the Save icon and close the dialog box.
- k. Right-click the DBVault Authorization reconciliation field, and then select **Define Property Fields** to open the Add Reconciliation Field dialog box.
- l. In the **Field Name** field, enter `Authorization Type`.
- m. From the **Field Type** list, select **String**.
- n. Click the Save icon and close the dialog box.
3. Create a reconciliation field mapping for the multivalued attribute as follows:
 - a. Expand the **Process Management** folder, and then double-click **Process Definition**.
 - b. Search for and open the **Oracle DB User** form.
 - c. On the Reconciliation Field Mappings tab of the process definition, click **Add Table Map**.
 - d. In the Add Reconciliation Table Mapping dialog box:
 - From the Field Name list, select **DBVault Authorization**.
 - From the Table Name list, select **UD_DB_ORA_V**.
 - Click the Save icon and close the dialog box.
 - e. Right-click the newly created attribute, DBVault Authorization (for example), and then select **Define Property Field Map**.
 - f. In the **Field Name** field, select **Realm Name**.
 - g. Double-click the **Process Data Field** field, and then select **UD_DB_ORA_V_REALM**.
 - h. Click the save icon and then close the dialog box.
 - i. Right-click the newly created attribute, DBVault Authorization (for example), and then select **Define Property Field Map**.
 - j. In the **Field Name** field, select **Authorization Type**.
 - k. Double-click the **Process Data Field** field, and then select **UD_DB_ORA_V_AUTHTYPE**.

- l. Click the save icon.
4. Create a lookup definition that maps fields of the DBVault Authorization resource object attribute with the column names used in the reconciliation query (that you added in Step 1.b) as follows:
 - a. Expand the **Administration** folder, and then double-click **Lookup Definition**.
 - b. In the **Code** field, enter `Lookup.DBUM.Oracle.TargetRecon.DBVault.Mapping` as the name of the lookup definition.
 - c. In the **Field** field, enter `DBUM`.
 - d. Select the **Lookup Type** option.
 - e. In the **Group** field, enter `DBUM`.
 - f. Click the Save icon.
The lookup definition is created.
 - g. Add the following entries to this lookup definition by clicking **Add** and specifying values for the Code Key and Decode columns:

Code Key	Decode
Realm Name	REALM_NAME
Authorization Type	AUTH_OPTIONS

5. Create a lookup definition, which contains configurable entries for the multivalued attribute, as follows:
Perform the procedure describes in Step 4 with the following differences:
 - While performing Step 4.b, in the **Code** field, enter `Lookup.DBUM.Oracle.TargetRecon.DBVault.Configuration`.
 - While performing Step 4.g, add the following entries to the lookup definition:

Code Key	Decode
Child Attribute Mapping Lookup	<code>Lookup.DBUM.Oracle.TargetRecon.DBVault.Mapping</code>
Child Query Name	<code>ORACLE_TARGET_USER_DBVAULT_AUTHORIZATION</code>
Child Reconciliation Query Filter Lookup	<code>Lookup.DBUM.Oracle.TargetRecon.DBVault.QueryFilter</code>
Parent Attribute	<code>USERNAME</code>

6. Update the `Lookup.DBUM.Oracle.TargetRecon.Mapping` lookup definition by adding a lookup entry corresponding to the multivalued attribute (added to the resource object in Step 2) as follows:
 - a. Expand **Administration**, and double-click **Lookup Definition**.
 - b. Search for and open the **Lookup.DBUM.Oracle.TargetRecon.Mapping** lookup definition.
 - c. Click **Add**.
 - d. In the **Code Key** column, enter `DBVAult Authorization`.

- e. In the **Decode** column, enter
`Child~Lookup.DBUM.Oracle.TargetRecon.DBVault.Configuration`
.
- f. Click the Save icon.

Configuring the Connector for a JDBC-Based Database

The Database User Management connector is built on a framework designed for JDBC-based connectors. If your target system is a JDBC-based database other than the certified databases listed in [Table 1-1](#), then you can create a connector for your target system by following the instructions given in this chapter.

Note: In this chapter, MySQL has been used as the sample JDBC-based database to explain the procedures.

The following sections describe the procedure to deploy the connector and create each object of the connector:

- [Section 5.1, "Deploying the Connector"](#)
- [Section 5.2, "Creating an IT Resource for Your Database"](#)
- [Section 5.3, "Creating a Resource Object"](#)
- [Section 5.4, "Creating a Process Form"](#)
- [Section 5.5, "Adding Attributes for Provisioning"](#)
- [Section 5.6, "Creating Lookup Definitions Used During Connector Operations"](#)
- [Section 5.7, "Creating a Process Definition"](#)
- [Section 5.8, "Adding Process Tasks, Assigning Adapters, and Mapping Adapter Variables"](#)
- [Section 5.9, "Adding Attributes for Reconciliation"](#)
- [Section 5.10, "Guidelines on Creating or Configuring Queries Used for Reconciliation and Lookup Synchronization"](#)
- [Section 5.11, "Creating Scheduled Tasks"](#)
- [Section 5.12, "Configuring Status Reconciliation"](#)

5.1 Deploying the Connector

You must deploy the Database User Management connector before you can customize it for a JDBC-based database.

Copy the MySQL database driver JAR into the *OIM_HOME/xellerate/ThirdParty* directory.

In addition, perform the procedure specified in the following sections for deploying the connector:

- [Section 2.1.1, "Preinstallation on Oracle Identity Manager"](#)
- [Section 2.2, "Installation"](#)

5.2 Creating an IT Resource for Your Database

The IT resource holds connection-related information about the target system. The DBUM ITResource IT resource type is the template from which IT resources are created for target systems of this connector. You must create an IT resource of the IT resource type, definition, which is a template for all IT resources associated with this connector.

To create an IT resource:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Create IT Resource**.
4. On the Step 1: Provide IT Resource Information page, enter the following information:
 - **IT Resource Name:** Enter a name for the IT resource. For example, MySQL.
 - **IT Resource Type:** Select the **DBUM ITResource definition** IT resource type for the IT resource.
5. Click **Continue**.
6. On the Step 2: Specify IT Resource Parameter Values page, specify values for the parameters of the IT resource. [Table 2–7](#) describes each parameter.

The following are sample parameter values:

Admin ID: User ID of the MySQL user with privileges to perform connector operations.

Sample value: root

Admin Password: Password for the user specified by the Admin ID parameter

Database Driver: Database drivers used to connect to MySQL

Sample value: com.mysql.jdbc.Driver

JDBC URL: Sample Value: jdbc:mysql://localhost/dbum

Configuration Lookup: Name of the lookup definition in which you store MySQL connector configuration information

Sample Value: Lookup.DBUM.MySQL.Configuration

7. Click **Continue**.

The Step 3: Set Access Permission to IT Resource page is displayed. On this 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.

8. On the Step 3: Set Access Permission to IT Resource page, 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**.

9. 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: 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**.

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

Note: 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**.

11. Click **Continue**.

12. 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.

13. To proceed with the creation of the IT resource, click **Continue**.

14. 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 **Create**. 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.
- Proceed with the creation process by clicking **Continue**. You can fix the problem later, and then rerun the connectivity test by using the Diagnostic Dashboard.

Note: If no errors are encountered, then the label of the button is **Create**, not **Continue**.

15. Click **Finish**.

5.3 Creating a Resource Object

You must create a resource object for your target system database. A resource object is a virtual representation of your target system.

To create a resource object:

1. Log in to the Design Console.
2. Expand **Resource Management**, and then double-click **Resource Objects**.
3. In the **Name** field, enter the name of the resource object. For example, enter `MySQL`.
4. If required, you can attach a resource form to the resource object. To do this, double-click the **Table Name** lookup field. From the Lookup dialog box, select the table that represents the form that will be associated with the resource object.
5. To request the resource object for a user, select **Order For User**.
6. If you want to associate a custom form with the provisioning process of the resource object, this form contains fields that have prepopulate adapters attached to them, and you want these fields to be populated automatically by Oracle Identity Manager, select the **Auto Pre-Populate** option.

Note: If the resource object has no custom form associated with it, or this form's fields have no prepopulate adapters attached to them, deselect the **Auto Pre-Populate** check box. For more information about prepopulate adapters, see *Oracle Identity Manager Tools Reference*.

7. Double-click the **Type** lookup field.
From the Lookup dialog box that is displayed, select the classification status **Application** to associate with the resource object.
8. If you want multiple instances of the resource object to be requested for a user or an organization, select the **Allow Multiple** option. Otherwise, go to Step 9.
9. If you want to be able to request the resource object for yourself, select the **Self Request Allowed** option.
10. To provision the resource object for all users, regardless of whether the organization to which the user belongs has the resource object assigned to it, select the **Allow All** check box.
11. To automatically initiate the provisioning process when the resource object's approval process has achieved a status of **Completed**, select the **Auto Launch** option.

Caution: By default, Oracle Identity Manager sets all resource objects to Auto Launch, even though this check box is not selected.

12. Click **Save**.

The resource object is created.

5.4 Creating a Process Form

All target system fields to which Oracle Identity Manager writes data during a provisioning operation are defined in a process form. In addition, the fields defined in the process form appear on the page (in the Administrative and User Console) that is used for provisioning a target system resource to an OIM User.

To create a process form:

Note: The procedure for creating child forms is similar to the process described here.

1. Log in to the Design Console.
2. Expand **Development Tools**, and then double-click **Form Designer**.
3. In the **Table Name** field, enter the name of the database table that is associated with the form.

Note: The table name contains the **UD_** prefix followed by the form name. If the name of the form is **DB_MYS_U**, its table name is **UD_DB_MYS_U**.

4. In the **Description** field, enter explanatory information about the form. For example, enter **DBUM Provisioning form for MySQL User**.
5. If the form is assigned to an approval or provisioning process, then select the **Process** option.
6. Click **Save**.

The form is created. The words **Initial Version** are displayed in the **Latest Version** field. This signifies that you can populate the tabs of the Form Designer form with information, so the form is functional with its assigned process or resource.

5.5 Adding Attributes for Provisioning

After you create the process form, you must add the target system fields to which Oracle Identity Manager writes data during a provisioning operation.

To add a target system fields to the process form:

Note: You must add to the process must a field for IT resource.

1. Expand the **Development Tools** folder, and then double-click **Form Designer**.
2. Search for and open the process form that you created in [Section 5.4, "Creating a Process Form."](#)
3. On the Additional Columns tab, click **Add**.
A blank row is displayed in the Additional Columns tab.
4. In the **Name** field, enter the name of the data field, which is displayed in the database, and is recognized by Oracle Identity Manager.

Note: This name consists of the <TABLENAME_> prefix, followed by the name of the data field.

For example, if the name that is displayed in the **Table Name** field is **UD_DB_MYS_U**, and the name for the data field is **USERNAME**, the data field name that is displayed in the database and Oracle Identity Manager recognizes, would be **UD_DB_MYS_U_USERNAME**.

5. Double-click the **Variant Type** lookup field.
From the Lookup window that is displayed, select the variant type for the data field.
6. In the **Length** field, enter the length (in characters) of the data field.
7. In the **Field Label** field, enter the label that will be associated with the data field.
This label is displayed next to the data field on the form that is generated by Oracle Identity Manager.
8. Double-click the **Field Type** lookup field.
From the Lookup dialog box that is displayed, select the data type for the data field.
9. In the **Default Value** field, enter the value that is displayed in the associated data field once the form is generated, and if no other default value has been specified.
10. In the **Order** field, enter the sequence number, which will represent where the data field will be positioned on the generated form.
For example, a data field with an order number of 2 is displayed below a data field with an order number of 1.
11. If you want a specific organization or user's values to supersede the value that is displayed in the **Default Value** field, select the **Application Profile** check box. Otherwise, go to Step 10.
12. If you want the information that is displayed in the data field to be encrypted when it is transmitted between the client and the server, then select the **Encrypted** check box. Otherwise, go to Step 11.
13. Click **Save**.
14. Repeat Steps 1 through 11 for each target system attribute that you want to add.
15. Activate the form by clicking **Make Version Active**.

5.6 Creating Lookup Definitions Used During Connector Operations

In Oracle Identity Manager, you must create lookup definitions of the following types that will be used during connector operations:

- Lookup definitions corresponding to lookup fields on the target system
- Lookup definitions that store configuration and other generic information

To create a lookup definition:

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

3. In the **Code** field, enter the name of the lookup definition. The lookup definitions that you must create are listed later in this section.
4. If the lookup definition is to represent a lookup field or box, select the **Lookup Type** option.
5. In the **Group** field, enter DBUM.
6. Click **Save**.

The lookup definition is created.

By performing the procedure described in this section, you must create the following lookup definitions:

See Also: [Appendix A, "Preconfigured Lookup Definitions"](#) for information about lookup definitions and their entries

- Lookup.DBUM.MySQL.Configuration
- Lookup.DBUM.MySQL.Error.Mapping
- Lookup.DBUM.MySQL.ExclusionList
- Lookup.DBUM.MySQL.Parameter.Configuration
- Lookup.DBUM.MySQL.Provisioning.Validation
- Lookup.DBUM.MySQL.Query.Configuration
- Lookup.DBUM.MySQL.TargetRecon.Delete.Mapping
- Lookup.DBUM.MySQL.TargetRecon.Mapping
- Lookup.DBUM.MySQL.TargetRecon.QueryFilter
- Lookup.DBUM.MySQL.TargetRecon.CHILD_DATA.Configuration
- Lookup.DBUM.MySQL.TargetRecon.CHILD_DATA.Mapping
- Lookup.DBUM.MySQL.TargetRecon.CHILD_DATA.QueryFilter
- Lookup.DBUM.MySQL.TargetRecon.Transformation
- Lookup.DBUM.MySQL.TargetRecon.Validation
- Lookup.DBUM.TargetRecon.StatusMapping

If you want to reconcile multivalued attributes, then in addition to the preceding lookup definitions, you must create the following lookup definitions:

- Lookup.DBUM.MySQL.TargetRecon.CHILD_DATA.Configuration
- Lookup.DBUM.MySQL.TargetRecon.CHILD_DATA.Mapping
- Lookup.DBUM.MySQL.TargetRecon.CHILD_DATA.QueryFilter

If your target system treats the Login and User database access entities as parent and child elements (respectively), then you have to create lookup definitions similar to the following:

Note: For MySQL, you need not create these lookup definitions.

- Lookup.DBUM.MSSQL.AuthType
- Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateLogin

- Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateUser
- Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteLogin
- Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteUser
- Lookup.DBUM.MSSQL.AuthType.KeyMapping.DisableLogin
- Lookup.DBUM.MSSQL.AuthType.KeyMapping.EnableLogin

5.7 Creating a Process Definition

You must create a process definition for the provisioning process. Each process definition consists of one or more process tasks. A process task performs a specific function during a provisioning operation. For example, you can create a process definition that consists of three process tasks, one each for the create user, modify user, and delete user operations.

To create a process definition:

1. Log in to the Design Console.
2. Expand **Process Management**, and then double-click **Process Definition**.
3. In the **Name** field, enter the name of the process definition. For example, enter MySQL DB User.

4. Double-click the **Type** lookup field.

5. From the Lookup dialog box that is displayed, select **Provisioning** as the classification type of the process definition.

6. Double-click the **Object Name** lookup field.

From the Lookup dialog box that is displayed, select the resource object (that you had created in [Section 5.3, "Creating a Resource Object"](#)) that will be associated with the process definition.

7. Select the **Default Process** check box to make this the default provisioning process for the resource object to which it is assigned.
8. Select the **Auto Pre-Populate** check box to enable Oracle Identity Manager to automatically populate the fields in this process form with prepopulate adapters.
9. Double-click the **Table Name** lookup field.

From the Lookup window that is displayed, select the table that represents the form (created in [Section 5.4](#)) associated with the process definition.

10. Click **Save**.

The process definition is created.

5.8 Adding Process Tasks, Assigning Adapters, and Mapping Adapter Variables

As mentioned in the preceding section, process tasks perform specific functions during a provisioning operation. You can add process tasks for functions such as the following:

- Create user
- Update user
- Disable user

- Enable user
- Delete user

The actual logic for implementing the functions in the preceding list is defined in adapters. The Database User Management connector is shipped with the following adapters listed in [Table 5–1](#).

Table 5–1 Adapters Used During Provisioning Operations

Adapter	Description
adpDBUMExecuteQuery	Use this adapter if your target system uses DDL statements for maintaining the system catalog. This adapter executes the SQL queries defined in the Query Configuration lookup definition.
adpDBUMExecuteStoredProcedure	Use this adapter if your target system database uses stored procedures for maintaining the system catalog. This adapter executes the stored procedures defined in the Query Configuration lookup definition.
adpDBUMExecuteQueryForAuthTypeUser	Use this adapter if you must run SQL queries for users or logins depending on the authentication type.
adpDBUMExecuteStoredProcAuthTypeUser	Uses this adapter if you must run stored procedures for users or logins depending on the authentication type.
adpDBUMPreventFunctionality	Use this adapter to restrict specific provisioning operations such as updating a field, enabling a target system record, and disabling a target system record. This adapter displays the following message when an attempt to update the particular field is made: This functionality is not supported.
adp DBUM Prepopulate UserLogin	Use this adapter to populate the Login Name or User Name fields with a value that was specified earlier in the UserLogin field of the OIM User form.
adp DBUM Prepopulate UserFullName	Use this adapter to populate the Full Name field with a value that was specified earlier in the FirstName, MiddleName, and LastName fields of OIM User form.
adp DBUMExecuteOldDataStoreProc	Use this adapter to retrieve the old value of a particular field. Depending on the value retrieved, the corresponding provisioning operation is performed by running stored procedures for updating child data and password.
adp DBUMExecuteOldDataQuery	Use this adapter to retrieve the old value of a particular field. Depending on value retrieved, the corresponding provisioning operation is performed by running SQL statements for updating child data and password.
adpDBUMUserNotExist	This adapter is used to check whether the user record being created exists on the target system. If such a user is found, then the USER_EXISTS message is displayed on the Administrative and User Console.

All the adapters listed in [Table 5–1](#) use some or all of the variables listed in [Table 5–2](#). Depending on the variable mapping that you create for each adapter, the corresponding task is run.

Table 5–2 Adapter Variables

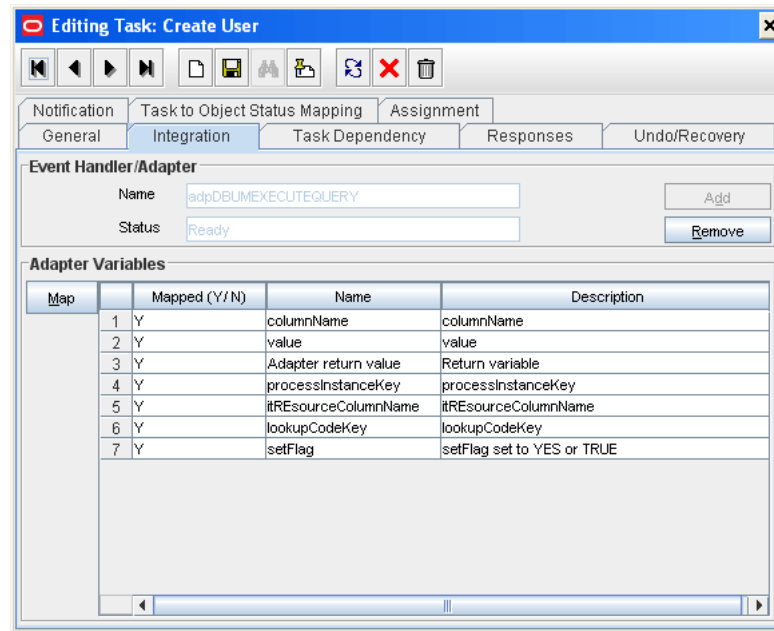
Variable Name	Description
setFlag	You can set the value of this variable to YES or TRUE. This is used to set process form data after success of corresponding provisioning operation.
columnName	Specify the column name for which you want to set data. For example, if you are using Oracle Database as the target system and you want to set value for the Account Status field on the Administrative and User Console, then you must specify the UD_DB_ORA_U_LOCK field on the process form as the value of this variable.
value	Set the value to be displayed when a user is disabled. For example, set the value to LOCKED.
action	This variable is used to perform specific operations. For example, you can set the value of the action variable to CREATEUSER, UPDATEUSER, ENABLELOGIN, or DISABLELOGIN.
itResourceColumnName	Provide the name of the field on the process form that holds the IT resource value.
authenticationType	It maps with process form authentication field in the process task to get the value of authentication type at run time.
processInstanceKey	It maps with process instance key in the process task to retrieve the process instance key at run time.
lookupCodeKey	Specify the query code key from the query configuration lookup corresponding to the specific operation.
childColumnName	Specify the process form field name to retrieve the old value of this field.
childFieldValue	Map this variable with the field specified above in process task and check old check box to retrieve old value of this field.

In order to run a process task successfully, you must assign an adapter to it. The following is the procedure to add a process task, assign an adapter to the process task, and then map adapter variables:

1. Expand **Process Management**, and then double-click **Process Definition**.
2. Search for and open the process definition task that you created in [Section 5.7, "Creating a Process Definition."](#)
3. To add a process task to the process definition:
 - a. On the **Tasks** tab, click **Add**.
The Creating New Task dialog box is displayed.
 - b. In the **Task Name** field, enter the name of the process task. For example, enter `Create User`.
 - c. In the **Task Description** field, enter descriptive information about the task.
 - d. From the Toolbar of the Creating New Task window, click **Save**. Then, click **Close**.
The process task is added to the process definition.
 - e. Repeat steps 3.a through 3.c for every process task that you want to create.
4. To assign an adapter to the process task:

- a. Double-click the row heading of the process task to which you want to assign an event handler or adapter.

The Editing Task dialog box is displayed. The following screenshot displays this dialog box after attaching the adapter and mapping adapter variables:

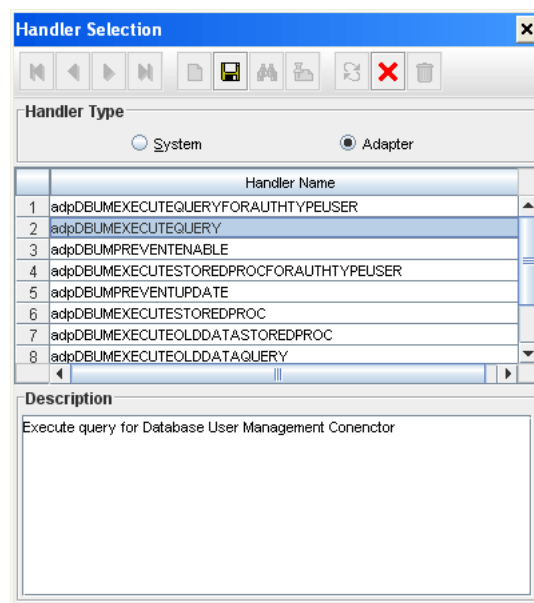


- b. On the **Integration** tab, click **Add**.

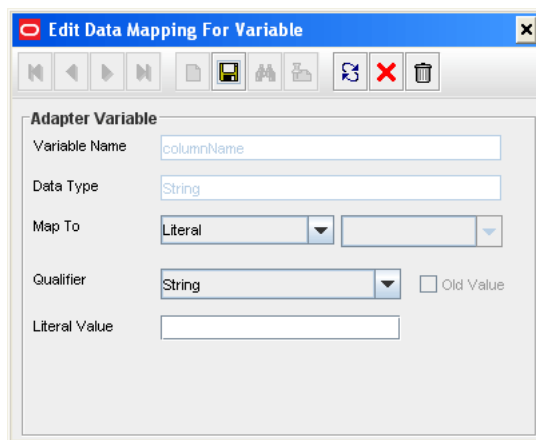
The Handler Selection dialog box is displayed [Figure 5-1](#).

- c. To add an adapter to the process task, select the **Adapter** option. A list of adapters, which you can assign to the process task, is displayed in the **Handler Name** region.

Figure 5-1 Handler Selection Dialog Box



- d. Select the adapter that you want to assign to the process task.
 - e. From the Handler Selection window's Toolbar, click **Save**.
A confirmation dialog box is displayed.
 - f. Click **OK**.
The adapter is assigned to the process task.
5. Depending on your requirement, add adapter variables as follows:
- a. Select the adapter variable that you want to map.
 - b. Click **Map**.
The Data Mapping for Variable dialog box is displayed.
 - c. For MySQL, there are no read-only fields for setting additional data. Map the columnName, value, and setFlag adapter variables to blank literals. The following screenshot displays the Edit Data Mapping For Variable dialog box in which the columnName adapter variable has been mapped to a blank literal:



Similarly, map the following adapter variables:

Adapter Return Value: Response Code.

processInstancekey: Select **Process Data**, and then select **Process Instance**.

itResourcecolumnName: From the Map To list, select **Literal**, from the Qualifier list select **String**, and then in the Literal Value field, enter the value of IT Resource column Name created on the process form.

Sample value: UD_DB_MYS_U_IT_RESOURCE

lookupCodeKey: Map to Literal, select **String**, and then enter the value of the code key from the Lookup.DBUM.MySQL.Query.Configuration.

Sample Value: MYSQL_CREATE_USER

- d. In the Data Mapping for Variable dialog box, click **Save**.
- e. Click **Close**.

The mapping status for the adapter variable changes from N to Y. This indicates that the adapter variable has been mapped.

5.9 Adding Attributes for Reconciliation

After you create the resource object, you must define the attributes on the target resources that must be used for reconciliation. In addition, you must also map these attributes to the corresponding fields on Oracle Identity Manager. Note that the attributes that you add to the resource object are mapped for reconciliation between Oracle Identity Manager and the target system.

See [Section 4.2, "Adding or Removing Attributes for Reconciliation"](#) for information about adding attributes for reconciliation.

5.10 Guidelines on Creating or Configuring Queries Used for Reconciliation and Lookup Synchronization

See [Section 4.1, "Guidelines on Extending the Functionality of the Connector"](#) for guidelines on creating or configuring queries used for reconciliation and lookup synchronization.

5.11 Creating Scheduled Tasks

You need scheduled tasks for the following reasons:

- For synchronizing lookup field values with the target system
- For fetching data from the target system for reconciliation with Oracle Identity Manager

You need not create scheduled tasks for lookup field synchronization. Instead, you can use the DBUM Lookup reconciliation scheduled task that is shipped with this connector. See [Section 3.3, "Scheduled Task for Lookup Field Synchronization"](#) for more information about this scheduled task.

Depending on your requirements, you must create one or more of the following scheduled tasks, to fetch user records from target system during reconciliation:

- Scheduled task for reconciliation of user records from a target system that is configured as a target resource
- Scheduled task for reconciliation of user records that have been deleted from a target system that is configured as a target resource.

For each of the items listed in the preceding list, perform the following procedure to create a scheduled task:

1. Expand **Resource Management**.
2. Click **Create Scheduled Task**.
3. On the Step 1: Provide Scheduled Task Details and Schedule page, enter the following information:
 - **Task Name:** Enter a name for the scheduled task.
Sample Value: DBUM MySQL Target Resource User Reconciliation
 - **Class Name:** Specify the Java class for running the scheduled task. To do this, click the magnifying glass icon to open the **Class Name** list of values and then select a class. Alternatively, enter the class name.
Sample Value: oracle.iam.connectors.dbum.tasks.DBUMReconTask

- **Status:** Specify whether or not you want to leave the task in the enabled state after it is created. In the enabled state, the task is ready for use. If the task is disabled, then you must enable it before you can use it. The default value is INACTIVE.
 - **Max Retries:** Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 1.
 - **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.
 - **Frequency:** Specify the frequency at which you want the task to run. The default value is Once.
4. Click **Continue**.
 5. On the Step 2: Define Scheduled Task Attributes page, create attributes for the task as follows. Table 3–2 lists the scheduled task attributes that you must create for reconciling user records from a target resource. Table 3–3 lists the scheduled task attributes that you must create for reconciling data about deleted target system user records from a target resource.
 - a. In the **Attribute** field, enter the name of the attribute.
 - b. In the **With** field, enter the value of the attribute.
 - c. Click **Add**.
 - d. Repeat Steps 5.a through 5.c for each attribute that you want to add.

Note: Each attribute that you add is displayed in a table. The attributes you add are not posted to the Oracle Identity Manager database until you complete the procedure to create the scheduled task. If required, you can modify the value of a newly added attribute by selecting it from the **Attribute** list, and then editing its value. To delete an attribute, click the cross-shaped icon displayed for that attribute.

6. Click **Continue**.
7. On the Step 3: Verify Scheduled Task Details page, review the information that you provided on the first and second pages. If you want to make changes in this information, click **Back** to revisit the first or second page and then make the required changes.
8. To proceed with the creation of the scheduled task, click **Continue**.
9. If the creation process is successful, then a message stating that the scheduled task has been created is displayed.

5.12 Configuring Status Reconciliation

If your target system database contains a column that holds the status of the user account, then you can perform status reconciliation by setting a value for the Status Reconciliation Primary Key Field attribute of the scheduled task.

If your target system database does not contain a column that holds a user account status, and requires retrieving input from several columns of the target database to

determine the status of the target system account, then perform the following procedure:

1. Add a new attribute, for example Status, in the corresponding resource object for status reconciliation.

See Also: The "Reconciliation Field Mappings Tab" section in *Oracle Identity Manager Design Console Guide* for information about status reconciliation

2. In the properties file for reconciliation, add the query for retrieving data from columns required to determine the target system user account status.
3. Write code that implements the required status reconciliation logic in a Java class.
This status reconciliation class must implement the DBUMStatusReconciliation interface and the getStatus method. See the Javadocs shipped with the connector for more information about this interface.
4. Log in to the Design console.
5. Search for and open the lookup definition that maps resource object fields with column names or column name aliases used in the reconciliation query.
6. In the **Decode** column of the resource object attribute that you added in Step 1, for example Status, enter a value in the following format:

`COL_NAME~STATUS_MAPPING_LOOKUP`

In this format:

- `COL_NAME` is the column name or column name alias used in the reconciliation query.
- `STATUS_MAPPING_LOOKUP` is the name of the lookup definition that maps user record status fetched from the target system with the status that can be displayed on the Administrative and User Console.

Sample value: `Status~Lookup.DBUM.TargetRecon.StatusMapping`

7. Save the changes to the lookup definition.
8. Search for and open the **Lookup.DBUM.TargetRecon.StatusMapping** the lookup definition. See [Section A.5.1, "Lookup.DBUM.TargetRecon.StatusMapping"](#) for more information about this lookup definition.
9. In the **Code Key** column, enter the status returned by the status reconciliation class that you created in Step 3.
10. In the **Decode** column, enter the corresponding status to be displayed on the process form in the Administrative and User Console.
11. Repeat Steps 9 and 10 for all possible statuses returned by the status reconciliation class.
12. Save the changes to the lookup definition.
13. To enable status reconciliation:
 - In the Configuration lookup definition for your target system, set values for the following Code Key columns:
 - Status Reconciliation Class Name: Enter the name of the class that you created in Step 3 that implements the logic for status reconciliation.

- Use Status Reconciliation: Enter `Yes` to specify that you want to enable status reconciliation.
- In the scheduled task for user reconciliation, set the value of the Status Reconciliation Primary Key Field attribute to the name of the resource object field, which is the key field for reconciliation matching.

Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected.

You can use the testing utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.

While running the testing utility, the testing utility reads the connectivity information from the IT Resource, lookup definitions from Oracle Identity Manager, and process form data is read from the config.properties file.

While running the testing utility, you must ensure that the connector should be deployed and Oracle Identity Manager should be running. Perform the following steps to test the connector for provisioning:

Note: The testing utility might not work for IBM WebSphere Application Server and Oracle WebLogic Server.

1. Copy the following files to *OIM_HOME*/xellerate/ThirdParty directory:

For IBM WebSphere Application Server:

com.ibm.ws.admin.client_6.1.0.jar from *WAS_HOME*/AppServer/runtimes

ibmorb.jar from *WAS_HOME*/AppServer/java/jre/lib

xlDataObjectBeans.jar from *OIM_CLIENT*/xlclient/lib

For JBoss Application Server:

jbossall-client.jar from *JBOSS_HOME*/client

log4j.jar from *JBOSS_HOME*/server/default/lib

xlGenericUtils.jar from *OIM_HOME*/xellerate/lib

For Oracle WebLogic Server:

weblogic.jar from *BEA_HOME*/weblogic81/server/lib

2. Modify the attributes of the config.properties file using the values specified in the following table. This file is located in the *OIM_HOME*/xellerate/XLIntegrations/DBUM/config directory.

Name	Description	Sample or Default Value
Attributes Common to all databases		

Name	Description	Sample or Default Value
ACTION	<p>Enter the type of operation that you want to test.</p> <p>You can specify one of the following values:</p> <p>For IBM DB2 UDB:</p> <p>CONNECT, CREATEUSER, DELETEUSER</p> <p>For Microsoft SQL Server:</p> <p>CONNECT, CREATELOGIN, DELETELOGIN, CREATEUSER, DELETEUSER, ENABLELOGIN, DISABLELOGIN</p> <p>For Oracle Database:</p> <p>CONNECT, CREATEUSER, DELETEUSER, ENABLEUSER, DISABLEUSER, ADDROLE, ADDPRIVILEGE, UPDATEPASSWORD</p> <p>For Sybase:</p> <p>CONNECT, CREATELOGIN, DELETELOGIN, CREATEUSER, DELETEUSER, ENABLELOGIN, DISABLELOGIN</p>	CREATEUSER
IT_RESOURCE_NAME	<p>Enter the name of the IT resource from which connectivity information must be read.</p> <p>You can specify one of the following values:</p> <p>DB2UDB, MS SQL Server, Oracle, Sybase</p>	Oracle
Process Form Fields and Query Code Keys for Oracle Database	Note: Enter values for these process form fields and query code keys if your target system is Oracle Database. For all other databases, do not enter values for these process form fields and query code keys of the other databases.	
ORA_CREATEUSER_CODE_KEY	Do not change the default values of these query code keys.	ORA_CREATE_USER
ORA_ENABLEUSER_CODE_KEY		ORA_ENABLE_USER
ORA_DISABLEUSER_CODE_KEY		ORA_DISABLE_USER
ORA_DELETEUSER_CODE_KEY		ORA_DELETE_USER
ORA_ADDROLE_CODE_KEY		ORA_ADD_ROLE
ORA_ADDPRIVILEGE_CODE_KEY		ORA_ADD_PRIVILEGE
ORA_UPDATEPASSWORD_CODE_KEY		ORA_UPDATE_PASSWORD
UD_DB_ORA_USERNAME	<p>Enter the user name for the provisioning operation.</p> <p>Note: This is a mandatory field. If you are planning to test a user enable, disable, or delete operation, then you must first ensure that the user exists on the target system.</p>	johndoe
UD_DB_ORA_UITRES	This attribute holds the name of the IT resource to be used for the provisioning operation.	Oracle
UD_DB_ORA_UMPASSWORD	<p>Enter the password for the user whose user name you enter as the value of UD_DB_ORA_UM_USERNAME in this file.</p> <p>Note: You must enter a password if you select the PASSWORD authentication type as the value of UD_DB_ORA_UM_AUTHTYPE in this file.</p>	mypassw0r1

Name	Description	Sample or Default Value
UD_DB_ORA_U_AU THTYPE	Enter the authentication type. You can select one of the following authentication types: PASSWORD, EXTERNAL, or GLOBAL. Note: This is a mandatory field.	PASSWORD
UD_DB_ORA_U_TE MP_QUOTASIZE	Enter values for the columns that you want to use in the provisioning operation.	NA
UD_DB_ORA_U_GL OBAL_DN	Note: You can enter values for all or a combination of these columns. If you do not want to enter a value for a particular property, then leave it empty.	
UD_DB_ORA_U_TE MPTABLESPACE		
UD_DB_ORA_U_TA BLESPLACE		
UD_DB_ORA_U_PR OFILE		
UD_DB_ORA_U_QU OTASIZE		
UD_DB_ORA_R_RO LE	Enter values for these attributes if you want to provision a role.	For UD_DB_ORA_R_ROLE, enter a value in the format shown in the following sample value: 1~CONNECT
UD_DB_ORA_R_AD MIN_OPTION		For UD_DB_ORA_R_ADMI N_OPTION, enter WITH ADMIN OPTION.
UD_DB_ORA_P_PRI VILEGE	Enter values for these attributes if you want to provision a privilege.	For UD_DB_ORA_P_PRIVIL EGE, enter a value in the format shown in the following sample value: 1~CREATE SESSION
UD_DB_ORA_P_AD MIN_OPTION		For UD_DB_ORA_P_ADMI N_OPTION, enter WITH ADMIN OPTION.
Process Form Fields and Query Code Keys for Sybase	Note: Enter values for these process form fields and query code keys if your target system is Sybase. For all other databases, do not enter values for these process form fields and query code keys of the other databases.	

Name	Description	Sample or Default Value
SYB_CREATELOGIN_CODE_KEY	Do not change the default values of these query code keys.	SYB_CREATE_LOGIN
SYB_DELETELOGIN_CODE_KEY		SYB_DELETE_LOGIN
Y		SYB_ENABLE_LOGIN
SYB_ENABLELOGIN_CODE_KEY		SYB_DISABLE_LOGIN
SYB_DISABLELOGIN_CODE_KEY		SYB_CREATE_USER
SYB_CREATEUSER_CODE_KEY		SYB_DELETE_USER
SYB_DELETEUSER_CODE_KEY		
UD_DB_SYB_L_LOGIN	Enter the login name for the provisioning operation. Note: This is a mandatory field. If you are planning to test a login enable, disable, or delete operation, then you must first ensure that the login exists on the target system.	johndoe
UD_DB_SYB_L_ITRES	This attribute holds the name of the IT resource to be used for the provisioning operation.	Sybase
UD_DB_SYB_L_PASSWORD	Enter the password for the user whose user name you enter as the value of UD_DB_SYB_L_LOGIN in this file. Note: You must enter a password.	mypassw0r1
UD_DB_SYB_L_FULLNAME	Enter values for the columns that you want to use in the provisioning operation.	NA
UD_DB_SYB_L_DEFAULTLANG	Note: You can enter values for all or a combination of these columns. If you do not want to enter a value for a particular property, then leave it empty.	
UD_DB_SYB_L_DEFAULTDB		
UD_DB_SYB_U_USERNAME	Enter the user name for the provisioning operation. Note: This is a mandatory field. If you are planning to test a user enable, disable, or delete operation, then you must first ensure that the user exists on the target system.	johndoe
UD_DB_SYB_U_LOGINNAME	Enter the login name for the user provisioning operation. Note: This is a mandatory field. The login name that you enter must exist of the target system.	johndoe
UD_DB_SYB_U_ITRES	This attribute holds the name of the IT resource to be used for the provisioning operation.	Sybase
UD_DB_SYB_U_DEBUGROUP	Enter a value for this column. Note: If you do not want to enter a value for this attribute, then leave it empty.	NA
Process Form Fields and Query Code Keys for IBM DB2 UDB	Note: Enter values for these process form fields and query code keys if your target system is IBM DB2 UDB. For all other databases, do not enter values for these process form fields and query code keys of the other databases.	

Name	Description	Sample or Default Value
DB2_CREATEUSER_CODE_KEY	Do not change the default values of these query code keys.	DB2_CREATE_USER
DB2_ENABLEUSER_CODE_KEY		DB2_GRANT_PRIVILEGE
DB2_DISABLEUSER_CODE_KEY		DB2_REVOKE_PRIVILEGE
DB2_DELETEUSER_CODE_KEY		DB2_DELETE_USER
UD_DB_DB2_U_USERNAME	Enter the user name for the provisioning operation. Note: This is a mandatory field. If you are planning to test a user delete operation, then you must first ensure that the user exists on the target system.	johndoe
UD_DB_DB2_U_ITERES	This attribute holds the name of the IT resource to be used for the provisioning operation.	DB2UDB
UD_DB_DB2_U_USERTYPE	Enter the user type. You can select one of the following user types: USER and GROUP Note: This is a mandatory field.	USER
Process Form Fields and Query Code Keys for Microsoft SQL Server	Note: Enter values for these process form fields and query code keys if your target system is Microsoft SQL Server. For all other databases, do not enter values for these process form fields and query code keys of the other databases.	
UD_DB_SQL_L_LOGIN	Enter the login name for the provisioning operation. Note: This is a mandatory field. If you are planning to test login enable, disable, or delete operation, then you must first ensure that the user exists on the target system.	janedoe
UD_DB_SQL_L_ITERES	This attribute holds the name of the IT resource to be used for the provisioning operation.	MS SQLServer
UD_DB_SQL_L_PASSWORD	Enter the password for the user whose user name you enter as the value of UD_DB_SQL_L_LOGIN in this file. Note: You must enter a password.	mypassw0r1
UD_DB_SQL_L_AUTHTYPE	Enter the authentication type. You can select one of the following authentication types: SQL_SERVER_AUTHENTICATION or WINDOWS_AUTHENTICATION. Note: This is a mandatory field.	SQL_SERVER_AUTHENTICATION
UD_DB_SQL_L_DEF_LANG	Enter values for the columns that you want to use in the provisioning operation.	NA
UD_DB_SQL_L_DEF_DB	Note: You can enter values for one or both these columns. If you do not want to enter a value for a particular attribute, then leave it empty.	
UD_DB_SQL_U_USERNAME	Enter the user name for the provisioning operation. Note: This is a mandatory field. If you are planning to test a user delete operation, then you must first ensure that the user exists on the target system.	rroe
UD_DB_SQL_U_LOGINNAME	Enter the login name for the user provisioning operation. Note: This is a mandatory field. The login name that you enter must exist of the target system.	

Name	Description	Sample or Default Value
UD_DB_SQL_U_ITRES	This attribute holds the name of the IT resource to be used for the provisioning operation.	Sybase
UD_DB_SQL_U_AUTHTYPE	Enter the authentication type. You can select one of the following authentication types: SQL_SERVER_AUTHENTICATION or WINDOWS_AUTHENTICATION. Note: This is a mandatory field.	SQL_SERVER_AUTHENTICATION
Attributes Used for Oracle Identity Manager Signature Login (Common to all Databases)		
XL_HOME_DIR	For a signature-based login in Oracle Identity Manager, you must set values for the following system properties:	NA
JAVA_SECURITY_POLICY	XL_HOME_DIR: Specify the path of the Oracle Identity Manager home directory. For example, the path until the xellerate directory.	OIM_HOME/xellerate
JAVA_SECURITY_AUTH_LOGIN_CONFIG	For example: C:\OIM_JBOSS_9102\OimServer\xellerate	
JAVA_NAMING_PROVIDER_URL	JAVA_SECURITY_POLICY: Specify the path of xl.policy file. It is present in the config directory. For example: C:\OIM_JBOSS_9102\OimServer\xellerate\config\xl.policy JAVA_SECURITY_AUTH_LOGIN_CONFIG: Specify the path of auth.conf file. It is present in the config directory. For example: C:\OIM_JBOSS_9102\OimServer\xellerate\config\auth.conf For JBoss Application Server: Specify the path of aut.conf For Oracle WebLogic Server: Specify the path of authwl.conf file For IBM WebSphere Application Server: Specify the path of authws.conf JAVA_NAMING_PROVIDER_URL: Specify the value of the "java.naming.provider.url" attribute present in the Discovery settings in OIM_HOME/xellerate/config/xlconfig.xml	Path of the xl.policy file, such as OIM_HOME/xellerate/config/xl.policy Path of the auth.conf file, such as OIM_HOME/xellerate/config/auth.conf Value of java.naming.provider.url in OIM_HOME/xellerate/config/xlconfig.xml

3. After you specify values in the config.properties file, run one of the following files:

For UNIX:

OIM_HOME/xellerate/XLIntegrations/DBUM/scripts/DBUMTestingUtility.sh

For Microsoft Windows:

OIM_HOME/XLIntegrations/DBUM/scripts/DBUMTestingUtility.bat

The following table lists the column names or attributes for create and update user in the config.properties and their labels:

Attributes	Labels
Oracle Database	
UD_DB_ORA_U_USERNAME	Username

Attributes	Labels
UD_DB_ORA_U_ITRES	IT Resource
UD_DB_ORA_U_PASSWORD	Password
UD_DB_ORA_U_AUTHTYPE	Authentication Type
UD_DB_ORA_U_TEMP_QUOTASIZE	Temporary Tablespace Quota (in MB)
UD_DB_ORA_U_GLOBAL_DN	Global DN
UD_DB_ORA_U_TEMPTABLESPACE	Temporary Tablespace
UD_DB_ORA_U_TABLESPAC	Default Tablespace
UD_DB_ORA_U_PROFILE	Profile Name
UD_DB_ORA_U_QUOTASIZE	Default Tablespace Quota (in MB)
UD_DB_ORA_R_ROLE	Role
UD_DB_ORA_R_ADMIN_OPTION	Role Admin Option
UD_DB_ORA_P_PRIVILEGE	Privilege
UD_DB_ORA_P_ADMIN_OPTION	Privilege Admin Option
Sybase database	
UD_DB_SYB_L_LOGIN	Login Name
UD_DB_SYB_L_PASSWORD	Password
UD_DB_SYB_L_ITRES	IT Resource
UD_DB_SYB_L_FULLNAME	Full Name
UD_DB_SYB_L_DEFAULTLANG	Default Language
UD_DB_SYB_L_DEFDB	Default Database
UD_DB_SYB_U_USERNAME	Username
UD_DB_SYB_U_LOGINNAME	Login Name
UD_DB_SYB_U_ITRES	IT Resource
UD_DB_SYB_U_DBGROUP	Database Group
DB2 database	
UD_DB_DB2_U_USERNAME	Username
UD_DB_DB2_U_ITRES	IT Resource
UD_DB_DB2_U_USERTYPE	User Type
MSSQL database	
UD_DB_SQL_L_LOGIN	Login Name
UD_DB_SQL_L_PASSWORD	Password
UD_DB_SQL_L_AUTHTYPE	Authentication Type
UD_DB_SQL_L_ITRES	IT Resource
UD_DB_SQL_L_DEFLANG	Default Language
UD_DB_SQL_L_DEFDB	Default DataBase
UD_DB_SQL_U_USERNAME	Username
UD_DB_SQL_U_LOGINNAME	Login Name
UD_DB_SQL_U_AUTHTYPE	Authentication Type

Attributes	Labels
UD_DB_SQL_U_ITRES	IT Resource

Known Issues

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

- **Bug 6696248**

The Database User Management connector does not support SSL communication between an Oracle Database target system and Oracle Identity Manager running on IBM WebSphere Application Server or Oracle Application Server.

- **Bug 9159594**

During an update password provisioning operation, if you modify the value in the Password field without clearing the existing password, then the newly added characters in the Password field are not encrypted. These characters are displayed in clear text. Therefore, as a work around, you must ensure that you clear the existing text in the Password field, and then enter the new password. This ensures that the value in the Password field is encrypted.

- **Bug 8766239**

In this release, the connector does not support management of Kerberos-authenticated users.

- **Bug 9226032**

The connector supports only the English language. Resource bundles for the other languages are not included in this release of the connector.

Preconfigured Lookup Definitions

This appendix discusses the following topics:

- [Section A.1, "Lookup Definitions for IBM DB2 UDB"](#)
- [Section A.2, "Lookup Definitions for Microsoft SQL Server"](#)
- [Section A.3, "Lookup Definitions for Oracle Database"](#)
- [Section A.4, "Lookup Definitions for Sybase"](#)
- [Section A.5, "Other Lookup Definitions"](#)

A.1 Lookup Definitions for IBM DB2 UDB

This section provides information about the following lookup definitions:

- [Section A.1.1, "Lookup.DBUM.DB2.Configuration"](#)
- [Section A.1.2, "Lookup.DBUM.DB2.Error.Mapping"](#)
- [Section A.1.3, "Lookup.DBUM.DB2.ExclusionList"](#)
- [Section A.1.4, "Lookup.DBUM.DB2.Parameter.Configuration"](#)
- [Section A.1.5, "Lookup.DBUM.DB2.Provisioning.Validation"](#)
- [Section A.1.6, "Lookup.DBUM.DB2.Query.Configuration"](#)
- [Section A.1.7, "Lookup.DBUM.DB2.TargetRecon.Delete.Mapping"](#)
- [Section A.1.8, "Lookup.DBUM.DB2.TargetRecon.Mapping"](#)
- [Section A.1.9, "Lookup.DBUM.DB2.TargetRecon.QueryFilter"](#)
- [Section A.1.10, "Lookup.DBUM.DB2.TargetRecon.Schema.Configuration"](#)
- [Section A.1.11, "Lookup.DBUM.DB2.TargetRecon.Schema.Mapping"](#)
- [Section A.1.12, "Lookup.DBUM.DB2.TargetRecon.Schema.QueryFilter"](#)
- [Section A.1.13, "Lookup.DBUM.DB2.TargetRecon.Tablespace.Configuration"](#)
- [Section A.1.14, "Lookup.DBUM.DB2.TargetRecon.Tablespace.Mapping"](#)
- [Section A.1.15, "Lookup.DBUM.DB2.TargetRecon.Tablespace.QueryFilter"](#)
- [Section A.1.16, "Lookup.DBUM.DB2.TargetRecon.Transformation"](#)
- [Section A.1.17, "Lookup.DBUM.DB2.TargetRecon.UserTypeMapping"](#)
- [Section A.1.18, "Lookup.DBUM.DB2.TargetRecon.Validation"](#)
- [Section A.1.19, "Lookup.DBUM.DB2.TrustedRecon.Configuration"](#)

- [Section A.1.20, "Lookup.DBUM.DB2.TrustedRecon.Delete.Mapping"](#)
- [Section A.1.21, "Lookup.DBUM.DB2.TrustedRecon.ExclusionList"](#)
- [Section A.1.22, "Lookup.DBUM.DB2.TrustedRecon.Mapping"](#)
- [Section A.1.23, "Lookup.DBUM.DB2.TrustedRecon.QueryFilter"](#)
- [Section A.1.24, "Lookup.DBUM.DB2.TrustedRecon.Transformation"](#)
- [Section A.1.25, "Lookup.DBUM.DB2.TrustedRecon.Validation"](#)
- [Section A.1.26, "Lookup.DBUM.DB2.UserType"](#)
- [Section A.1.27, "Lookup.DBUM.DB2.WithGrantOption"](#)

A.1.1 Lookup.DBUM.DB2.Configuration

The Lookup.DBUM.DB2.Configuration lookup definition holds connector configuration entries that are used during target resource reconciliation and provisioning operations.

Note: You cannot add entries to this lookup definition. However, you can modify the Decode values of the existing entries.

[Table A–1](#) lists the default entries in this lookup definition.

Table A–1 Entries in the Lookup.DBUM.DB2.Configuration Lookup Definition

Code Key	Decode	Description
Error Mapping Lookup	Lookup.DBUM.DB2.Error.Mapping	See Section A.1.2, "Lookup.DBUM.DB2.Error.Mapping" for information about this lookup definition.
Parameter Configuration Lookup	Lookup.DBUM.DB2.Parameter.Configuration	See Section A.1.4, "Lookup.DBUM.DB2.Parameter.Configuration" for information about this lookup definition.
Provisioning Validation Lookup	Lookup.DBUM.DB2.Provisioning.Validation	See Section A.1.5, "Lookup.DBUM.DB2.Provisioning.Validation" for information about this lookup definition.
Query Configuration Lookup	Lookup.DBUM.DB2.Query.Configuration	See Section A.1.6, "Lookup.DBUM.DB2.Query.Configuration" for information about this lookup definition.
Reconciliation Class Name	oracle.iam.connectors.dbum.tasks.impl.DBUMQueryReconciliationImpl.java	Name of the class that implements the logic for target resource reconciliation.
Reconciliation Query Property File	Enter a value	Enter the full path and name of the file containing queries that must be run during reconciliation.
Reconciliation SQL Injection Keywords	NODATA	List of SQL keywords (separated by tilde (~) character) that must not be used in the reconciliation query. The connector does not run a query (used for target resource reconciliation) that contains any of the keywords listed in the Decode column.

Table A-1 (Cont.) Entries in the Lookup.DBUM.DB2.Configuration Lookup Definition

Code Key	Decode	Description
Reserved Words List	GRANT ~REVOKE ~OF ~ON ~TO ~DATABASE ~TABLESPACE ~SCHEMA ~CREATEIN ~ALTERIN ~DROPIN ~FROM ~USE ~GRANT\t~REVOKE\t~OF\t~ON\t~T O\t~DATABASE\t~TABLESPACE\t~SC HEMA\t~CREATEIN\t~ALTERIN\t~D ROPIN\t~FROM\t~USE\t	List of reserve words that are not supported in the OIM User process form fields during provisioning operations.
Resource Exclusion Column Key	UD_DB_DB2_U_USERNAME	Name of the process form field that is excluded during provisioning operations.
Resource Exclusion List Lookup	Lookup.DBUM.DB2.ExclusionList	See Section A.1.3 , "Lookup.DBUM.DB2.ExclusionList" for more information about this lookup definition.
Status Reconciliation Class Name	NODATA	Name of the class that implements the logic for deriving the status of a target system user account.
SSL Keystore Properties	NODATA	If you want to configure secure communication between the target system and Oracle Identity Manager, then enter the SSL keystore details in the following format: javax.net.ssl.trustStore=truststore~javax.net.ssl.trustStorePassword=password
Target Date Format	NODATA	Enter the format in which date values are stored on the target system.
Unsupported Special Characters	NODATA	Enter the list of special characters that are not supported in the process form fields during provisioning operations.
Use Status Reconciliation	No	Specifies whether you want to run reconciliation for the status of a target system user account.
Use Validation For Provisioning	No	Specifies whether you want to enable validation of user attributes during provisioning operations.

A.1.2 Lookup.DBUM.DB2.Error.Mapping

When an error is encountered during a provisioning operation, an error message is displayed on the Administrative and User Console.

The Lookup.DBUM.DB2.Error.Mapping lookup definition maps error codes displayed by the database with error messages to be displayed on the process form in the Administrative and User Console during provisioning operations.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** SQL error code returned by the database
- **Decode:** Corresponding error message to be displayed on the process form

To add or modify entries in this lookup definition, you must enter values in the format specified in the preceding paragraph.

[Table A-2](#) lists the default entries in this lookup definition.

Table A-2 Entries in the Lookup.DBUM.DB2.Error.Mapping Lookup Definition

Code Key	Decode
-287	OBJECT_NOT_USED
-551	PERMISSION_NOT_GRANTED
-556	QUERY_EXECUTION_FAILED
900	INVALID_SQL

A.1.3 Lookup.DBUM.DB2.ExclusionList

The Lookup.DBUM.DB2.ExclusionList lookup definition holds user attributes of the target system accounts for which you do not want to perform target resource reconciliation and provisioning.

For target system accounts on which you do not want to perform provisioning operations, the following is the format of the Code Key and Decode values:

- **Code Key:** Name of the process form field
- **Decode:** Process form field values separated by the tilde (~) character

For target system accounts that must not be reconciled during a target resource reconciliation run, the following is the format of the Code Key and Decode values:

- **Code Key:** Resource object field name
- **Decode:** Resource object field values separated by the tilde (~) character

[Table A-3](#) lists the default entry in this lookup definition.

See Also: [Section 3.1.3, "Setting Up the ExclusionList Lookup Definition"](#) for information about adding or modifying entries in this lookup definition

Table A-3 Entries in the Lookup.DBUM.DB2.ExclusionList Lookup Definition

Code Key	Decode
UD_DB_DB2_U_USERNAME	db2admin
User Name	db2admin

A.1.4 Lookup.DBUM.DB2.Parameter.Configuration

The Lookup.DBUM.DB2.Parameter.Configuration lookup definition maps identifiers in a SQL statement or SQL fragment (defined in the Lookup.DBUM.DB2.Query.Configuration lookup definition) with names of the process form fields.

During provisioning operations, the data that you enter on the OIM User form is stored in the corresponding fields of the process form in the Design Console. The fields of the process form are mapped to the identifiers of SQL statements or SQL fragments used for provisioning. In other words, the SQL statements use the data present in the process form to run SQL statements. These SQL statements or SQL fragments are defined in the Lookup.DBUM.DB2.Query.Configuration lookup definition.

See Also: [Section A.1.6, "Lookup.DBUM.DB2.Query.Configuration"](#) for more information about the Lookup.DBUM.DB2.Query.Configuration lookup definition

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Identifier in a SQL statement or SQL fragment used for provisioning operations
- **Decode:** Combination of the following elements separated by the tilde (~) character:

PF_FIELD_NAME~PF_DATA_TYPE~PARAMETER_TYPE~QUOTE_TYPE~EXCLUDE_VALIDATION~UPPERCASE

Note: The sequence of elements in the Decode value must not be changed.

In this format:

- *PF_FIELD_NAME* is name of the process form field.
- *PF_DATA_TYPE* is the data type of the process form field.
- *PARAMETER_TYPE* specifies whether the value in the process form field is of type input or output.

If the value in the process form field is used as an input parameter, for example, as an input to a variable in the SQL statement, then use IN. Otherwise, OUT.

- *QUOTE_TYPE* specifies whether the value from the process form field that is passed to the SQL statement must be enclosed in a single quotation mark or double quotation mark. The *QUOTE_TYPE* element is optional.

If you want the value in the process form field to be enclosed in single quotation marks, then use SINGLE_QUOTE. If you want the value in the process form field to be enclosed in double quotation marks, then use DOUBLE_QUOTE.

- EXCLUDE_VALIDATION element is optional. This element is used in the following scenario:

Suppose you specify values for the Reserved Words List or Unsupported Special Characters entries of the Lookup.DBUM.DB2.Configuration lookup definition. During provisioning operations, the connector checks whether the fields on the OIM User form contain any of the values specified in the Reserved Words List or Unsupported Special Characters entries. If such values are found, then no provisioning operations are performed on that record. If you do not want the connector to perform this check on a particular field of the OIM User form, then include EXCLUDE_VALIDATION along with the name of the process form field.

For example, the

UD_DB_DB2_T_TABLESPACE~varchar2~IN~EXCLUDE_VALIDATION

Decode value specifies that during a particular provisioning operation, the connector does not check whether the Tablespace field contains any of the values specified in the Reserved Words List or Unsupported Special Characters entries of the Lookup.DBUM.DB2.Configuration lookup definition.

- UPPERCASE element is an optional element. You use this element if you want to save on the target system the value entered in the process form field in upper case.

If you want to add or modify entries in this lookup definition, then you must enter values in the format specified earlier in this section. Note that changes that you make in the Code Key column of this lookup definition must be duplicated in the Lookup.DBUM.DB2.Query.Configuration lookup definition. This is illustrated by the following example:

Suppose, in [Table A-4](#), if you change the db2_user_name Code Key value to db2_username, then in the Lookup.DBUM.DB2.Query.Configuration lookup definition, you must change all occurrences of db2_user_name to db2_username.

[Table A-4](#) lists the default entries in this lookup definition.

Table A-4 Entries in the Lookup.DBUM.DB2.Parameter.Configuration Lookup Definition

Code Key	Decode
db2_s_grant_option	UD_DB_DB2_S_GRANT_OPTION~varchar2~IN~EXCLUDE_VALIDATION
db2_schema	UD_DB_DB2_S_SCHEMA~varchar2~IN~EXCLUDE_VALIDATION
db2_t_grant_option	UD_DB_DB2_T_GRANT_OPTION~varchar2~IN~EXCLUDE_VALIDATION
db2_tablespace	UD_DB_DB2_T_TABLESPACE~varchar2~IN~EXCLUDE_VALIDATION
db2_user_name	UD_DB_DB2_U_USERNAME~varchar2~IN
db2_user_type	UD_DB_DB2_U_USERTYPE~varchar2~IN~EXCLUDE_VALIDATION

A.1.5 Lookup.DBUM.DB2.Provisioning.Validation

The Lookup.DBUM.DB2.Provisioning.Validation lookup definition is used to store the mapping between the attribute for which validation has to be applied (during provisioning) and the validation implementation class.

The Lookup.DBUM.DB2.Provisioning.Validation lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.1.6 Lookup.DBUM.DB2.Query.Configuration

As mentioned earlier in this guide, the Database User Management connector uses SQL statements for provisioning operations. These SQL statements are defined in the Lookup.DBUM.DB2.Query.Configuration lookup definition. Depending on the provisioning operations that you are performing, adapters run the appropriate SQL statements on the target system. In this chapter, this connector uses SQL statements to perform provisioning operations.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the SQL statement or SQL fragment
- **Decode:** Corresponding SQL statement or SQL fragment. The SQL statement is a combination of the following entries:
 - SQL Keywords

This is a mandatory element. Examples of SQL keywords are GRANT and REVOKE.

- Identifiers

This is a mandatory element.

In [Table A-5](#), db2_user_name, db2_user_type, db2_tablespace, and db2_schema are identifiers. The actual values for these identifiers are determined at run time.

- Name of the SQL fragment

In [Table A-5](#), WITH_GRANT_OPTION_S and WITH_GRANT_OPTION_T are names of SQL fragments.

For example, in the Decode value of the DB2_ASSIGN_SCHEMA Code Key in [Table A-5](#), it is optional to include WITH_GRANT_OPTION_S in the SQL statement that is used to grant schema to a user account on the target system. The name of the SQL fragment, WITH_GRANT_OPTION_S, has been specified as optional as you may not want to grant to all user accounts on the target system privileges to grant schemas to other users.

[Table A-5](#) lists the default entries in this lookup definition.

If you want to add or modify entries in this lookup definition, then you must enter values in the format specified earlier in this section. Note that changes that you make to identifiers in this lookup definition must be duplicated in the corresponding Code Key value of the Lookup.DBUM.DB2.Parameter.Configuration lookup definition. In addition, you must also duplicate this change in all occurrences of the identifier in this lookup definition.

Table A-5 Entries in the Lookup.DBUM.DB2.Query.Configuration Lookup Definition

Code Key	Decode
DB2_ASSIGN_SCHEMA	GRANT CREATEIN,DROPIN,ALTERIN ON SCHEMA :db2_schema TO :db2_user_type :db2_user_name~WITH_GRANT_OPTION_S
DB2_ASSIGN_TABLESPACE	GRANT USE OF TABLESPACE :db2_tablespace TO :db2_user_type :db2_user_name~WITH_GRANT_OPTION_T
DB2_CREATE_USER	GRANT CONNECT,DBADM,CREATETAB,BINDADD,CREATE_NOT_FENCED_ROUTINE,IMPLICIT_SCHEMA,LOAD,CREATE_EXTERNAL_ROUTINE,QUIESCE_CONNECTION ON DATABASE TO :db2_user_type :db2_user_name
DB2_DELETE_USER	REVOKE CONNECT,DBADM ON DATABASE FROM :db2_user_type :db2_user_name
DB2_REVOKE_SCHEMA	REVOKE CREATEIN,DROPIN,ALTERIN ON SCHEMA :db2_schema FROM :db2_user_type :db2_user_name
DB2_REVOKE_TABLESPACE	REVOKE USE OF TABLESPACE :db2_tablespace FROM :db2_user_type :db2_user_name
WITH_GRANT_OPTION_S	:db2_s_grant_option
WITH_GRANT_OPTION_T	:db2_t_grant_option
DB2_GET_USER	select GRANTEE from SYSIBM.SYSDBAUTH where GRANTEE=:db2_user_name

A.1.7 Lookup.DBUM.DB2.TargetRecon.Delete.Mapping

The Lookup.DBUM.DB2.TargetRecon.Delete.Mapping lookup definition maps the resource object attribute with the primary key column name used in the reconciliation

query. Note that this resource object attribute is the key field for reconciliation matching.

The Lookup.DBUM.DB2.TargetRecon.Delete.Mapping lookup definition is used during delete user target reconciliation runs.

During a delete user reconciliation run, the resource object attribute that you specify in this lookup definition is used for comparing target system user records with existing target system resource assigned to OIM Users. During this comparison process, if no match is found between the target system user record and the resource provisioned to the OIM User, then the database user resource is revoked from the OIM User.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the resource object attribute, which is the key field for reconciliation matching
- **Decode:** Primary key column name used in the reconciliation query for performing delete user reconciliation

Table A–6 lists the default entry in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify values of the existing Code Key and Decode values.

Table A–6 Entries in the Lookup.DBUM.DB2.TargetRecon.Delete.Mapping Lookup Definition

Code Key	Decode
User Name	GRANTEE

A.1.8 Lookup.DBUM.DB2.TargetRecon.Mapping

The Lookup.DBUM.DB2.TargetRecon.Mapping lookup definition maps resource object attributes with column names or column name aliases used in the reconciliation query. This lookup definition is used for performing target resource user reconciliation runs.

In this lookup definition, the Code Key contains the reconciliation attribute of the resource object.

For Code Key columns that store single-valued attributes, the Decode value can be in one of the following formats:

- COL_NAME or COL_NAME_ALIAS

In this format, COL_NAME is the target system column name used in the reconciliation query. COL_NAME_ALIAS is the alias of the target system column names used in the reconciliation query.

You use this format if the target system contains a column corresponding to the resource object attribute.

For example, consider the User Name attribute, which is a single-valued attribute on the resource object. The target system contains GRANTEE, which is a column corresponding to the User Name attribute. Therefore, the mapping is as follows:

Code Key: User Name

Decode: GRANTEE

- CONSTANT~CONSTANT_VALUE

In this format, `CONSTANT` specifies that the data in this column is constant. `CONSTANT_VALUE` is the value to be displayed in the corresponding field of the OIM User form in the Administrative and User Console.

You use this format if you want to set a constant value for a particular field on the OIM User form.

- `COLUMN_NAME~LOOKUP_NAME`

In this format, `COLUMN_NAME` is the target system column name from which value is fetched. `LOOKUP_NAME` is the name of the lookup definition that maps values fetched from the target system with values to be displayed in the OIM User form field.

You use this format if you want values fetched from the target system to be displayed in a format that is accepted by Oracle Identity Manager.

For example, consider the User Type attribute of the resource object. This is a single valued attribute. The target system contains `GRANTEETYPE`, which is a column corresponding to the User Type attribute of the resource object. However, we do not map the User Type resource object attribute to the `GRANTEETYPE` column for the following reason:

The `GRANTEETYPE` column stores values such as U and G. Therefore, during reconciliation, this connector fetches a value of U or G from the `GRANTEETYPE` target system column. A value of U means that the grantee is a user account. A value of G means that the grantee is a group account.

However, the values U or G cannot be displayed in the User Type field of the OIM User form. This is because Oracle Identity Manager accepts only one of the following values as the type of a user account:

- User
- Group

Therefore, in order to display the status retrieved from the `GRANTEETYPE` column in a format that is accepted by Oracle Identity Manager, the User Type attribute of the resource object has been mapped to `GRANTEETYPE~Lookup.DBUM.DB2.TargetRecon.UserTypeMapping`.

This implies that in the Code Key column of the `Lookup.DBUM.DB2.TargetRecon.UserTypeMapping` lookup definition, the connector searches for the value that is fetched from the `GRANTEETYPE` column of the target system. Then, the corresponding Decode value is displayed as the type of the user account in Oracle Identity Manager. This is illustrated by the following example:

Suppose the value fetched from the `GRANTEETYPE` column for a particular user account on the target system is U. In the Code Key column of the `Lookup.DBUM.DB2.TargetRecon.UserTypeMapping` lookup definition, the connector searches for the value U. The Decode value of the U Code Key is User. Therefore, in Oracle Identity Manager, the connector displays User as the status of the User Type field.

See Also: [Section A.1.17, "Lookup.DBUM.DB2.TargetRecon.UserTypeMapping"](#)

- `LOOKUP~COL_NAME`

In this format:

- LOOKUP specifies that the data retrieved from the target system is lookup data.
- COL_NAME is the corresponding column name or column name alias used in the reconciliation query

You use this format if process form field corresponding to the Code Key value is a lookup type field.

For Code Key columns that store multivalued attributes, the Decode value is specified in the following format:

`CHILD~MULTIVALUED_ATTR_CONFIG_LOOKUP`

In this format:

- CHILD specifies that the data in this column is the child attribute data
- MULTIVALUED_ATTR_CONFIG_LOOKUP is name of the lookup definition that holds configurable entries for the multivalued attribute.

For example, Schema List is a multivalued attribute. The Decode value of the Schema List Code Key value is

`CHILD~Lookup.DBUM.DB2.TargetRecon.Schema.Configuration`. The `Lookup.DBUM.DB2.TargetRecon.Schema.Configuration` lookup definition contains configurable entries for the Schema List attribute.

You can add or remove entries in the `Lookup.DBUM.DB2.TargetRecon.Mapping` lookup definition. See [Section 4.2, "Adding or Removing Attributes for Reconciliation"](#) for information about adding or modifying entries in this lookup definition.

[Table A-7](#) lists the default entries in this lookup definition.

Table A-7 Entries in the Lookup.DBUM.DB2.TargetRecon.Mapping Lookup Definition

Code Key	Decode
Schema List	CHILD~Lookup.DBUM.DB2.TargetRecon.Schema.Configuration
Status	CONSTANT~Enabled
Tablespace List	CHILD~Lookup.DBUM.DB2.TargetRecon.Tablespace.Configuration
User Name	GRANTEE
User Type	GRANTEETYPE~Lookup.DBUM.DB2.TargetRecon.UserTypeMapping

A.1.9 Lookup.DBUM.DB2.TargetRecon.QueryFilter

The `Lookup.DBUM.DB2.TargetRecon.QueryFilter` lookup definition holds information about the filter parameters that you want to use while running the SQL query for target resource reconciliation.

The `Lookup.DBUM.DB2.TargetRecon.QueryFilter` lookup definition is empty by default.

See [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#) for information about adding entries to this lookup definition.

A.1.10 Lookup.DBUM.DB2.TargetRecon.Schema.Configuration

The `Lookup.DBUM.DB2.TargetRecon.Schema.Configuration` lookup definition holds configuration entries related to the Schema List multivalued attribute.

[Table A-8](#) lists the default entries in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify the Decode values of existing entries.

Table A–8 Entries in the *Lookup.DBUM.DB2.TargetRecon.Schema.Configuration* Lookup Definition

Code Key	Decode	Description
Child Attribute Mapping Lookup	Lookup.DBUM.DB2.TargetRecon.Schema.Mapping	See Section A.1.11 , "Lookup.DBUM.DB2.TargetRecon.Schema.Mapping" for information about this lookup definition.
Child Query Name	DB2_TARGET_USER_SCHEMA	Name of the query in the reconciliation query file that you want to run for reconciling data about the child attribute.
Child Reconciliation Query Filter Lookup	Lookup.DBUM.DB2.TargetRecon.Schema.QueryFilter	Name of the lookup definition that contains information about reconciliation filter parameters for the child attribute. See Section A.1.12 , "Lookup.DBUM.DB2.TargetRecon.Schema.QueryFilter" for more information about this lookup definition.
Parent Attribute	GRANTEE	Primary key column of the query used for running target resource user reconciliation.

A.1.11 Lookup.DBUM.DB2.TargetRecon.Schema.Mapping

The Lookup.DBUM.DB2.TargetRecon.Schema.Mapping lookup definition maps the attributes of the Schema List multivalued attribute with column names used in the reconciliation query. This lookup definition is used to retrieve data about the Schema List attribute during target resource reconciliation.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Attribute name of the multivalued attribute
- **Decode:** The value is specified in one of the following formats:

- LOOKUP~COL_NAME

In this format:

- LOOKUP specifies that the data retrieved from the target system is lookup data.
- COL_NAME is the corresponding column name or column name alias used in the reconciliation query

You use this format if process form field corresponding to the Code Key value is a lookup type field.

- COL_NAME

This is the column name used in the reconciliation query corresponding to the value in the code key column.

If you want to add or modify the entries in this lookup definition, then you must specify values in the format described in this section.

[Table A-9](#) lists the default entry in this lookup definition.

Table A-9 Entries in the *Lookup.DBUM.DB2.TargetRecon.Schema.Mapping* Lookup Definition

Code Key	Decode
Schema Name	LOOKUP~SCHEMANAME

A.1.12 Lookup.DBUM.DB2.TargetRecon.Schema.QueryFilter

The Lookup.DBUM.DB2.TargetRecon.Schema.QueryFilter lookup definition holds information about the filter parameters that you want to use while running the SQL query for retrieving data about the Schema List multivalued attribute during target resource reconciliation.

The Lookup.DBUM.DB2.TargetRecon.Schema.QueryFilter lookup definition is empty by default.

See [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#) for information about adding entries to this lookup definition.

A.1.13 Lookup.DBUM.DB2.TargetRecon.Tablespace.Configuration

The Lookup.DBUM.DB2.TargetRecon.Tablespace.Configuration lookup definition holds configuration entries related to the Tablespace List multivalued attribute.

[Table A-10](#) lists the default entries in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify the Decode values of existing entries.

Table A-10 Entries in the *Lookup.DBUM.DB2.TargetRecon.Tablespace.Configuration* Lookup Definition

Code Key	Decode	Description
Child Attribute Mapping Lookup	Lookup.DBUM.DB2.TargetRecon.Tablespace.Mapping	See Section A.1.14, "Lookup.DBUM.DB2.TargetRecon.Tablespace.Mapping" for information about this lookup definition.
Child Query Name	DB2_TARGET_USER_TABLESPACE	Name of the query in the reconciliation query file that you want to run for reconciling data about the child attribute. .
Child Reconciliation Query Filter Lookup	Lookup.DBUM.DB2.TargetRecon.Tablespace.QueryFilter	Name of the lookup definition that contains information about reconciliation filter parameters for the child attribute. See Section A.1.15, "Lookup.DBUM.DB2.TargetRecon.Tablespace.QueryFilter" for more information about this lookup definition.
Parent Attribute	GRANTEE	Primary key column of the query used for running target resource user reconciliation.

A.1.14 Lookup.DBUM.DB2.TargetRecon.Tablespace.Mapping

The Lookup.DBUM.DB2.TargetRecon.Tablespace.Mapping lookup definition maps the attributes of the Tablespace List multivalued attribute with column names used in the reconciliation query. This lookup definition is used to retrieve data about the Tablespace List attribute during target resource reconciliation.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Attribute name of the multivalued attribute
- **Decode:** The value is specified in one of the following formats:

- LOOKUP~COL_NAME

In this format:

- LOOKUP specifies that the data retrieved from the target system is lookup data.
- COL_NAME is the corresponding column name or column name alias used in the reconciliation query

You use this format if process form field corresponding to the Code Key value is a lookup type field.

- COL_NAME

This is the column name used in the reconciliation query corresponding to the value in the code key column.

If you want to add or modify the entries in this lookup definition, then you must specify values in the format described in this section.

[Table A-11](#) lists the default entries in this lookup definition.

Table A-11 Entries in the Lookup.DBUM.DB2.TargetRecon.Tablespace.Mapping Lookup Definition

Code Key	Decode
Tablespace Name	LOOKUP~TBSPACE

A.1.15 Lookup.DBUM.DB2.TargetRecon.Tablespace.QueryFilter

The Lookup.DBUM.DB2.TargetRecon.Tablespace.QueryFilter lookup definition holds information about the filter parameters that you want to use while running the SQL query for retrieving data about the Tablespace List multivalued attribute during target resource reconciliation.

The Lookup.DBUM.DB2.TargetRecon.Tablespace.QueryFilter lookup definition is empty by default.

See [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#) for information about adding entries to this lookup definition.

A.1.16 Lookup.DBUM.DB2.TargetRecon.Transformation

The Lookup.DBUM.DB2.TargetRecon.Transformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during target resource reconciliation.

The Lookup.DBUM.DB2.TargetRecon.Transformation lookup definition is empty by default.

See [Section 4.9, "Configuring Transformation of Data During Reconciliation"](#) for information about adding entries to this lookup definition.

A.1.17 Lookup.DBUM.DB2.TargetRecon.UserTypeMapping

The Lookup.DBUM.DB2.TargetRecon.UserTypeMapping maps user account types in the target system with corresponding user types to be displayed in the User Type field of the OIM User form.

During target resource reconciliation, this connector fetches a value of U or G from the GRANTEETYPE target system column. A value of U means that the grantee is a user account. A value of G means that the grantee is a group account.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Character in the GRANTEETYPE target system column
- **Decode:** Corresponding value to be displayed in the User Type field of the OIM User form.

If you want to add or modify entries in this lookup definition, then you must specify entries in the format described in the preceding paragraph.

[Table A-12](#) lists the entries in this lookup definition.

Table A-12 Entries in the Lookup.DBUM.DB2.TargetRecon.UserTypeMapping Lookup Definition

Code Key	Decode
G	Group
U	User

A.1.18 Lookup.DBUM.DB2.TargetRecon.Validation

The Lookup.DBUM.DB2.TargetRecon.Validation lookup definition is used to configure validation of attribute values that are fetched from the target system during target resource reconciliation.

The Lookup.DBUM.DB2.TargetRecon.Validation lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.1.19 Lookup.DBUM.DB2.TrustedRecon.Configuration

The Lookup.DBUM.DB2.TrustedRecon.Configuration lookup definition holds connector configuration entries that are used during trusted source reconciliation.

[Table A-13](#) lists the default entries in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify the Decode values of existing entries.

Table A–13 Entries in the Lookup.DBUM.DB2.TrustedRecon.Configuration Lookup Definition

Code Key	Decode	Description
Reconciliation Class Name	oracle.iam.connectors.dbum.tasks.impl.DBUMQueryReconciliationImpl	Name of the class that implements the logic for trusted source reconciliation.
Reconciliation Query Property File	Enter a value	Enter the full path and name of the file containing queries that must be run during reconciliation.
Reconciliation SQL Injection Keywords	DROP ~DROP\t~INSERT ~INSERT\t~ALTER ~ALTER\t~CREATE ~CREATE\t~DELETE ~DELETE\t~UPDATE ~UPDATE\t~TRUNCATE ~TRUNCATE\t~EXEC ~EXEC\t~/*~---~;	List of SQL keywords that must not be used in the reconciliation query. The connector does not run a query (used for trusted source reconciliation) that contains any of the keywords listed in the Decode column.
Resource Exclusion List Lookup	Lookup.DBUM.DB2.TrustedRecon.ExclusionList	See Section A.1.21, "Lookup.DBUM.DB2.TrustedRecon.ExclusionList" for more information about this lookup definition.
Status Reconciliation Class Name	NODATA	Name of the class that implements the logic for deriving the status of a target system user account. You must enter a value for this entry only if you want to retrieve the status of a target system account. See Section 5.12, "Configuring Status Reconciliation" if you want to reconcile the status of an account on the target system
Target Date Format	NODATA	Enter the format in which date values are stored on the target system.
Use Status Reconciliation	No	Specifies whether you want to run reconciliation for the status of a target system user account.

A.1.20 Lookup.DBUM.DB2.TrustedRecon.Delete.Mapping

The Lookup.DBUM.DB2.TrustedRecon.Delete.Mapping lookup definition maps the resource object attribute with the primary key column name used in the reconciliation query (for retrieving all users from the target system). Note that this resource object attribute is the key field for reconciliation matching.

The Lookup.DBUM.DB2.TrustedRecon.Delete.Mapping lookup definition is used during delete user trusted reconciliation runs.

During a delete user reconciliation run, the resource object attribute that you specify in this lookup definition is used for comparing target system user records with existing OIM Users. During this comparison process, if no match is found between the target system user record and OIM User, then the OIM User is deleted.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the resource object attribute, which is the key field for reconciliation matching
- **Decode:** Primary key column name used in the reconciliation query for performing delete user reconciliation

[Table A–14](#) lists the default entry in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify values of the existing Code Key and Decode values.

Table A–14 *Entries in the Lookup.DBUM.DB2.TrustedRecon.Delete.Mapping Lookup Definition*

Code Key	Decode
User Login	GRANTEE

A.1.21 Lookup.DBUM.DB2.TrustedRecon.ExclusionList

The Lookup.DBUM.DB2.TrustedRecon.ExclusionList lookup definition holds user attributes of target system accounts that must not be reconciled during trusted source reconciliation.

The following is the format of the Code Key and Decode values for this lookup definition:

- **Code Key:** Resource object field name
- **Decode:** Resource object field values separated by the tilde (~) character

Table A–15 lists the default entry in this lookup definition.

See Also: [Section 3.1.3, "Setting Up the ExclusionList Lookup Definition"](#) for information about adding or modifying entries in this lookup definition

Table A–15 *Entries in the Lookup.DBUM.DB2.TrustedRecon.ExclusionList Lookup Definition*

Code Key	Decode
User Login	db2admin

A.1.22 Lookup.DBUM.DB2.TrustedRecon.Mapping

The Lookup.DBUM.DB2.TrustedRecon.Mapping lookup definition maps the fields of the OIM User form with corresponding column names used in the reconciliation query. This lookup definition is used for performing trusted source reconciliation.

In this lookup definition, the Code Key contains names of the fields on the OIM User form. The Decode value can be in one of the following formats:

- COL_NAME or COL_NAME_ALIAS

In this format, *COL_NAME* is the target system column name used in the reconciliation query. *COL_NAME_ALIAS* is the alias of the target system column name used in the reconciliation query.

You use this format if the target system contains a column corresponding to the resource object attribute.

For example, consider the User Login attribute on the resource object. The target system contains GRANTEE, which is a column corresponding to the User Login attribute. Therefore, the mapping is as follows:

Code Key: User Login

Decode: GRANTEE

- *CONSTANT~CONSTANT_VALUE*

In this format:

- *CONSTANT* specifies that the data in this column is constant.
- *CONSTANT_VALUE* is the value to be displayed in the corresponding field of the OIM User form in the Administrative and User Console.

You use this format if you want to set a constant value for a particular field on the OIM User form.

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 *CONSTANT~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.

By default, in this lookup definition, the Decode values for the Employee Type, Organization, and User Type Code Key columns have been set to constant values Full-Time, Xellerate Users, and End-User, respectively. However, depending on your requirement, you can change these values to one of the following:

- For the Employee Type Code Key, you can set one of the following constant values:
 - Full-Time
 - Part-Time
 - Temp
 - Intern
 - Consultant
- For the Organization Code Key, you can set one of the following constant values:
 - Xellerate Users
 - Requests
- For the User Type Code Key, you can set one of the following constant values:
 - End-User
 - End-User Administrator

- *COLUMN_NAME~LOOKUP_NAME*

In this format:

- *COLUMN_NAME* is the target system column name from which value is fetched.
- *LOOKUP_NAME* is the name of the lookup definition that maps values fetched from the target system with values to be displayed in the OIM User form field.

You use this format if you want values fetched from the target system to be displayed in a format that is accepted by Oracle Identity Manager. By default, the Lookup.DBUM.DB2.TrustedRecon.Mapping lookup definition does not contain any entry in this format. See [Section A.3.25](#),

["Lookup.DBUM.Oracle.TrustedRecon.Mapping"](#) for an example on using this format.

You can add to or remove entries in the `Lookup.DBUM.DB2.TrustedRecon.Mapping` lookup definition. See [Section 4.2, "Adding or Removing Attributes for Reconciliation"](#) for information about adding or modifying entries in this lookup definition.

[Table A-16](#) lists the default entries in this lookup definition.

Table A-16 *Entries in the Lookup.DBUM.DB2.TrustedRecon.Mapping Lookup Definition*

Code Key	Decode
Employee Type	CONSTANT~Full-Time
First Name	GRANTEE
Last Name	GRANTEE
Organization	CONSTANT~Xellerate Users
Status	CONSTANT~Active
User Login	GRANTEE
User Type	CONSTANT~End-User

A.1.23 Lookup.DBUM.DB2.TrustedRecon.QueryFilter

The `Lookup.DBUM.DB2.TrustedRecon.QueryFilter` lookup definition is used for configuring limited reconciliation if your target system is configured as a trusted source. This lookup definition holds information about the filter parameters that you want to use while running the SQL query for trusted source reconciliation.

The `Lookup.DBUM.DB2.TargetRecon.QueryFilter` lookup definition is empty by default.

See [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#) for information about adding entries to this lookup definition.

A.1.24 Lookup.DBUM.DB2.TrustedRecon.Transformation

The `Lookup.DBUM.DB2.TrustedRecon.Transformation` lookup definition is used to configure transformation of attribute values that are fetched from the target system during trusted source reconciliation.

The `Lookup.DBUM.DB2.TrustedRecon.Transformation` lookup definition is empty by default.

See [Section 4.9, "Configuring Transformation of Data During Reconciliation"](#) for information about adding entries to this lookup definition.

A.1.25 Lookup.DBUM.DB2.TrustedRecon.Validation

The `Lookup.DBUM.DB2.TrustedRecon.Validation` lookup definition is used to configure validation of attribute values that are fetched from the target system during trusted source reconciliation.

The `Lookup.DBUM.DB2.TrustedRecon.Validation` lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.1.26 Lookup.DBUM.DB2.UserType

During a provisioning operation, you use the Lookup.DBUM.DB2.UserType lookup definition to specify a value for the User Type field. A value of GROUP specifies that the account being created is a group account. A value of USER specifies that the account being created is a user account.

Table A-17 lists the default entries in this lookup definition.

Table A-17 Entries in the Lookup.DBUM.DB2.UserType Lookup Definition

Code Key	Decode
GROUP	GROUP
USER	USER

A.1.27 Lookup.DBUM.DB2.WithGrantOption

During a provisioning operation, you use this lookup definition to specify whether target system user record being created has the option to grant tablespaces or schemas for other user records.

Note: You cannot add or modify entries in this lookup definition.

Table A-18 lists the default entry in this lookup definition.

Table A-18 Entries in the Lookup.DBUM.DB2.WithGrantOption Lookup Definition

Code Key	Decode
WITH GRANT OPTION	WITH GRANT OPTION

A.2 Lookup Definitions for Microsoft SQL Server

This section provides information about the following lookup definitions

- Section A.2.1, "Lookup.DBUM.MSSQL.AuthType"
- Section A.2.2, "Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateLogin"
- Section A.2.3, "Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateUser"
- Section A.2.4, "Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteLogin"
- Section A.2.5, "Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteUser"
- Section A.2.6, "Lookup.DBUM.MSSQL.AuthType.KeyMapping.DisableLogin"
- Section A.2.7, "Lookup.DBUM.MSSQL.AuthType.KeyMapping.EnableLogin"
- Section A.2.8, "Lookup.DBUM.MSSQL.Configuration"
- Section A.2.9, "Lookup.DBUM.MSSQL.Error.Mapping"
- Section A.2.10, "Lookup.DBUM.MSSQL.ExclusionList"
- Section A.2.11, "Lookup.DBUM.MSSQL.Parameter.Configuration"
- Section A.2.12, "Lookup.DBUM.MSSQL.Provisioning.Validation"
- Section A.2.13, "Lookup.DBUM.MSSQL.Query.Configuration"
- Section A.2.14, "Lookup.DBUM.MSSQL.TargetRecon.Auth.Mapping"

- [Section A.2.15, "Lookup.DBUM.MSSQL.TargetRecon.Delete.Login.Mapping"](#)
- [Section A.2.16, "Lookup.DBUM.MSSQL.TargetRecon.Delete.User.Mapping"](#)
- [Section A.2.17, "Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping"](#)
- [Section A.2.18, "Lookup.DBUM.MSSQL.TargetRecon.Login.Transformation"](#)
- [Section A.2.19, "Lookup.DBUM.MSSQL.TargetRecon.Login.Validation"](#)
- [Section A.2.20, "Lookup.DBUM.MSSQL.TargetRecon.QueryFilter"](#)
- [Section A.2.21, "Lookup.DBUM.MSSQL.TargetRecon.Role.Mapping"](#)
- [Section A.2.22, "Lookup.DBUM.MSSQL.TargetRecon.User.Mapping"](#)
- [Section A.2.23, "Lookup.DBUM.MSSQL.TargetRecon.User.Transformation"](#)
- [Section A.2.24, "Lookup.DBUM.MSSQL.TrustedRecon.Configuration"](#)
- [Section A.2.25, "Lookup.DBUM.MSSQL.TrustedRecon.Delete.Mapping"](#)
- [Section A.2.26, "Lookup.DBUM.MSSQL.TrustedRecon.ExclusionList"](#)
- [Section A.2.27, "Lookup.DBUM.MSSQL.TrustedRecon.Mapping"](#)
- [Section A.2.28, "Lookup.DBUM.MSSQL.TrustedRecon.QueryFilter"](#)
- [Section A.2.29, "Lookup.DBUM.MSSQL.TrustedRecon.Transformation"](#)
- [Section A.2.30, "Lookup.DBUM.MSSQL.TrustedRecon.Validation"](#)

A.2.1 Lookup.DBUM.MSSQL.AuthType

In Microsoft SQL server, you can create an account (login or user) that uses either Windows authentication or SQL server authentication.

The Lookup.DBUM.MSSQL.AuthType lookup definition holds information about authentication types that you can select for a target system account (login or user) that you create through Oracle Identity Manager.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Type of authentication
- **Decode:** Description of the type of authentication

[Table A-19](#) lists the default entries in this lookup definition.

Table A-19 Entries in the Lookup.DBUM.MSSQL.AuthType Lookup Definition

Code Key	Decode
SQL_SERVER_AUTHENTICATION	SQL_SERVER_AUTHENTICATION
WINDOWS_AUTHENTICATION	WINDOWS_AUTHENTICATION

A.2.2 Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateLogin

The Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateLogin lookup definition holds mapping between authentication types and stored procedure names used for creating login entities.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Type of authentication

- **Decode:** Stored procedure name used to create the login entity or combination of stored procedure names separated by a tilde (~) character.

Table A–20 lists the default entries in this lookup definition.

Table A–20 Entries in the Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateLogin Lookup Definition

Code Key	Decode
SQL_SERVER_AUTHENTICATION	MSSQL_CREATE_SQLAUTHTYPE_LOGIN
WINDOWS_AUTHENTICATION	MSSQL_CREATE_WINDOWSAUTHTYPE_LOGIN~ MSSQL_GRANT_WINAUTHTYPE_DEFAULTDB~M SSQL_GRANT_WINAUTHTYPE_DEFAULTLANG

The following scenario illustrates how to add entries to this lookup definition.

Suppose you want to add an entry for creating a login entity that uses Windows authentication. Therefore, in the Code Key column, you enter WINDOWS_AUTHENTICATION, which is the authentication type for the login entity.

In the Decode column, enter the name of the stored procedure that is used for creating the login entity. If more than one stored procedure is required to create the login entity, then enter the names of all those stored procedures separated by a tilde (~) character. In this scenario, creating a login entity requires running three stored procedures. Therefore, enter MSSQL_CREATE_WINDOWSAUTHTYPE_LOGIN~MSSQL_GRANT_WINAUTHTYPE_DEFAULTDB~MSSQL_GRANT_WINAUTHTYPE_DEFAULTLANG as the value of the Decode column.

In the Decode column:

- MSSQL_CREATE_WINDOWSAUTHTYPE_LOGIN is the name of the stored procedure that creates the login.
- MSSQL_GRANT_WINAUTHTYPE_DEFAULTDB is the name of the stored procedure that sets the default database for the login when the login is added to the Microsoft SQL Server.
- MSSQL_GRANT_WINAUTHTYPE_DEFAULTLANG is the name of the stored procedure that sets the default language for the login when the login is added to the Microsoft SQL Server.

A.2.3 Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateUser

The Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateUser lookup definition holds mapping between authentication types and stored procedure names used for creating user entities.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Type of authentication
- **Decode:** Corresponding stored procedure name used to create the user entity

Table A–21 lists the default entries in this lookup definition.

Table A–21 Entries in the *Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateUser* Lookup Definition

Code Key	Decode
SQL_SERVER_AUTHENTICATION	MSSQL_CREATE_SQLAUTHTYPE_USER
WINDOWS_AUTHENTICATION	MSSQL_CREATE_WINDOWSAUTHTYPE_USER

A.2.4 Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteLogin

The Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteLogin lookup definition holds mapping between authentication types and stored procedure names used for deleting login entities from Microsoft SQL Server.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Type of authentication
- **Decode:** Corresponding stored procedure name used to delete the login entity

[Table A–22](#) lists the default entries in this lookup definition.

Table A–22 Entries in the *Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteLogin* Lookup Definition

Code Key	Decode
SQL_SERVER_AUTHENTICATION	MSSQL_DELETE_SQLAUTHTYPE_LOGIN
WINDOWS_AUTHENTICATION	MSSQL_DELETE_WINDOWSAUTHTYPE_LOGIN

A.2.5 Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteUser

The Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteUser lookup definition holds mapping between authentication types and stored procedure names used for deleting user entities from Microsoft SQL Server.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Type of authentication
- **Decode:** Corresponding stored procedure name used to delete the user entity

[Table A–23](#) lists the default entries in this lookup definition.

Table A–23 Entries in the *Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteUser* Lookup Definition

Code Key	Decode
SQL_SERVER_AUTHENTICATION	MSSQL_DELETE_SQLAUTHTYPE_USER
WINDOWS_AUTHENTICATION	MSSQL_DELETE_WINDOWSAUTHTYPE_USER

A.2.6 Lookup.DBUM.MSSQL.AuthType.KeyMapping.DisableLogin

The Lookup.DBUM.MSSQL.AuthType.KeyMapping.DisableLogin lookup definition holds mapping between authentication types and stored procedure names used to disable login entities in Microsoft SQL Server.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Type of authentication
- **Decode:** Corresponding stored procedure name used to disable the login entity

Table A-24 lists the default entries in this lookup definition.

Table A-24 *Entries in the Lookup.DBUM.MSSQL.AuthType.KeyMapping.DisableLogin Lookup Definition*

Code Key	Decode
SQL_SERVER_AUTHENTICATION	MSSQL_DISABLE_SQL_LOGIN
WINDOWS_AUTHENTICATION	MSSQL_DISABLE_WINDOWS_LOGIN

A.2.7 Lookup.DBUM.MSSQL.AuthType.KeyMapping.EnableLogin

The Lookup.DBUM.MSSQL.AuthType.KeyMapping.EnableLogin lookup definition holds mapping between authentication types and stored procedure names used to enable login entities in Microsoft SQL Server.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Type of authentication
- **Decode:** Corresponding stored procedure name used to enable the login entity

Table A-25 lists the default entries in this lookup definition.

Table A-25 *Entries in the Lookup.DBUM.MSSQL.AuthType.KeyMapping.EnableLogin Lookup Definition*

Code Key	Decode
SQL_SERVER_AUTHENTICATION	MSSQL_ENABLE_SQL_LOGIN
WINDOWS_AUTHENTICATION	MSSQL_ENABLE_WINDOWS_LOGIN

A.2.8 Lookup.DBUM.MSSQL.Configuration

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

Note: You cannot add entries to this lookup definition. However, you can modify the Decode values of the existing entries.

Table A-26 lists the default entries in this lookup definition.

Table A–26 Entries in the *Lookup.DBUM.MSSQL.Configuration* Lookup Definition

Code Key	Decode	Description
AuthType QueryCodeKey Mapping Lookup For CreateLogin	Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateLogin	See Section A.2.2 , "Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateLogin" for information about this lookup definition.
AuthType QueryCodeKey Mapping Lookup For CreateUser	Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateUser	See Section A.2.3 , "Lookup.DBUM.MSSQL.AuthType.KeyMapping.CreateUser" for information about this lookup definition.
AuthType QueryCodeKey Mapping Lookup For DeleteLogin	Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteLogin	See Section A.2.4 , "Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteLogin" for information about this lookup definition.
AuthType QueryCodeKey Mapping Lookup For DeleteUser	Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteUser	See Section A.2.5 , "Lookup.DBUM.MSSQL.AuthType.KeyMapping.DeleteUser" for information about this lookup definition.
AuthType QueryCodeKey Mapping Lookup For DisableLogin	Lookup.DBUM.MSSQL.AuthType.KeyMapping.DisableLogin	See Section A.2.6 , "Lookup.DBUM.MSSQL.AuthType.KeyMapping.DisableLogin" for information about this lookup definition.
AuthType QueryCodeKey Mapping Lookup For EnableLogin	Lookup.DBUM.MSSQL.AuthType.KeyMapping.EnableLogin	See Section A.2.7 , "Lookup.DBUM.MSSQL.AuthType.KeyMapping.EnableLogin" for information about this lookup definition.
Error Mapping Lookup	Lookup.DBUM.MSSQL.Error.Mapping	See Section A.2.9 , "Lookup.DBUM.MSSQL.Error.Mapping" for information about this lookup definition.
Parameter Configuration Lookup	Lookup.DBUM.MSSQL.Parameter.Configuration	See Section A.2.11 , "Lookup.DBUM.MSSQL.Parameter.Configuration" for information about this lookup definition.
Provisioning Validation Lookup	Lookup.DBUM.MSSQL.Provisioning.Validation	See Section A.2.12 , "Lookup.DBUM.MSSQL.Provisioning.Validation" for information about this lookup definition.
Query Configuration Lookup	Lookup.DBUM.MSSQL.Query.Configuration	See Section A.2.13 , "Lookup.DBUM.MSSQL.Query.Configuration" for information about this lookup definition.
Reconciliation Class Name	oracle.iam.connectors.dbum.tasks.impl.DBUMSQLServerReconciliationImpl	Name of the class that implements the logic for target resource reconciliation.
Reconciliation Query Property File	Enter a value	Enter the full path and name of the file containing queries that must be run during reconciliation.
Reconciliation SQL Injection Keywords	NODATA	Enter the SQL keywords (separated by a tilde (~) character) that must not be used in the reconciliation query. The connector does not run a query (used for target resource reconciliation) that contains any of the keywords listed in the Decode column.

Table A–26 (Cont.) Entries in the Lookup.DBUM.MSSQL.Configuration Lookup Definition

Code Key	Decode	Description
Reserved Words List	NODATA	List of reserve words that are not supported in the OIM User process form fields during provisioning operations.
Resource Exclusion Column Key	UD_DB_SQL_L_LOGIN	Name of the process form field that is excluded during provisioning operations.
Resource Exclusion List Lookup	Lookup.DBUM.MSSQL.ExclusionList	See for more information about this lookup definition.
Status Reconciliation Class Name	NODATA	You must enter a value for this entry only if your target system does not contain a column from which you can retrieve the status of a target system account. In Microsoft SQL server, the <code>is_disabled</code> column holds the status of the target system account. Therefore, <i>do not</i> enter any value for this entry.
Target Date Format	NODATA	Enter the format in which date values are stored on the target system.
Unsupported Special Characters	NODATA	Enter the list of special characters that are not supported in the process form fields during provisioning operations.
Use Status Reconciliation	No	Specifies whether you want to run reconciliation for the status of a target system user account. Note: Do not change the value of this entry.
Use Validation For Provisioning	No	Specifies whether you want to enable validation of user attributes during provisioning operations. See Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning" for information about configuring data validation during provisioning operations.

A.2.9 Lookup.DBUM.MSSQL.Error.Mapping

When an error is encountered during a provisioning operation, an error message is displayed on the Administrative and User Console.

The Lookup.DBUM.MSSQL.Error.Mapping lookup definition maps error codes displayed by the database with error messages that must be displayed on the OIM User process form during provisioning operations.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** SQL error code returned by the database
- **Decode:** Corresponding error message to be displayed on the OIM User process form

To add or modify entries in this lookup definition, you must enter values in the format specified in the preceding paragraph.

[Table A–27](#) lists the default entries in this lookup definition.

Table A–27 Entries in the *Lookup.DBUM.MSSQL.Error.Mapping* Lookup Definition

Code Key	Decode
102	INCORRECT_SYNTAX
900	INVALID_SQL
15006	INVALID_CHARACTERS
15023	USER_ALREADY_EXIST
15025	LOGIN_ALREADY_EXIST
15118	PASSWORD_POLICY_NOT_MATCH
15247	PERMISSION_DENIED
15407	INVALID_WINDOWS_NAME

A.2.10 Lookup.DBUM.MSSQL.ExclusionList

The Lookup.DBUM.MSSQL.ExclusionList lookup definition holds user attributes of the target system accounts for which you do not want to perform target resource reconciliation and provisioning.

For target system accounts on which you do not want to perform provisioning operations, the following is the format of the Code Key and Decode values:

- **Code Key:** Name of the process form field
- **Decode:** Process form field values separated by the tilde (~) character

For target system accounts that must not be reconciled during a target resource reconciliation run, the following is the format of the Code Key and Decode values:

- **Code Key:** Resource object field name
- **Decode:** Resource object field values separated by the tilde (~) character

Table A–28 lists the default entry in this lookup definition.

See Also: [Section 3.1.3, "Setting Up the ExclusionList Lookup Definition"](#) for information about adding or modifying entries in this lookup definition

Table A–28 Entries in the *Lookup.DBUM.MSSQL.ExclusionList* Lookup Definition

Code Key	Decode
UD_DB_SQL_L_LOGIN	sa
Login Name	sa
User Name	sa

A.2.11 Lookup.DBUM.MSSQL.Parameter.Configuration

The Lookup.DBUM.MSSQL.Parameter.Configuration lookup definition maps identifiers of stored procedures and SQL statements (defined in the Lookup.DBUM.MSSQL.Query.Configuration lookup definition) with names of the process form fields.

This connector uses stored procedures and SQL statements to perform provisioning operations. The data that you enter on the process form while performing provisioning operations are stored in the corresponding process form fields in the Design Console.

The process form field is mapped to the identifiers of stored procedures or SQL statements that are defined in the Lookup.DBUM.MSSQL.Query.Configuration lookup definition.

See Also: [Section A.2.13, "Lookup.DBUM.MSSQL.Query.Configuration"](#) for more information about the Lookup.DBUM.MSSQL.Query.Configuration lookup definition

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Identifier in the stored procedure or SQL statement used for provisioning operations
- **Decode:** Combination of the following elements separated by the tilde (~) character:

PF_FIELD_NAME~PF_DATA_TYPE~PARAMETER_TYPE~QUOTE_TYPE~EXCLUDE_VALIDATION~UPPERCASE

Note: The sequence of elements in this format must not be changed

In this format:

- *PF_FIELD_NAME* is process form field name
- *PF_DATA_TYPE* is process form field data type
- *PARAMETER_TYPE* specifies whether the value in the process form field is of type input or output.

If the value in the process form field is used as an input parameter, for example, as an input to a variable in the SQL statement, then use IN. Otherwise, use OUT.

- *QUOTE_TYPE* specifies whether the value from the process form field that is passed to the SQL statement must be enclosed in a single quotation mark or double quotation mark. The *QUOTE_TYPE* element is optional.

If you want the value in the process form field to be enclosed in single quotation marks, then use SINGLE_QUOTE. If you want the value in the process form field to be enclosed in double quotation marks, then use DOUBLE_QUOTE.

- EXCLUDE_VALIDATION is an optional element. It is used in the following scenario:

Suppose you specify values for the Reserved Words List or Unsupported Special Characters entries of the Lookup.DBUM.MSSQL.Configuration lookup definition. During provisioning operations, the connector checks whether the OIM User process form fields contain any of the values specified in the Reserved Words List or Unsupported Special Characters entries. If such values are found, then no provisioning operations are performed on that record. If you do not want the connector to perform this check on a particular field on the OIM User process form, then include EXCLUDE_VALIDATION along with the name of that process form field.

For example, the

UD_DB_SQL_L_LOGIN~varchar2~IN~DOUBLE_QUOTE~EXCLUDE_VALI

DATION Decode values specifies that during a particular provisioning operation, the connector does not check whether the Login Name field contains any of the values specified in the Reserved Words List or Unsupported Special Characters entries of the Lookup.DBUM.MSSQL.Configuration lookup definition.

- UPPERCASE element is an optional element. You use this element if you want to save on the target system the value entered in the process form field in upper case.

Table A-29 lists the default entries in this lookup definition.

Table A-29 Entries in the Lookup.DBUM.MSSQL.Parameter.Configuration Lookup Definition

Code Key	Decode
mssql_dbdefaultlang	UD_DB_SQL_L_DEFLANG~varchar2~IN~EXCLUDE_VALIDATION
mssql_dbname	UD_DB_SQL_L_DEFDB~varchar2~IN~EXCLUDE_VALIDATION
mssql_login	UD_DB_SQL_L_LOGIN~varchar2~IN
mssql_parent_login	UD_DB_SQL_U_LOGINNAME~varchar2~IN
mssql_pass	UD_DB_SQL_L_PASSWORD~varchar2~IN
mssql_role	UD_DB_SQL_R_ROLE~varchar2~IN~EXCLUDE_VALIDATION
mssql_user_id	UD_DB_SQL_U_USERNAME~varchar2~IN
mssql_win_login	UD_DB_SQL_L_LOGIN~varchar2~IN~DOUBLE_QUOTE~EXCLUDE_VALIDATION

A.2.12 Lookup.DBUM.MSSQL.Provisioning.Validation

The Lookup.DBUM.MSSQL.Provisioning.Validation lookup definition is used to store the mapping between the attribute for which validation has to be applied and the validation implementation class.

The Lookup.DBUM.MSSQL.Provisioning.Validation lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.2.13 Lookup.DBUM.MSSQL.Query.Configuration

As mentioned in one of the sections in this chapter, this connector uses stored procedures and SQL statements to perform provisioning operations.

The Lookup.DBUM.MSSQL.Query.Configuration lookup definition contains stored procedures and SQL statements that are used to perform provisioning operations.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the stored procedure or SQL statement
- **Decode:** Corresponding stored procedure or SQL statement

Depending on the provisioning operations that you are performing, adapters run the appropriate stored procedures or SQL statements on the target system.

Table A-30 lists the default entries in this lookup definition.

Table A-30 Entries in the *Lookup.DBUM.MSSQL.Query.Configuration Lookup Definition*

Code Key	Decode
MSSQL_ADD_ROLE	{CALL sp_addrolemember(:mssql_role,:mssql_user_id)}
MSSQL_CREATE_SQLAUTHTYPE_LOGIN	{CALL sp_addlogin(:mssql_login,:mssql_pass,:mssql_dbname,:mssql_dbdefaultlang)}
MSSQL_CREATE_SQLAUTHTYPE_USER	{CALL sp_adduser(:mssql_parent_login,:mssql_user_id,null)}
MSSQL_CREATE_WINDOWSAUTHTYPE_LOGIN	{CALL sp_grantlogin(:mssql_login)}
MSSQL_CREATE_WINDOWSAUTHTYPE_USER	{CALL sp_grantdbaccess(:mssql_parent_login,:mssql_user_id)}
MSSQL_DELETE_ROLE	{CALL sp_droprolemember(:mssql_role,:mssql_user_id)}
MSSQL_DELETE_SQLAUTHTYPE_LOGIN	{CALL sp_droplogin(:mssql_login)}
MSSQL_DELETE_SQLAUTHTYPE_USER	{CALL sp_dropuser(:mssql_user_id)}
MSSQL_DELETE_WINDOWSAUTHTYPE_LOGIN	{CALL sp_revokelogin(:mssql_login)}
MSSQL_DELETE_WINDOWSAUTHTYPE_USER	{CALL sp_revokedbaccess(:mssql_user_id)}
MSSQL_DISABLE_SQL_LOGIN	ALTER LOGIN :mssql_login DISABLE
MSSQL_DISABLE_WINDOWSAUTH_LOGIN	ALTER LOGIN :mssql_win_login DISABLE
MSSQL_ENABLE_SQL_LOGIN	ALTER LOGIN :mssql_login ENABLE
MSSQL_ENABLE_WINDOWSAUTH_LOGIN	ALTER LOGIN :mssql_win_login ENABLE
MSSQL_GRANT_WINAUTHTYPE_DEFAULTDB	{CALL sp_defaultdb(:mssql_login,:mssql_dbname)}
MSSQL_GRANT_WINAUTHTYPE_DEFAULTLANG	{CALL sp_defaultlanguage(:mssql_login,:mssql_dbdefaultlang)}
MSSQL_UPDATE_DEFAULTTDB	{CALL sp_defaultdb(:mssql_login,:mssql_dbname)}
MSSQL_UPDATE_DEFAULTTLANG	{CALL sp_defaultlanguage(:mssql_login,:mssql_dbdefaultlang)}
MSSQL_UPDATE_LOGIN_PASSWORD	{call sp_password(null,:mssql_pass,:mssql_login)}

A.2.14 Lookup.DBUM.MSSQL.TargetRecon.Auth.Mapping

The Lookup.DBUM.MSSQL.TargetRecon.Auth.Mapping lookup definition maps authentication types on the target system with corresponding values to be displayed in the User Type field of the OIM User process form. This lookup definition is used during target resource reconciliation.

During reconciliation, this connector fetches values such as WINDOWS_LOGIN or SQL_LOGIN from the type_desc target system column. A value of WINDOWS_LOGIN means that the target system account uses Windows

authentication. A value of `SQL_LOGIN` means that the target system account uses SQL Server authentication.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Value in the `type_desc` target system column
- **Decode:** Corresponding value to be displayed in the User Type process form field

To add or modify entries in this lookup definition, you must enter values in the format specified in the preceding paragraph.

[Table A-12](#) lists the entries in this lookup definition.

Table A-31 *Entries in the Lookup.DBUM.MSSQL.TargetRecon.Auth.Mapping Lookup Definition*

Code Key	Decode
SQL_LOGIN	SQL_SERVER_AUTHENTICATION
WINDOWS_LOGIN	WINDOWS_AUTHENTICATION

A.2.15 Lookup.DBUM.MSSQL.TargetRecon.Delete.Login.Mapping

The Lookup.DBUM.MSSQL.TargetRecon.Delete.Login.Mapping lookup definition maps the resource object attribute with the primary key column name used in the reconciliation query. Note that this resource object attribute is the key field for reconciliation matching.

The Lookup.DBUM.MSSQL.TargetRecon.Delete.Login.Mapping lookup definition is used during delete login target reconciliation runs.

During a delete login reconciliation run, the resource object field that you specify in this lookup definition is used for comparing target system login entity records with existing target system resource assigned to OIM Users. During this comparison process, if no match is found between the target system login entity record and the resource provisioned to the OIM User, then the database user resource is revoked from the OIM User.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the resource object attribute, which is the key field for reconciliation matching
- **Decode:** Primary key column name used in the reconciliation query for performing delete user reconciliation

[Table A-32](#) lists the default entry in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify values of the existing Code Key and Decode values.

Table A-32 *Entries in the Lookup.DBUM.MSSQL.TargetRecon.Delete.Login.Mapping Lookup Definition*

Code Key	Decode
Login Name	LoginName

A.2.16 Lookup.DBUM.MSSQL.TargetRecon.Delete.User.Mapping

The Lookup.DBUM.MSSQL.TargetRecon.Delete.User.Mapping lookup definition maps the resource object attribute with the primary key column name used in the reconciliation query. Note that this resource object attribute is the key field for reconciliation matching.

The Lookup.DBUM.MSSQL.TargetRecon.Delete.User.Mapping lookup definition is used during delete user target reconciliation runs.

During a delete user reconciliation run, the resource object field that you specify in this lookup definition is used for comparing target system user entity records with existing target system resource assigned to OIM Users. During this comparison process, if no match is found between the target system user entity record and the resource provisioned to the OIM User, then the database user resource is revoked from the OIM User.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the resource object attribute, which is the key field for reconciliation matching
- **Decode:** Primary key column name used in the reconciliation query for performing delete user reconciliation

Table A-33 lists the default entry in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify values of the existing Code Key and Decode values.

Table A-33 Entries in the Lookup.DBUM.MSSQL.TargetRecon.Delete.User.Mapping Lookup Definition

Code Key	Decode
User Name	UserName

A.2.17 Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping

The Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping lookup definition maps resource object attributes with column names used in the stored procedure or SQL query for reconciliation. This lookup definition is used for performing target resource login reconciliation runs.

In this lookup definition, the Code Key contains the reconciliation attribute of the resource object.

For Code Key columns that store single-valued attributes, the Decode value can be in one of the following formats:

- COL_NAME or COL_NAME_ALIAS

In this format, COL_NAME is the target system column name used in the reconciliation query. COL_NAME_ALIAS is the alias of the target system column names used in the reconciliation query.

You use this format if the target system contains a column corresponding to the resource object attribute.

For example, consider the Login Name attribute, which is a single-valued attribute on the resource object. The target system contains LoginName, which is a column corresponding to the Login Name attribute. Therefore, the mapping is as follows:

Code Key: Login Name

Decode: LoginName

- *CONSTANT~CONSTANT_VALUE*

In this format, *CONSTANT* specifies that the data in this column is constant. *CONSTANT_VALUE* is the value to be displayed in the corresponding field of the OIM User form in the Administrative and User Console.

You use this format if you want to set a constant value for a particular field on the OIM User form.

For example, consider the Password attribute of the resource object. The Decode value of this attribute is set to *CONSTANT~Dummy*. This implies that the Password field on the OIM User form displays Dummy for all records reconciled from the target system.

- *COLUMN_NAME~LOOKUP_NAME*

In this format, *COLUMN_NAME* is the target system column name from which value is fetched. *LOOKUP_NAME* is the name of the lookup definition that maps values fetched from the target system with values to be displayed in the OIM User form field.

You use this format if you want values fetched from the target system to be displayed in a format that is accepted by Oracle Identity Manager.

For example, consider the Authentication Type attribute of the resource object. This is a single valued attribute. The target system contains type_desc, which is a column corresponding to the Authentication Type attribute of the resource object. However, we do not map the Authentication Type resource object attribute to the type_desc column for the following reason:

The type_desc column stores values such as SQL_LOGIN and WINDOWS_LOGIN. Therefore, during reconciliation, this connector fetches values such as SQL_LOGIN or WINDOWS_LOGIN from the type_desc target system column. However, these values cannot be displayed in the Authentication Type field of the OIM User form. This is because Oracle Identity Manager accepts only one of the following values as the authentication type of an account:

- SQL_SERVER_AUTHENTICATION
- WINDOWS_AUTHENTICATION

Therefore, in order to display the value retrieved from the type_desc column in a format that is accepted by Oracle Identity Manager, the Authentication Type attribute of the resource object has been mapped to `TYPE_DESC~Lookup.DBUM.MSSQL.TargetRecon.Auth.Mapping`.

This implies that in the Code Key column of the `Lookup.DBUM.MSSQL.TargetRecon.Auth.Mapping` lookup definition, the connector searches for the value that is fetched from the type_desc column of the target system. Then, the corresponding Decode value is displayed as the type of the user account in Oracle Identity Manager. This is illustrated by the following example:

Suppose the value fetched from the type_desc column for a particular user account on the target system is WINDOWS_LOGIN. In the Code Key column of the

Lookup.DBUM.MSSQL.TargetRecon.Auth.Mapping lookup definition, the connector searches for the value WINDOWS_LOGIN. The Decode value of the WINDOWS_LOGIN Code Key is WINDOWS_AUTHENTICATION. Therefore, in Oracle Identity Manager, the connector displays WINDOWS_AUTHENTICATION as the values of the Authentication Type field.

See Also: [Section A.1.17, "Lookup.DBUM.DB2.TargetRecon.UserTypeMapping"](#)

■ LOOKUP~COL_NAME

In this format:

- LOOKUP specifies that the data retrieved from the target system is lookup data.
- COL_NAME is the corresponding column name or column name alias used in the reconciliation query

You use this format if process form field corresponding to the Code Key value is a lookup type field.

For Code Key columns that store multivalued attributes, the Decode value is specified in the following format:

CHILD~MULTIVALUED_ATTR_CONFIG_LOOKUP

In this format:

- CHILD specifies that the data in this column is the child attribute data
- MULTIVALUED_ATTR_CONFIG_LOOKUP is name of the lookup definition that holds configurable entries for the multivalued attribute.

By default, the Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping lookup definition does not contain an entry for this format. See [Section A.3.11, "Lookup.DBUM.Oracle.TargetRecon.Mapping"](#) for an example on using this format.

You can add or remove entries in the Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping lookup definition. See [Section 4.2, "Adding or Removing Attributes for Reconciliation"](#) for information about adding or modifying entries in this lookup definition.

[Table A-34](#) lists the default entries in this lookup definition.

Table A-34 Entries in the Lookup.DBUM.MSSQL.TargetRecon.Login.Mapping Lookup Definition

Code Key	Decode
Authentication Type	TYPE_DESC~Lookup.DBUM.MSSQL.TargetRecon.Auth.Mapping
Default Database Name	DefDBName
Default Language	DefLangName
Login Name	LoginName
Password	Constant~Dummy
Status	IS_DISABLED~Lookup.DBUM.TargetRecon.StatusMapping

A.2.18 Lookup.DBUM.MSSQL.TargetRecon.Login.Transformation

The Lookup.DBUM.MSSQL.TargetRecon.Login.Transformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during target resource reconciliation of login entities.

The Lookup.DBUM.MSSQL.TargetRecon.Login.Transformation lookup definition is empty by default.

See [Section 4.9, "Configuring Transformation of Data During Reconciliation"](#) for information about adding entries to this lookup definition.

A.2.19 Lookup.DBUM.MSSQL.TargetRecon.Login.Validation

The Lookup.DBUM.MSSQL.TargetRecon.Login.Validation lookup definition is used to configure validation of login entity attribute values that are fetched from the target system during target resource reconciliation.

The Lookup.DBUM.MSSQL.TargetRecon.Login.Validation lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.2.20 Lookup.DBUM.MSSQL.TargetRecon.QueryFilter

The Lookup.DBUM.MSSQL.TargetRecon.QueryFilter lookup definition holds information about the filter parameters that you want to use while running the SQL query for target resource reconciliation.

The Lookup.DBUM.MSSQL.TargetRecon.QueryFilter lookup definition is empty by default.

See [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#) for information about adding entries to this lookup definition.

A.2.21 Lookup.DBUM.MSSQL.TargetRecon.Role.Mapping

The Lookup.DBUM.MSSQL.TargetRecon.Role.Mapping lookup definition holds mapping between the Role multivalued attribute and the corresponding column name used in the stored procedure for target resource reconciliation.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the multivalued attribute
- **Decode:** The value can be specified in one the following formats:

- LOOKUP~COL_NAME

In this format:

- LOOKUP specifies that the data retrieved from the target system is lookup data.
 - COL_NAME is the corresponding column name or column name alias used in the reconciliation query

You use this format if process form field corresponding to the Code Key value is a lookup type field.

- COL_NAME

This is the column name used in the reconciliation query corresponding to the value in the code key column.

If you want to add or modify the entries in this lookup definition, then you must specify values in the format described in this section.

Table A-35 lists the default entry in this lookup definition.

Table A-35 *Entries in the Lookup.DBUM.MSSQL.TargetRecon.Role.Mapping Lookup Definition*

Code Key	Decode
Role	RoleName

A.2.22 Lookup.DBUM.MSSQL.TargetRecon.User.Mapping

The Lookup.DBUM.MSSQL.TargetRecon.User.Mapping lookup definition maps resource object fields with column names used in the stored procedure or SQL query for reconciliation. This lookup definition is used for performing target resource user reconciliation runs.

In this lookup definition, the Code Key contains the reconciliation field of the resource object.

For Code Key columns that store single-valued attributes, the Decode value can be one of the following formats:

- *COL_NAME* or *COL_NAME_ALIAS*

In this format, *COL_NAME* is the target system column name used in the reconciliation query. *COL_NAME_ALIAS* is the alias of the target system column names used in the reconciliation query.

You use this format if the target system contains a column corresponding to the resource object attribute that you added.

- *CONSTANT~CONSTANT_VALUE*

In this format, *CONSTANT* specifies that the data in this column is constant. *CONSTANT_VALUE* is value that you want to be displayed in the corresponding OIM User form field in the Administrative and User Console.

You use this format if you want to display in a particular OIM User form field, a constant value for all records.

- *COLUMN_NAME~LOOKUP_NAME*

In this format, *COLUMN_NAME* is the target system column name from which value is fetched. *LOOKUP_NAME* is the name of the lookup definition that maps values fetched from the target system with values that must be displayed in the OIM User form field.

You use this format if you want to specify the format in which values fetched from the target system must be displayed in the OIM User form field.

- *LOOKUP~COL_NAME*

In this format:

- *LOOKUP* specifies that the data retrieved from the target system is lookup data.
- *COL_NAME* is the corresponding column name or column name alias used in the reconciliation query

You use this format if process form field corresponding to the Code Key value is a lookup type field.

For Code Key columns that store multivalued attributes, the Decode value is specified in the following format:

`CHILD~MULTIVALUED_ATTR_CONFIG_LOOKUP`

In this format:

- `CHILD` specifies that the data in this column is the child attribute data
- `MULTIVALUED_ATTR_CONFIG_LOOKUP` is name of the lookup definition that holds configurable entries for the multivalued attribute.

[Table A-36](#) lists the default entries in this lookup definition, and the descriptions for most of the lookup entries.

Table A-36 Entries in the `Lookup.DBUM.MSSQL.TargetRecon.User.Mapping` Lookup Definition

Code Key	Decode
Authentication Type	SQL_SERVER_AUTHENTICATION
Database Name	DefDBName
Login Name	LoginName
Role List	CHILD~Lookup.DBUM.MSSQL.TargetRecon.Role.Mapping
User Name	UserName

A.2.23 `Lookup.DBUM.MSSQL.TargetRecon.User.Transformation`

The `Lookup.DBUM.MSSQL.TargetRecon.User.Transformation` lookup definition is used to configure transformation of user entity attribute values that are fetched from the target system during target resource reconciliation.

The `Lookup.DBUM.MSSQL.TargetRecon.Login.Transformation` lookup definition is empty by default.

See [Section 4.9, "Configuring Transformation of Data During Reconciliation"](#) for information about adding entries to this lookup definition.

A.2.24 `Lookup.DBUM.MSSQL.TrustedRecon.Configuration`

The `Lookup.DBUM.MSSQL.TrustedRecon.Configuration` lookup definition holds connector configuration entries that are used during trusted source reconciliation.

[Table A-37](#) lists the default entries in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify the Decode values of the existing entries.

Table A–37 Entries in the *Lookup.DBUM.MSSQL.TrustedRecon.Configuration* Lookup Definition

Code Key	Decode	Description
Reconciliation Class Name	oracle.iam.connectors.dbum.tasks.impl.DBUMSQLServerReconciliationImpl	Name of the class that implements the logic for trusted source reconciliation.
Reconciliation Query Property File	Enter a value	Enter the full path and name of the file containing queries that must be run during reconciliation.
Reconciliation SQL Injection Keywords	NODATA	Enter the list of SQL keywords (separated by the tilde (~) character) that must not be used in the reconciliation query. The connector does not run a query (used for trusted source reconciliation) that contains any of the keywords listed in the Decode column.
Resource Exclusion List Lookup	Lookup.DBUM.MSSQL.TrustedRecon.ExclusionList	See Section A.2.26 , "Lookup.DBUM.MSSQL.TrustedRecon.ExclusionList" for more information about this lookup definition.
Status Reconciliation Class Name	NODATA	You must enter a value for this entry only if your target system does not contain a column from which you can retrieve the status of a target system account. In Microsoft SQL server, the <code>is_disabled</code> column holds the status of the target system account. Therefore, <i>do not</i> enter any value for this entry.
Target Date Format	NODATA	Enter the format in which date values are stored on the target system.
Use Status Reconciliation	No	Specifies whether you want to run reconciliation for the status of a target system user account. Note: Do not change the value of this entry.

A.2.25 Lookup.DBUM.MSSQL.TrustedRecon.Delete.Mapping

The Lookup.DBUM.MSSQL.TrustedRecon.Delete.Mapping lookup definition maps the resource object attribute with the primary key column name used in the reconciliation query (for retrieving all login entities from the target system). Note that this resource object attribute is the key field for reconciliation matching.

The Lookup.DBUM.MSSQL.TrustedRecon.Delete.Mapping lookup definition is used during delete login trusted reconciliation runs.

During a delete login reconciliation run, the resource object attribute that you specify in this lookup definition is used for comparing target system accounts with existing OIM Users. During this comparison process, if no match is found between the target system account and OIM User, then the OIM User is deleted.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the resource object attribute, which is the key field for reconciliation matching
- **Decode:** Primary key column name used in the reconciliation query for performing delete login reconciliation

[Table A-38](#) lists the default entry in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify values of the existing Code Key and Decode values.

Table A-38 Entries in the *Lookup.DBUM.MSSQL.TrustedRecon.Delete.Mapping* Lookup Definition

Code Key	Decode
User Login	LoginName

A.2.26 Lookup.DBUM.MSSQL.TrustedRecon.ExclusionList

The Lookup.DBUM.MSSQL.TrustedRecon.ExclusionList lookup definition holds user attributes of target system accounts that must not be reconciled during trusted source reconciliation.

The following is the format of the Code Key and Decode values for this lookup definition:

- **Code Key:** Resource object field name
- **Decode:** Resource object field values separated by the tilde (~) character

[Table A-39](#) lists the default entry in this lookup definition.

See Also: [Section 3.1.3, "Setting Up the ExclusionList Lookup Definition"](#) for information about adding or modifying entries in this lookup definition

Table A-39 Entries in the *Lookup.DBUM.MSSQL.TrustedRecon.ExclusionList* Lookup Definition

Code Key	Decode
User Login	sa

A.2.27 Lookup.DBUM.MSSQL.TrustedRecon.Mapping

The Lookup.DBUM.MSSQL.TrustedRecon.Mapping lookup definition maps the fields of the OIM User form with corresponding column names used in the reconciliation query. This lookup definition is used for performing trusted source reconciliation.

In this lookup definition, the Code Key contains names of the fields on the OIM User form. The Decode value can be in one of the following formats:

- COL_NAME or COL_NAME_ALIAS

In this format, *COL_NAME* is the target system column name used in the reconciliation query. *COL_NAME_ALIAS* is the alias of the target system column name used in the reconciliation query.

You use this format if the target system contains a column corresponding to the resource object attribute.

For example, consider the User Login attribute on the resource object. The target system contains Loginame, which is a column corresponding to the User Login attribute. Therefore, the mapping is as follows:

Code Key: User Login

Decode: Loginame

- *CONSTANT~CONSTANT_VALUE*

In this format:

- *CONSTANT* specifies that the data in this column is constant.
- *CONSTANT_VALUE* is the value to be displayed in the corresponding field of the OIM User form in the Administrative and User Console.

You this format if you want to set a constant value for a particular field on the OIM User form.

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 *CONSTANT~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.

By default, in this lookup definition, the Decode values for the Employee Type, Organization, and User Type Code Key columns have been set to constant values Full-Time, Xellerate Users, and End-User, respectively. However, depending on your requirement, you can change these values to one of the following:

- For the Employee Type Code Key, you can set one of the following constant values:
 - Full-Time
 - Part-Time
 - Temp
 - Intern
 - Consultant
- For the Organization Code Key, you can set one of the following constant values:
 - Xellerate Users
 - Requests
- For the User Type Code Key, you can set one of the following constant values:
 - End-User
 - End-User Administrator

- *COLUMN_NAME~LOOKUP_NAME*

In this format:

- *COLUMN_NAME* is the target system column name from which value is fetched.
- *LOOKUP_NAME* is the name of the lookup definition that maps values fetched from the target system with values to be displayed in the OIM User form field.

You use this format if you want values fetched from the target system to be displayed in a format that is accepted by Oracle Identity Manager.

You can add or remove entries in the Lookup.DBUM.Oracle.TrustedRecon.Mapping lookup definition. See [Section 4.2, "Adding or Removing Attributes for Reconciliation"](#) for more information.

[Table A-40](#) lists the default entries in this lookup definition.

Table A-40 *Entries in the Lookup.DBUM.DB2.TrustedRecon.Mapping Lookup Definition*

Code Key	Decode
Employee Type	CONSTANT~Full-Time
First Name	GRANTEE
Last Name	GRANTEE
Organization	CONSTANT~Xellerate Users
Status	CONSTANT~Active
User Login	GRANTEE
User Type	CONSTANT~End-User

A.2.28 Lookup.DBUM.MSSQL.TrustedRecon.QueryFilter

The Lookup.DBUM.MSSQL.TrustedRecon.QueryFilter lookup definition is used for configuring limited reconciliation if your target system is configured as a trusted source. This lookup definition holds information about the filter parameters that you want to use while running the SQL query or stored procedure for trusted source reconciliation.

The Lookup.DBUM.MSSQL.TargetRecon.QueryFilter lookup definition is empty by default.

See [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#) for information about adding entries to this lookup definition.

A.2.29 Lookup.DBUM.MSSQL.TrustedRecon.Transformation

The Lookup.DBUM.MSSQL.TrustedRecon.Transformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during trusted source reconciliation.

The Lookup.DBUM.MSSQL.TrustedRecon.Transformation lookup definition is empty by default.

See [Section 4.9, "Configuring Transformation of Data During Reconciliation"](#) for information about adding entries to this lookup definition.

A.2.30 Lookup.DBUM.MSSQL.TrustedRecon.Validation

The Lookup.DBUM.MSSQL.TrustedRecon.Validation lookup definition is used to configure validation of attribute values that are fetched from the target system during trusted source reconciliation.

The Lookup.DBUM.MSSQL.TrustedRecon.Validation lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.3 Lookup Definitions for Oracle Database

This section provides information about the following lookup definitions:

- [Section A.3.1, "Lookup.DBUM.Oracle.AuthType"](#)
- [Section A.3.2, "Lookup.DBUM.Oracle.AuthType.KeyMapping.CreateUser"](#)
- [Section A.3.3, "Lookup.DBUM.Oracle.AuthType.KeyMapping.UpdateUser"](#)
- [Section A.3.4, "Lookup.DBUM.Oracle.Configuration"](#)
- [Section A.3.5, "Lookup.DBUM.Oracle.Error.Mapping"](#)
- [Section A.3.6, "Lookup.DBUM.Oracle.ExclusionList"](#)
- [Section A.3.7, "Lookup.DBUM.Oracle.Parameter.Configuration"](#)
- [Section A.3.8, "Lookup.DBUM.Oracle.Provisioning.Validation"](#)
- [Section A.3.9, "Lookup.DBUM.Oracle.Query.Configuration"](#)
- [Section A.3.10, "Lookup.DBUM.Oracle.TargetRecon.Delete.Mapping"](#)
- [Section A.3.11, "Lookup.DBUM.Oracle.TargetRecon.Mapping"](#)
- [Section A.3.12, "Lookup.DBUM.Oracle.TargetRecon.Privilege.Configuration"](#)
- [Section A.3.13, "Lookup.DBUM.Oracle.TargetRecon.Privilege.Mapping"](#)
- [Section A.3.14, "Lookup.DBUM.Oracle.TargetRecon.Privilege.QueryFilter"](#)
- [Section A.3.16, "Lookup.DBUM.Oracle.TargetRecon.Role.Configuration"](#)
- [Section A.3.17, "Lookup.DBUM.Oracle.TargetRecon.Role.Mapping"](#)
- [Section A.3.19, "Lookup.DBUM.Oracle.TargetRecon.Transformation"](#)
- [Section A.3.20, "Lookup.DBUM.Oracle.TargetRecon.Validation"](#)
- [Section A.3.21, "Lookup.DBUM.Oracle.WithAdminOption"](#)
- [Section A.3.22, "Lookup.DBUM.Oracle.TrustedRecon.Configuration"](#)
- [Section A.3.23, "Lookup.DBUM.Oracle.TrustedRecon.Delete.Mapping"](#)
- [Section A.3.24, "Lookup.DBUM.Oracle.TrustedRecon.ExclusionList"](#)
- [Section A.3.25, "Lookup.DBUM.Oracle.TrustedRecon.Mapping"](#)
- [Section A.3.26, "Lookup.DBUM.Oracle.TrustedRecon.QueryFilter"](#)
- [Section A.3.27, "Lookup.DBUM.Oracle.TrustedRecon.Transformation"](#)
- [Section A.3.28, "Lookup.DBUM.Oracle.TrustedRecon.Validation"](#)

A.3.1 Lookup.DBUM.Oracle.AuthType

The Database User Management connector enables you to create user accounts in the target system that can access the database by being authenticated by using a password. In addition, this connector enables you to create global user accounts that can be authenticated by an enterprise directory, and external users that can be authenticated by an external service.

The Lookup.DBUM.Oracle.AuthType lookup definition holds information about authentication types that you can select for a target system account that you create through Oracle Identity Manager.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Type of authentication
- **Decode:** Description of the type of authentication

Table A–41 lists the default entries in this lookup definition.

Table A–41 Entries in the *Lookup.DBUM.Oracle.AuthType* Lookup Definition

Code Key	Decode
EXTERNAL	EXTERNAL
GLOBAL	GLOBAL
PASSWORD	PASSWORD

A.3.2 Lookup.DBUM.Oracle.AuthType.KeyMapping.CreateUser

The Lookup.DBUM.Oracle.AuthType.KeyMapping.CreateUser lookup definition maps each authentication type (in the Lookup.DBUM.Oracle.AuthType lookup definition) with names of SQL statements used for creating users on the target system.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Type of authentication
- **Decode:** Name of the SQL statement used to create a target system user account

Note: The Decode column contains just the name of the SQL statement that must be run. The complete SQL statement that must be run is specified in the Lookup.DBUM.Oracle.Query.Configuration lookup definition. See [Section A.3.9, "Lookup.DBUM.Oracle.Query.Configuration"](#) for more information about this lookup definition.

Table A–42 lists the default entries in this lookup definition.

Table A–42 Entries in the *Lookup.DBUM.Oracle.AuthType.KeyMapping.CreateUser* Lookup Definition

Code Key	Decode
EXTERNAL	ORA_CREATE_EXTERNAL_USER
GLOBAL	ORA_CREATE_GLOBAL_USER
PASSWORD	ORA_CREATE_USER

If you want to add or modify entries in this lookup definition, then you must enter values in the format specified earlier in this section. Note that changes that you make in the Code Key column of this lookup definition must be duplicated in the Lookup.DBUM.Oracle.AuthType lookup definition. Similarly, changes that you make in the Decode column of this lookup definition must be duplicated in the Lookup.DBUM.Oracle.Query.Configuration and Lookup.DBUM.Oracle.Parameter.Configuration lookup definitions. These lookup definitions are discussed later in this Appendix.

A.3.3 Lookup.DBUM.Oracle.AuthType.KeyMapping.UpdateUser

The Lookup.DBUM.Oracle.AuthType.KeyMapping.UpdateUser lookup definition maps each authentication type (in the Lookup.DBUM.Oracle.AuthType lookup definition) with names of SQL statements used for updating users on the target system.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Type of authentication
- **Decode:** Name of the SQL statement used to update a target system user account

[Table A-43](#) lists the default entries in this lookup definition.

Table A-43 Entries in the Lookup.DBUM.Oracle.AuthType.KeyMapping.UpdateUser Lookup Definition

Code Key	Decode
EXTERNAL	ORA_UPDATE_USER_AUTHTYPE_EXTERNALLY
GLOBAL	ORA_UPDATE_USER_AUTHTYPE_GLOBALLY
PASSWORD	ORA_UPDATE_PASSWORD

If you want to add or modify entries in this lookup definition, then you must enter values in the format specified earlier in this section. Note that changes that you make in the Code Key column of this lookup definition must be duplicated in the Lookup.DBUM.Oracle.AuthType lookup definition. Similarly, changes that you make in the Decode column of this lookup definition must be duplicated in the Lookup.DBUM.Oracle.Query.Configuration and Lookup.DBUM.Oracle.Parameter.Configuration lookup definitions. These lookup definitions are discussed later in this Appendix.

A.3.4 Lookup.DBUM.Oracle.Configuration

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

Note: You cannot add entries to this lookup definition. However, you can modify the Decode values of the existing entries.

[Table A-44](#) lists the default entries in this lookup definition.

Table A–44 Entries in the *Lookup.DBUM.Oracle.Configuration* Lookup Definition

Code Key	Decode	Description
AuthType QueryCodeKey Mapping Lookup For CreateUser	Lookup.DBUM.Oracle.AuthType.KeyMapping.CreateUser	See Section A.3.2 , "Lookup.DBUM.Oracle.AuthType.KeyMapping.CreateUser" for information about this lookup definition.
AuthType QueryCodeKey Mapping Lookup For UpdateUser	Lookup.DBUM.Oracle.AuthType.KeyMapping.UpdateUser	See Section A.3.3 , "Lookup.DBUM.Oracle.AuthType.KeyMapping.UpdateUser" for information about this lookup definition.
Error Mapping Lookup	Lookup.DBUM.Oracle.Error.Mapping	See Section A.3.5 , "Lookup.DBUM.Oracle.Error.Mapping" for information about this lookup definition.
Parameter Configuration Lookup	Lookup.DBUM.Oracle.Parameter.Configuration	See Section A.3.7 , "Lookup.DBUM.Oracle.Parameter.Configuration" for information about this lookup definition.
Provisioning Validation Lookup	Lookup.DBUM.Oracle.Provisioning.Validation	See Section A.3.8 , "Lookup.DBUM.Oracle.Provisioning.Validation" for information about this lookup definition.
Query Configuration Lookup	Lookup.DBUM.Oracle.Query.Configuration	See Section A.3.9 , "Lookup.DBUM.Oracle.Query.Configuration" for information about this lookup definition.
Reconciliation Class Name	oracle.iam.connectors.dbum.tasks.impl.DBUMQueryReconciliationImpl	Name of the class that implements the logic for target resource reconciliation.
Reconciliation Query Property File	Enter a value	Enter the full path and name of the file containing queries that must be run during reconciliation.
Reconciliation SQL Injection Keywords	DROP ~DROP\t~INSERT ~INSERT\t~ALTER ~ALTER\t~CREATE ~CREATE\t~DELETE ~DELETE\t~UPDATE ~UPDATE\t~TRUNCATE ~TRUNCATE\t~EXEC ~EXEC\t~/*~---~;	<p>List of SQL keywords (separated by a tilde (~) character) that modify or can be used to modify data in the database. The connector does not run a query (used for target resource reconciliation) that contains any of the keywords listed in the Decode column.</p> <p>You can add to or remove from the list of SQL keywords. See Section 3.1.1, "Setting Up the Configuration Lookup Definition for a Target Resource" for information about setting a value for this entry.</p>

Table A–44 (Cont.) Entries in the Lookup.DBUM.Oracle.Configuration Lookup Definition

Code Key	Decode	Description
Reserved Words List	DROP ~INSERT ~ALTER ~CREATE ~DELETE ~UPDATE ~GRANT ~TRUNCATE ~EXEC ~TEMPORARY ~TABLESPACE ~DEFAULT ~QUOTA ~PROFILE ~IDENTIFIED ~EXTERNALLY ~AS ~GLOBALLY ~REVOKE ~ACCOUNT ~UNLOCK ~LOCK ~CASCADE ~DROP\t~INSERT\t~ALTER\t~CREAT E\t~DELETE\t~UPDATE\t~GRANT\t~ TRUNCATE\t~EXEC\t~TEMPORARY\t ~TABLESPACE\t~DEFAULT\t~QUOTA \t~PROFILE\t~IDENTIFIED\t~EXTERN ALLY\t~AS\t~GLOBALLY\t~REVOKE\ t~ACCOUNT\t~UNLOCK\t~LOCK\t~ CASCADE\t	List of reserve words that are not supported in the OIM User process form fields during provisioning operations. You can add to or remove from the list of reserve words.
Resource Exclusion Column Key	UD_DB_ORA_U_USERNAME	Name of the process form field that is excluded during provisioning operations.
Resource Exclusion List Lookup	Lookup.DBUM.Oracle.ExclusionList	See for more information about this lookup definition.
Status Reconciliation Class Name	NODATA	Name of the class that implements the logic for deriving the status of a target system user account. You must enter a value for this entry only if your target system does not contain a column from which you can retrieve the status of a target system account. In Oracle Database, the ACCOUNT_STATUS column holds the status of the user in the target system. Therefore, <i>do not</i> enter any value for this entry.
Target Date Format	NODATA	Enter the format in which date values are stored on the target system.
Unsupported Special Characters	--/*~;	The Decode column contains a list of special characters that are not supported in the process form fields during provisioning operations. You can add to or remove from the list of unsupported special characters.
Use Status Reconciliation	No	Specifies whether you want to run reconciliation for the status of a target system user account. Note: Do not change the value of this entry.
Use Validation For Provisioning	No	Specifies whether you want to enable validation of user attributes during provisioning operations. See Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning" for information about configuring data validation during provisioning operations.

A.3.5 Lookup.DBUM.Oracle.Error.Mapping

The Lookup.DBUM.Oracle.Error.Mapping lookup definition maps error codes displayed by the database with error messages to be displayed on the OIM User form during provisioning operations.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** SQL error code returned by the database
- **Decode:** Corresponding error message to be displayed on the OIM User form

To add or modify entries in this lookup definition, you must enter values in the format specified in the preceding paragraph.

[Table A-45](#) lists the default entries in this lookup definition.

Table A-45 Entries in the Lookup.DBUM.Oracle.Error.Mapping Lookup Definition

Code Key	Decode
900	INVALID_SQL
959	INVALID_TABLE_NAME
998	INVALID_PASSWORD
1031	INSUFFICIENT_PRIVILEGE
1920	USER_ALREADY_EXIST
1935	MISSING_ROLE
50004	CHILDNAME_NOT_PROVIDED

A.3.6 Lookup.DBUM.Oracle.ExclusionList

The Lookup.DBUM.Oracle.ExclusionList lookup definition holds user attributes of the target system accounts for which you do not want to perform target resource reconciliation and provisioning.

For target system accounts on which you do not want to perform provisioning operations, the following is the format of the Code Key and Decode values:

- **Code Key:** Name of the process form field
- **Decode:** Process form field values separated by the tilde (~) character

For target system accounts that must not be reconciled during a target resource reconciliation run, the following is the format of the Code Key and Decode values:

- **Code Key:** Resource object field name
- **Decode:** Resource object field values separated by the tilde (~) character

[Table A-46](#) lists the default entries in this lookup definition.

See Also: [Section 3.1.3, "Setting Up the ExclusionList Lookup Definition"](#) for information about adding or modifying entries in this lookup definition

Table A-46 Entries in the Lookup.DBUM.Oracle.ExclusionList Lookup Definition

Code Key	Decode
UD_DB_ORA_U_USERNAME	sys~system

Table A–46 (Cont.) Entries in the Lookup.DBUM.Oracle.ExclusionList Lookup Definition

Code Key	Decode
User Name	sys~system

The first row in [Table A–46](#) specifies that no provisioning operations must be performed on target system accounts whose user name is sys and system. Similarly, the second row specifies that target system accounts with user name sys and system must not be fetched in to Oracle Identity Manager.

A.3.7 Lookup.DBUM.Oracle.Parameter.Configuration

The Lookup.DBUM.Oracle.Parameter.Configuration lookup definition maps identifiers of the SQL statement or SQL fragment (defined in the Lookup.DBUM.Oracle.Query.Configuration lookup definition) with names of the process form fields.

During provisioning operations, the data that you enter on the OIM User form is stored in the corresponding fields of the process form in the Design Console. The fields of the process form are mapped to the identifiers of SQL statements or SQL fragments used for provisioning. In other words, the SQL statements use the data present in the process form to run SQL statements. These SQL statements or SQL fragments are defined in the Lookup.DBUM.Oracle.Query.Configuration lookup definition.

See Also: [Section A.1.6, "Lookup.DBUM.DB2.Query.Configuration"](#) for more information about the Lookup.DBUM.Oracle.Query.Configuration lookup definition

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Identifier in a SQL statement or SQL fragment used for provisioning operations
- **Decode:** Combination of the following elements separated by the tilde (~) character:

`PF_FIELD_NAME~PF_DATA_TYPE~PARAMETER_TYPE~QUOTE_TYPE~EXCLUDE_VALIDATION~UPPERCASE`

In this format:

- `PF_FIELD_NAME` is the name of the process form field
- `PF_DATA_TYPE` is the data type of the process form field
- `PARAMETER_TYPE` specifies whether the value in the process form field is of type input or output.

If the value in the process form field is used as an input parameter, for example as an input to an identifier in a SQL statement, then use IN. Otherwise, OUT.

- `QUOTE_TYPE` element is optional. This element specifies whether the value from the process form field that is passed to the SQL statement must be enclosed in a single quotation mark or double quotation mark.

If you want the value in the process form field to be enclosed in single quotation marks, then use `SINGLE_QUOTE`. If you want the value in the

process form field to be enclosed in double quotation marks, then use `DOUBLE_QUOTE`.

- `EXCLUDE_VALIDATION` element is optional. It is used in the following scenario:

Suppose you specify values for the Reserved Words List or Unsupported Special Characters entries of the `Lookup.DBUM.Oracle.Configuration` lookup definition. During provisioning operations, the connector checks whether the fields on the OIM User form contain any of the values specified in the Reserved Words List or Unsupported Special Characters entries. If such values are found, then no provisioning operations are performed on that record. If you do not want the connector to perform this check on a particular field on the OIM User form, then include `EXCLUDE_VALIDATION` along with the name of the process form field.

For example, in [Table A-47](#), the `UD_DB_ORA_R_ROLE~varchar2~IN~EXCLUDE_VALIDATION` Decode value specifies that during a particular provisioning operation, the connector does not check whether the Role Name field contains any of the values specified in the Reserved Words List or Unsupported Special Characters entries of the `Lookup.DBUM.Oracle.Configuration` lookup definition. In other words, a provisioning operation is not interrupted if the connector finds in the Role Name field, any of the values specified in the Reserved Words List or Unsupported Special Characters entries of the `Lookup.DBUM.Oracle.Configuration` lookup definition.

- `UPPERCASE` element is an optional element. You use this element if you want to save on the target system the value entered in the process form field in upper case.

If you want to add or modify entries in this lookup definition, then you must enter values in the format specified earlier in this section. Note that changes that you make in the Code Key column of this lookup definition must be duplicated in the `Lookup.DBUM.Oracle.Query.Configuration` lookup definition. This is illustrated by the following example:

Suppose, in [Table A-47](#), if you change the `ora_password` Code Key value to `ora_pwd`, then in the `Lookup.DBUM.Oracle.Query.Configuration` lookup definition, you must change all occurrences of `ora_password` to `ora_pwd`.

See Also: [Section 4.3, "Adding or Removing Attribute Mappings for Provisioning"](#)

[Table A-47](#) lists the default entries in this lookup definition.

Table A-47 Entries in the `Lookup.DBUM.Oracle.Parameter.Configuration` Lookup Definition

Code Key	Decode
<code>ora_default_tablespace</code>	<code>UD_DB_ORA_U_TABLESPACE~varchar2~IN~EXCLUDE_VALIDATION</code>
<code>ora_defaultts_quota_size</code>	<code>UD_DB_ORA_U_QUOTASIZE~varchar2~IN</code>
<code>ora_global_dn</code>	<code>UD_DB_ORA_U_GLOBAL_DN~varchar2~IN~SINGLE_QUOTE</code>
<code>ora_password</code>	<code>UD_DB_ORA_U_PASSWORD~varchar2~IN</code>
<code>ora_privilege_admin_option</code>	<code>UD_DB_ORA_P_ADMIN_OPTION~varchar2~IN~EXCLUDE_VALIDATION</code>
<code>ora_privilege_name</code>	<code>UD_DB_ORA_P_PRIVILEGE~varchar2~IN~EXCLUDE_VALIDATION</code>
<code>ora_profile</code>	<code>UD_DB_ORA_U_PROFILE~varchar2~IN~EXCLUDE_VALIDATION</code>

Table A–47 (Cont.) Entries in the Lookup.DBUM.Oracle.Parameter.Configuration Lookup Definition

Code Key	Decode
ora_role_admin_option	UD_DB_ORA_R_ADMIN_OPTION~varchar2~IN~EXCLUDE_VALIDATION
ora_role_name	UD_DB_ORA_R_ROLE~varchar2~IN~EXCLUDE_VALIDATION
ora_temp_tablespace	UD_DB_ORA_U_TEMPTABLESPACE~varchar2~IN~EXCLUDE_VALIDATION
ora_tempts_quota_size	UD_DB_ORA_U_TEMP_QUOTASIZE~varchar2~IN
ora_user_id	UD_DB_ORA_U_USERNAME~varchar2~IN~UPPERCASE
ora_user_id_external	UD_DB_ORA_U_USERNAME~varchar2~IN~DOUBLE_QUOTE~EXCLUDE_VALIDATION~UPPERCASE

A.3.8 Lookup.DBUM.Oracle.Provisioning.Validation

The Lookup.DBUM.Oracle.Provisioning.Validation lookup definition maps the attribute for which validation has to be applied with the validation implementation class.

The Lookup.DBUM.Oracle.Provisioning.Validation lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.3.9 Lookup.DBUM.Oracle.Query.Configuration

As mentioned earlier in this chapter, the Database User Management connector uses SQL statements for provisioning operations. These SQL statements are defined in the Lookup.DBUM.Oracle.Query.Configuration lookup definition. Depending on the provisioning operations that you are performing, adapters run the appropriate SQL statements on the target system.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the SQL statement or SQL fragment
- **Decode:** Corresponding SQL statement or SQL fragment. A SQL statement in this lookup definition is a combination of the following elements:
 - SQL Keywords:
This is a mandatory element. Examples of SQL keywords are GRANT, CREATE, REVOKE, and ALTER.
 - Identifiers:
This is a mandatory element.
In [Table A–48](#), ora_user_id, ora_password, ora_default_tablespace, and ora_profile are identifiers. The actual values for these identifiers are determined at run time.
 - Name of the SQL fragment:
This is an optional element.
In [Table A–48](#), PROFILE_QUERY, ROLE_WITH_ADMIN_OPTION, DEFAULTTS_QUOTA_QUERY, and TEMP_TABLESPACE_QUERY are names of SQL fragments.

For example, in the Decode value of the ORA_ADD_PRIVILEGE Code Key in [Table A-48](#), it is optional to include PRIVILEGE_WITH_ADMIN_OPTION in the SQL statement that is used to grant privileges to a user account on the target system. The name of the SQL fragment, PRIVILEGE_WITH_ADMIN_OPTION, has been specified as optional as you may not want to grant to all user accounts on the target system privileges with the admin option.

[Table A-48](#) lists the default entries in this lookup definition.

If you want to add or modify entries in this lookup definition, then you must enter values in the format specified earlier in this section. Note that changes that you make to identifiers in this lookup definition must be duplicated in the corresponding Code Key value of the Lookup.DBUM.Oracle.Parameter.Configuration lookup definition. In addition, you must also duplicate this change in all occurrences of the identifier in this lookup definition.

Table A-48 Entries in the Lookup.DBUM.Oracle.Query.Configuration Lookup Definition

Code Key	Decode
DEFAULTTS_QUOTA_QUERY	QUOTA :ora_defaultts_quota_size ON :ora_default_tablespace
ORA_ADD_PRIVILEGE	GRANT :ora_privilege_name TO :ora_user_id_external~PRIVILEGE_WITH_ADMIN_OPTION
ORA_ADD_ROLE	GRANT :ora_role_name TO :ora_user_id_external~ROLE_WITH_ADMIN_OPTION
ORA_CREATE_EXTERNAL_USER	CREATE USER :ora_user_id_external IDENTIFIED EXTERNALLY ACCOUNT UNLOCK~TABLESPACE_QUERY~TEMP_TABLESPACE_QUERY~PROFILE_QUERY~DEFAULTTS_QUOTA_QUERY~TEMPTS_QUOTA_QUERY
ORA_CREATE_GLOBAL_USER	CREATE USER :ora_user_id IDENTIFIED GLOBALLY AS :ora_global_dn ACCOUNT UNLOCK~TABLESPACE_QUERY~TEMP_TABLESPACE_QUERY~PROFILE_QUERY~DEFAULTTS_QUOTA_QUERY~TEMPTS_QUOTA_QUERY
ORA_CREATE_USER	CREATE USER :ora_user_id IDENTIFIED BY :ora_password ACCOUNT UNLOCK~TABLESPACE_QUERY~TEMP_TABLESPACE_QUERY~PROFILE_QUERY~DEFAULTTS_QUOTA_QUERY~TEMPTS_QUOTA_QUERY
ORA_DELETE_USER	DROP USER :ora_user_id_external CASCADE
ORA_DISABLE_USER	ALTER USER :ora_user_id_external ACCOUNT LOCK
ORA_ENABLE_USER	ALTER USER :ora_user_id_external ACCOUNT UNLOCK
ORA_REVOKE_PRIVILEGE	REVOKE :ora_privilege_name FROM :ora_user_id_external
ORA_REVOKE_ROLE	REVOKE :ora_role_name FROM :ora_user_id_external
ORA_UPDATE_DEFAULT_TABLESPACE	ALTER USER :ora_user_id_external DEFAULT TABLESPACE :ora_default_tablespace
ORA_UPDATE_DEFAULTTS_QUOTA_SIZE	ALTER USER :ora_user_id_external DEFAULT TABLESPACE :ora_default_tablespace QUOTA :ora_defaultts_quota_size ON :ora_default_tablespace
ORA_UPDATE_GLOBAL_DN	ALTER USER :ora_user_id_external IDENTIFIED GLOBALLY AS :ora_global_dn
ORA_UPDATE_PASSWORD	ALTER USER :ora_user_id_external IDENTIFIED BY :ora_password
ORA_UPDATE_PROFILE	ALTER USER :ora_user_id_external PROFILE :ora_profile

Table A–48 (Cont.) Entries in the Lookup.DBUM.Oracle.Query.Configuration Lookup Definition

Code Key	Decode
ORA_UPDATE_TEMP_TABLESPACE	ALTER USER :ora_user_id_external TEMPORARY TABLESPACE :ora_temp_tablespace
ORA_UPDATE_TEMPPTS_QUOTA_SIZE	ALTER USER :ora_user_id_external TEMPORARY TABLESPACE :ora_temp_tablespace QUOTA :ora_tempts_quota_size ON :ora_temp_tablespace\
ORA_UPDATE_USER_AUTHTYPE_EXTERNALLY	ALTER USER :ora_user_id_external IDENTIFIED EXTERNALLY
ORA_UPDATE_USER_AUTHTYPE_GLOBALLY	ALTER USER :ora_user_id_external IDENTIFIED GLOBALLY AS :ora_global_dn
PRIVILEGE_WITH_ADMIN_OPTION	:ora_privilege_admin_option
PROFILE_QUERY	PROFILE :ora_profile
ROLE_WITH_ADMIN_OPTION	:ora_role_admin_option
TABLESPACE_QUERY	DEFAULT TABLESPACE :ora_default_tablespace
TEMP_TABLESPACE_QUERY	TEMPORARY TABLESPACE :ora_temp_tablespace
TEMPTS_QUOTA_QUERY	QUOTA :ora_tempts_quota_size ON :ora_temp_tablespace

A.3.10 Lookup.DBUM.Oracle.TargetRecon.Delete.Mapping

The Lookup.DBUM.Oracle.TargetRecon.Delete.Mapping lookup definition maps the resource object attribute with the primary key column name used in the reconciliation query. Note that this resource object attribute is the key field for reconciliation matching.

The Lookup.DBUM.Oracle.TargetRecon.Delete.Mapping lookup definition is used during delete user target reconciliation runs.

During a delete user reconciliation run, the resource object attribute that you specify in this lookup definition is used for comparing target system user records with existing target system resource assigned to OIM Users. During this comparison process, if no match is found between the target system user record and the resource provisioned to the OIM User, then the database user resource is revoked from the OIM User.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the resource object attribute, which is the key field for reconciliation matching
- **Decode:** Primary key column name used in the reconciliation query for performing delete user reconciliation

Table A–49 lists the default entry in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify values of the existing Code Key and Decode values.

Table A–49 *Entries in the Lookup.DBUM.Oracle.TargetRecon.Delete.Mapping Lookup Definition*

Code Key	Decode
User Name	USERNAME

A.3.11 Lookup.DBUM.Oracle.TargetRecon.Mapping

The Lookup.DBUM.Oracle.TargetRecon.Mapping lookup definition maps resource object attribute with column names or column name aliases used in the reconciliation query. This lookup definition is used for performing target resource user reconciliation runs.

In this lookup definition, the Code Key contains the reconciliation attribute of the resource object.

For Code Key columns that store single-valued attributes, the Decode value can be in one of the following formats:

- `COL_NAME` or `COL_NAME_ALIAS`

In this format, `COL_NAME` is the target system column name used in the reconciliation query. `COL_NAME_ALIAS` is the alias of the target system column names used in the reconciliation query.

You use this format if the target system contains a column corresponding to the resource object attribute.

For example, consider the User Name attribute, which is a single-valued attribute on the resource object. The target system contains USER NAME, which is a column corresponding to the User Name attribute. In addition, the SELECT clause of the ORACLE_TARGET_USER_RECON reconciliation query contains the USER NAME column. Therefore, the mapping is as follows:

Code Key: User Name

Decode: USER NAME

- `CONSTANT~CONSTANT_VALUE`

In this format, `CONSTANT` specifies that the data in this column is constant. `CONSTANT_VALUE` is the value to be displayed in the corresponding field of the OIM User form in the Administrative and User Console.

You use this format if you want to set a constant value for a particular field on the OIM User form.

For example, consider the Password attribute of the resource object. The Decode value of this attribute is set to `CONSTANT~Dummy`. This implies that the Password field on the OIM User form displays Dummy for all records reconciled from the target system.

- `COLUMN_NAME~LOOKUP_NAME`

In this format, `COLUMN_NAME` is the target system column name from which value is fetched. `LOOKUP_NAME` is the name of the lookup definition that maps values fetched from the target system with values to be displayed in the corresponding field of the OIM User form.

You use this format if you want values fetched from the target system to be displayed in a format that is accepted by Oracle Identity Manager.

For example, consider the Status attribute of the resource object. This is a single valued attribute. The target system contains ACCOUNT_STATUS, which is a column corresponding to the Status attribute of the resource object. However, we do not map the Status resource object attribute to the ACCOUNT_STATUS column for the following reason:

A user account reconciled from the target system can be in one of the following statuses:

- OPEN
- LOCKED
- EXPIRED & LOCKED

However, these statuses cannot be displayed in the Status field of the OIM User form. This is because Oracle Identity Manager accepts only one of the following values as the status of a user account:

- Active
- Disabled
- Disabled Until Start Date
- Deleted

Therefore, in order to display the status retrieved from the ACCOUNT_STATUS column in a format that is accepted by Oracle Identity Manager, the Status resource object attribute has been mapped to

`ACCOUNT_STATUS~Lookup.DBUM.TargetRecon.StatusMapping`.

This implies that in the Code Key column of the `Lookup.DBUM.TargetRecon.StatusMapping` lookup definition, the connector searches for the value that is fetched from the ACCOUNT_STATUS column of the target system. Then, the corresponding Decode value is displayed as the status of the user account in Oracle Identity Manager. This is illustrated by the following example:

Suppose the value fetched from the ACCOUNT_STATUS column for a particular user account on the target system is OPEN. In the Code Key column of the `Lookup.DBUM.TargetRecon.StatusMapping` lookup definition, the connector searches for the value OPEN. The Decode value of the OPEN Code Key is Enabled. Therefore, in Oracle Identity Manager, the connector displays Enabled as the status of the user account.

See Also: [Section A.5.1, "Lookup.DBUM.TargetRecon.StatusMapping"](#)

■ LOOKUP~COL_NAME

In this format:

- LOOKUP specifies that the data retrieved from the target system is lookup data.
- COL_NAME is the corresponding column name or column name alias used in the reconciliation query

You use this format if process form field corresponding to the Code Key value is a lookup type field.

For Code Key columns that store multivalued attributes, the Decode value is specified in the following format:

CHILD~MULTIVALUED_ATTR_CONFIG_LOOKUP

In this format:

- CHILD specifies that the data in this column is the child attribute data
- MULTIVALUED_ATTR_CONFIG_LOOKUP is name of the lookup definition that holds configurable entries for the multivalued attribute.

For example, Role List is a multivalued attribute. The Decode value of the Role List Code Key value is

CHILD~Lookup.DBUM.Oracle.TargetRecon.Role.Configuration. The Lookup.DBUM.Oracle.TargetRecon.Role.Configuration lookup definition contains configurable entries for the Role List attribute.

You can add to or remove entries in the Lookup.DBUM.Oracle.TargetRecon.Mapping lookup definition. See [Section 4.2, "Adding or Removing Attributes for Reconciliation"](#) for information about adding or modifying entries in this lookup definition.

[Table A-50](#) lists the default entries in the Lookup.DBUM.Oracle.TargetRecon.Mapping lookup definition.

Table A-50 Entries in the Lookup.DBUM.Oracle.TargetRecon.Mapping Lookup Definition

Code Key	Decode
Account Status	ACCOUNT_STATUS
Authentication Type	PASSWORD
Default Tablespace	LOOKUP~DEFAULT_TABLESPACE
Default Tablespace Quota	DEFAULT_TABLESPACE_QUOTA
Global DN	EXTERNAL_NAME
Password	CONSTANT~Dummy
Privilege List	CHILD~Lookup.DBUM.Oracle.TargetRecon.Privilege.Configuration
Profile Name	PROFILE
Role List	CHILD~Lookup.DBUM.Oracle.TargetRecon.Role.Configuration
Status	ACCOUNT_STATUS~Lookup.DBUM.TargetRecon.StatusMapping
Temporary Tablespace	TEMPORARY_TABLESPACE
Temporary Tablespace Quota	TEMPORARY_TABLESPACE_QUOTA
User Name	USERNAME

A.3.12 Lookup.DBUM.Oracle.TargetRecon.Privilege.Configuration

The Lookup.DBUM.Oracle.TargetRecon.Privilege.Configuration lookup definition holds configuration entries related to the Privilege multivalued attribute.

[Table A-51](#) lists the default entries in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify the Decode values of existing entries.

Table A–51 Entries in the *Lookup.DBUM.Oracle.TargetRecon.Privilege.Configuration* Lookup Definition

Code Key	Decode	Description
Child Attribute Mapping Lookup	Lookup.DBUM.Oracle.TargetRecon.Privilege.Mapping	See Section A.3.13 , "Lookup.DBUM.Oracle.TargetRecon.Privilege.Mapping" for information about this lookup definition.
Child Query Name	ORACLE_TARGET_USER_PRIVILEGE	Name of the query in the reconciliation query file that you want to run for reconciling data about the child attribute.
Child Reconciliation Query Filter Lookup	Lookup.DBUM.Oracle.TargetRecon.Privilege.QueryFilter	Name of the lookup definition that contains information about reconciliation filter parameters for the child attribute. See Section A.3.14 , "Lookup.DBUM.Oracle.TargetRecon.Privilege.QueryFilter" for more information about this lookup definition.
Parent Attribute	USERNAME	Primary key column of the query used for running target resource user reconciliation.

A.3.13 Lookup.DBUM.Oracle.TargetRecon.Privilege.Mapping

The Lookup.DBUM.Oracle.TargetRecon.Privilege.Mapping lookup definition maps the attributes of the Privilege multivalued attribute on the resource object with column names used in the ORACLE_TARGET_USER_PRIVILEGE reconciliation query. This lookup definition is used to retrieve data about the Privilege attribute during target resource reconciliation.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Attribute name of the multivalued attribute
- **Decode:** The value can be specified in one of the following formats:

- LOOKUP~COL_NAME

In this format:

- LOOKUP specifies that the data retrieved from the target system is lookup data.
- COL_NAME is the corresponding column name or column name alias used in the reconciliation query

You use this format if process form field corresponding to the Code Key value is a lookup type field.

- COL_NAME

This is the column name used in the reconciliation query corresponding to the value in the code key column.

If you want to add or modify the entries in this lookup definition, then you must specify values in the format described in this section.

[Table A–52](#) lists the default entries in this lookup definition.

Table A–52 Entries in the *Lookup.DBUM.Oracle.TargetRecon.Privilege.Mapping* Lookup Definition

Code Key	Decode
Privilege Admin Option	ADMIN_OPTION
Privilege Name	PRIVILEGE

A.3.14 Lookup.DBUM.Oracle.TargetRecon.Privilege.QueryFilter

The Lookup.DBUM.Oracle.TargetRecon.Privilege.QueryFilter lookup definition holds information about the filter parameters that you want to use while running the ORACLE_TARGET_USER_PRIVILEGE query.

The Lookup.DBUM.Oracle.TargetRecon.Privilege.QueryFilter lookup definition is empty by default.

See [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#) for information about adding entries to this lookup definition.

A.3.15 Lookup.DBUM.Oracle.TargetRecon.QueryFilter

The Lookup.DBUM.Oracle.TargetRecon.QueryFilter lookup definition holds information about the filter parameters that you want to use while running the ORACLE_TARGET_USER_RECON query for target resource reconciliation.

The Lookup.DBUM.MSSQL.TargetRecon.QueryFilter lookup definition is empty by default.

See [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#) for information about adding entries to this lookup definition.

A.3.16 Lookup.DBUM.Oracle.TargetRecon.Role.Configuration

The Lookup.DBUM.Oracle.TargetRecon.Role.Configuration lookup definition holds configuration entries related to the Role multivalued field.

[Table A–53](#) lists the default entries in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify the Decode values of the existing entries.

Table A–53 Entries in the *Lookup.DBUM.Oracle.TargetRecon.Role.Configuration* Lookup Definition

Code Key	Decode	Description
Child Attribute Mapping Lookup	Lookup.DBUM.Oracle.TargetRecon.Role.Mapping	See Section A.3.17, "Lookup.DBUM.Oracle.TargetRecon.Role.Mapping" for information about this lookup definition.
Child Query Name	ORACLE_TARGET_USER_ROLE	Name of the query in the reconciliation query file that you want to run for reconciling data about the child attribute..
Child Reconciliation Query Filter Lookup	Lookup.DBUM.Oracle.TargetRecon.Role.QueryFilter	Name of the lookup definition that contains information about reconciliation filter parameters for the child attribute. See Section A.3.18, "Lookup.DBUM.Oracle.TargetRecon.Role.QueryFilter" for more information about this lookup definition.
Parent Attribute	USERNAME	Primary key column of the query used for running target resource user reconciliation.

A.3.17 Lookup.DBUM.Oracle.TargetRecon.Role.Mapping

The Lookup.DBUM.Oracle.TargetRecon.Role.Mapping lookup definition maps attributes of the Role multivalued attribute on the resource object with column names used in the ORACLE_TARGET_USER_ROLE reconciliation query. This lookup definition is used to retrieve data about the Role attribute during target resource reconciliation.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Attribute name of the multivalued attribute
- **Decode:** The value can be specified in one of the following formats:

- LOOKUP~COL_NAME

In this format:

- LOOKUP specifies that the data retrieved from the target system is lookup data.
- COL_NAME is the corresponding column name or column name alias used in the reconciliation query

You use this format if process form field corresponding to the Code Key value is a lookup type field.

- COL_NAME

This is the column name used in the reconciliation query corresponding to the value in the code key column.

If you want to add or modify the entries in this lookup definition, then you must specify values in the format described in this section.

If you want to add or modify entries in this lookup definition, then you must enter values in the format specified in the preceding paragraph.

[Table A–54](#) lists the default entries in this lookup definition.

Table A–54 *Entries in the Lookup.DBUM.Oracle.TargetRecon.Role.Mapping Lookup Definition*

Code Key	Decode
Role Admin Option	ADMIN_OPTION
Role Name	GRANTED_ROLE

A.3.18 Lookup.DBUM.Oracle.TargetRecon.Role.QueryFilter

The Lookup.DBUM.Oracle.TargetRecon.Role.QueryFilter lookup definition holds information about the filter parameters that you want to use while running the ORACLE_TARGET_USER_ROLE query.

The Lookup.DBUM.Oracle.TargetRecon.Role.QueryFilter lookup definition is empty by default.

See [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#) for information about adding entries to this lookup definition.

A.3.19 Lookup.DBUM.Oracle.TargetRecon.Transformation

The Lookup.DBUM.Oracle.TargetRecon.Transformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during target resource reconciliation.

The Lookup.DBUM.Oracle.TargetRecon.Transformation lookup definition is empty by default.

See [Section 4.9, "Configuring Transformation of Data During Reconciliation"](#) for information about adding entries to this lookup definition.

A.3.20 Lookup.DBUM.Oracle.TargetRecon.Validation

The Lookup.DBUM.Oracle.TargetRecon.Validation lookup definition is used to configure validation of attribute values that are fetched from the target system during target resource reconciliation.

The Lookup.DBUM.Oracle.TargetRecon.Validation lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.3.21 Lookup.DBUM.Oracle.WithAdminOption

During a provisioning operation, you use the Lookup.DBUM.Oracle.WithAdminOption lookup definition to specify whether the target system user record being created has administrative options on the role or privilege being grant to the user record.

Note: You cannot add or modify entries in this lookup definition.

[Table A–55](#) lists the default entry in this lookup definition.

Table A–55 Entries in the *Lookup.DBUM.DB2.WithGrantOption* Lookup Definition

Code Key	Decode
WITH ADMIN OPTION	WITH ADMIN OPTION

A.3.22 Lookup.DBUM.Oracle.TrustedRecon.Configuration

The *Lookup.DBUM.Oracle.TrustedRecon.Configuration* lookup definition holds connector configuration entries that are used during trusted source reconciliation.

[Table A–56](#) lists the default entries in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify the Decode values of the existing entries.

Table A–56 Entries in the *Lookup.DBUM.Oracle.TrustedRecon.Configuration* Lookup Definition

Code Key	Decode	Description
Reconciliation Class Name	oracle.iam.connectors.dbum.tasks.impl.DBUMQueryReconciliationImpl	Name of the class that implements the logic for trusted source reconciliation.
Reconciliation Query Property File	Enter a value	Enter the full path and name of the file containing queries that must be run during reconciliation.
Reconciliation SQL Injection Keywords	DROP ~DROP\t~INSERT ~INSERT\t~ALTER ~ALTER\t~CREATE ~CREATE\t~DELETE ~DELETE\t~UPDATE ~UPDATE\t~TRUNCATE ~TRUNCATE\t~EXEC ~EXEC\t~/*~--~;	List of SQL keywords (separated by a tilde (~) character) that modify or can be used to modify data in the database. The connector does not run a query (used for trusted source reconciliation) that contains any of the keywords listed in the Decode column. You can add to or remove from the list of SQL keywords. See Section 3.1.2, "Setting Up the Configuration Lookup Definition for a Trusted Source" for information about setting a value for this entry.
Resource Exclusion List Lookup	Lookup.DBUM.Oracle.TrustedRecon.ExclusionList	See Section A.3.24, "Lookup.DBUM.Oracle.TrustedRecon.ExclusionList" for more information about this lookup definition.

Table A–56 (Cont.) Entries in the Lookup.DBUM.Oracle.TrustedRecon.Configuration Lookup Definition

Code Key	Decode	Description
Status Reconciliation Class Name	NODATA	<p>Name of the class that implements the logic for deriving the status of a target system user account.</p> <p>You must enter a value for this entry only if your target system does not contain a column from which you can retrieve the status of a target system account. In Oracle Database, the ACCOUNT_STATUS column holds the status of the user in the target system. Therefore, <i>do not</i> enter any value for this entry.</p>
Target Date Format	NODATA	Enter the format in which date values are stored on the target system.
Use Status Reconciliation	No	<p>Specifies whether you want to run reconciliation for the status of a target system user account.</p> <p>Note: Do not change the value of this entry.</p>

A.3.23 Lookup.DBUM.Oracle.TrustedRecon.Delete.Mapping

The Lookup.DBUM.Oracle.TrustedRecon.Delete.Mapping lookup definition maps the resource object field with the primary key column name used in the reconciliation query (for retrieving all users from the target system). Note that this resource object field is the key field for reconciliation matching.

The Lookup.DBUM.Oracle.TrustedRecon.Delete.Mapping lookup definition is used during delete user trusted reconciliation runs.

During a delete user reconciliation run, the resource object field that you specify in this lookup definition is used for comparing target system user records with existing OIM Users. During the comparison process, if no match is found between the target system user record and OIM User, then the OIM User is deleted.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the resource object field, which is the key field for reconciliation matching
- **Decode:** Primary key column name used in the reconciliation query for performing delete user reconciliation

Table A–57 lists the default entry in this lookup definition.

Note: You cannot add entries to this lookup definition. You modify the entry in this lookup definition if you change the key field for reconciliation matching on the resource object.

Table A–57 Entries in the Lookup.DBUM.Oracle.TrustedRecon.Delete.Mapping Lookup Definition

Code Key	Decode
User Login	USER NAME

A.3.24 Lookup.DBUM.Oracle.TrustedRecon.ExclusionList

The Lookup.DBUM.Oracle.TrustedRecon.ExclusionList lookup definition holds user attributes of target system accounts that must not be reconciled during trusted source reconciliation.

The following is the format of the Code Key and Decode values for this lookup definition:

- **Code Key:** Resource object attribute name
- **Decode:** Resource object attribute values separated by the tilde (~) character

[Table A-58](#) lists the default entry in this lookup definition.

See Also: [Section 3.1.3, "Setting Up the ExclusionList Lookup Definition"](#) for information about adding or modifying entries in this lookup definition

Table A-58 Entries in the Lookup.DBUM.DB2.TrustedRecon.ExclusionList Lookup Definition

Code Key	Decode
User Login	sys~system

A.3.25 Lookup.DBUM.Oracle.TrustedRecon.Mapping

The Lookup.DBUM.Oracle.TrustedRecon.Mapping lookup definition maps the fields of the OIM User form with corresponding column names used in the reconciliation query. This lookup definition is used for performing trusted source reconciliation.

In this lookup definition, the Code Key contains names of the fields on the OIM User form. The Decode value can be in one of the following formats:

- COL_NAME or COL_NAME_ALIAS

In this format, *COL_NAME* is the target system column name used in the reconciliation query. *COL_NAME_ALIAS* is the alias of the target system column name used in the reconciliation query.

You use this format if the target system contains a column corresponding to the resource object attribute.

For example, consider the User Login attribute on the resource object. The target system contains USERNAME, which is a column corresponding to the User Login attribute. In addition, the SELECT clause of the ORACLE_TRUSTED_USER_RECON reconciliation query contains the USERNAME column. Therefore, the mapping is as follows:

Code Key: User Login

Decode: USERNAME

- CONSTANT~CONSTANT_VALUE

In this format:

- CONSTANT specifies that the data in this column is constant.
- CONSTANT_VALUE is the value to be displayed in the corresponding field of the OIM User form in the Administrative and User Console.

You this format if you want to set a constant value for a particular field on the OIM User form.

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 `CONSTANT~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.

By default, in this lookup definition, the Decode values for the Employee Type, Organization, and User Type Code Key columns have been set to constant values Full-Time, Xellerate Users, and End-User, respectively. However, depending on your requirement, you can change these values to one of the following:

- For the Employee Type Code Key, you can set one of the following constant values:
 - Full-Time
 - Part-Time
 - Temp
 - Intern
 - Consultant
- For the Organization Code Key, you can set one of the following constant values:
 - Xellerate Users
 - Requests
- For the User Type Code Key, you can set one of the following constant values:
 - End-User
 - End-User Administrator
- *COLUMN_NAME~LOOKUP_NAME*
In this format:
 - *COLUMN_NAME* is the target system column name from which value is fetched.
 - *LOOKUP_NAME* is the name of the lookup definition that maps values fetched from the target system with values to be displayed in the OIM User form field.

You use this format if you want values fetched from the target system to be displayed in a format that is accepted by Oracle Identity Manager.

For example, consider the Status attribute of the resource object. The target system contains `ACCOUNT_STATUS`, which is a column corresponding to the Status attribute of the resource object. However, we do not map the Status attribute to the `ACCOUNT_STATUS` column for the following reason:

A user account reconciled from the target system can be in one of the following statuses:

- OPEN
- LOCKED
- EXPIRED & LOCKED

However, these statuses cannot be displayed in the Status field of the OIM User form. This is because Oracle Identity Manager accepts only one of the following values as the status of a user account:

- Active
- Disabled
- Disabled Until Start Date
- Deleted

Therefore, in order to display the status retrieved from the ACCOUNT_STATUS column in a format that is accepted by Oracle Identity Manager, the Status resource object attribute has been mapped to

ACCOUNT_STATUS~Lookup.DBUM.TrustedRecon.StatusMapping.

This implies that in the Code Key column of the Lookup.DBUM.TrustedRecon.StatusMapping lookup definition, the connector searches for the value that is fetched from the ACCOUNT_STATUS column of the target system. Then, the corresponding Decode value is displayed as the status of the user account in Oracle Identity Manager. This is illustrated by the following example:

Suppose the value fetched from the ACCOUNT_STATUS column for a particular user account on the target system is OPEN. In the Code Key column of the Lookup.DBUM.TrustedRecon.StatusMapping lookup definition, the connector searches for the value OPEN. The Decode value of the OPEN Code Key is Active. Therefore, in Oracle Identity Manager, the connector displays Active as the status of the user account.

See Also: [Section A.5.2, "Lookup.DBUM.TrustedRecon.StatusMapping"](#)

You can add to or remove entries in the Lookup.DBUM.Oracle.TrustedRecon.Mapping lookup definition. See [Section 4.2, "Adding or Removing Attributes for Reconciliation"](#) for information about adding or modifying entries in this lookup definition.

[Table A-59](#) lists the default entries in this lookup definition.

Table A-59 *Entries in the Lookup.DBUM.Oracle.TrustedRecon.Mapping Lookup Definition*

Code Key	Decode
Employee Type	CONSTANT~Full-Time
First Name	USERNAME
Last Name	USERNAME
Organization	CONSTANT~Xellerate Users
Status	ACCOUNT_STATUS~Lookup.DBUM.TrustedRecon.StatusMapping
User Login	USERNAME
User Type	CONSTANT~End-User

A.3.26 Lookup.DBUM.Oracle.TrustedRecon.QueryFilter

The Lookup.DBUM.Oracle.TrustedRecon.QueryFilter lookup definition is used for configuring limited reconciliation if your target system is configured as a trusted

source. This lookup definition holds information about the filter parameters that you want to use while running the SQL query for trusted source reconciliation.

The Lookup.DBUM.Oracle.TargetRecon.QueryFilter lookup definition is empty by default.

See [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#) for information about adding entries to this lookup definition.

A.3.27 Lookup.DBUM.Oracle.TrustedRecon.Transformation

The Lookup.DBUM.Oracle.TrustedRecon.Transformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during trusted source reconciliation.

The Lookup.DBUM.Oracle.TrustedRecon.Transformation lookup definition is empty by default.

See [Section 4.9, "Configuring Transformation of Data During Reconciliation"](#) for information about adding entries to this lookup definition.

A.3.28 Lookup.DBUM.Oracle.TrustedRecon.Validation

The Lookup.DBUM.Oracle.TrustedRecon.Validation lookup definition is used to configure validation of attribute values that are fetched from the target system during trusted source reconciliation.

The Lookup.DBUM.Oracle.TrustedRecon.Validation lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.4 Lookup Definitions for Sybase

This section provides information about the following lookup definitions:

- [Section A.4.1, "Lookup.DBUM.Sybase.Configuration"](#)
- [Section A.4.2, "Lookup.DBUM.Sybase.Error.Mapping"](#)
- [Section A.4.3, "Lookup.DBUM.Sybase.ExclusionList"](#)
- [Section A.4.4, "Lookup.DBUM.Sybase.Parameter.Configuration"](#)
- [Section A.4.5, "Lookup.DBUM.Sybase.Provisioning.Validation"](#)
- [Section A.4.6, "Lookup.DBUM.Sybase.Query.Configuration"](#)
- [Section A.4.7, "Lookup.DBUM.Sybase.TargetRecon.Delete.Login.Mapping"](#)
- [Section A.4.8, "Lookup.DBUM.Sybase.TargetRecon.Delete.User.Mapping"](#)
- [Section A.4.9, "Lookup.DBUM.Sybase.TargetRecon.Login.Mapping"](#)
- [Section A.4.10, "Lookup.DBUM.Sybase.TargetRecon.Login.Transformation"](#)
- [Section A.4.11, "Lookup.DBUM.Sybase.TargetRecon.Login.Validation"](#)
- [Section A.4.12, "Lookup.DBUM.Sybase.TargetRecon.QueryFilter"](#)
- [Section A.4.13, "Lookup.DBUM.Sybase.TargetRecon.Role.Mapping"](#)
- [Section A.4.14, "Lookup.DBUM.Sybase.TargetRecon.User.Mapping"](#)
- [Section A.4.15, "Lookup.DBUM.Sybase.TargetRecon.User.Transformation"](#)

- [Section A.4.16, "Lookup.DBUM.Sybase.TargetRecon.User.Validation"](#)
- [Section A.4.17, "Lookup.DBUM.Sybase.TrustedRecon.Configuration"](#)
- [Section A.4.18, "Lookup.DBUM.Sybase.TrustedRecon.Delete.Mapping"](#)
- [Section A.4.19, "Lookup.DBUM.Sybase.TrustedRecon.ExclusionList"](#)
- [Section A.4.20, "Lookup.DBUM.Sybase.TrustedRecon.Mapping"](#)
- [Section A.4.21, "Lookup.DBUM.Sybase.TrustedRecon.QueryFilter"](#)
- [Section A.4.22, "Lookup.DBUM.Sybase.TrustedRecon.Transformation"](#)
- [Section A.4.23, "Lookup.DBUM.Sybase.TrustedRecon.Validation"](#)

A.4.1 Lookup.DBUM.Sybase.Configuration

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

Note: You cannot add entries to this lookup definition. However, you can modify the Decode values of the existing entries.

[Table A–60](#) lists the default entries in this lookup definition.

Table A–60 Entries in the Lookup.DBUM.Sybase.Configuration Lookup Definition

Code Key	Decode	Description
Error Mapping Lookup	Lookup.DBUM.Sybase.Error.Mapping	See Section A.2.9, "Lookup.DBUM.MSSQL.Error.Mapping" for information about this lookup definition.
Parameter Configuration Lookup	Lookup.DBUM.Sybase.Parameter.Configuration	See Section A.2.11, "Lookup.DBUM.MSSQL.Parameter.Configuration" for information about this lookup definition.
Provisioning Validation Lookup	Lookup.DBUM.Sybase.Provisioning.Validation	See Section A.2.12, "Lookup.DBUM.MSSQL.Provisioning.Validation" for information about this lookup definition.
Query Configuration Lookup	Lookup.DBUM.Sybase.Query.Configuration	See Section A.2.13, "Lookup.DBUM.MSSQL.Query.Configuration" for information about this lookup definition.
Reconciliation Class Name	oracle.iam.connectors.dbum.tasks.impl.DBUMSybaseReconciliationImpl	Name of the class that implements the logic for target resource reconciliation.
Reconciliation Query Property File	Enter a value	Enter the full path and name of the file containing queries that must be run during reconciliation.
Reconciliation SQL Injection Keywords	NODATA	Enter the SQL keywords (separated by a tilde (~) character) that must not be used in the reconciliation query. The connector does not run a query (used for target resource reconciliation) that contains any of the keywords listed in the Decode column.

Table A–60 (Cont.) Entries in the Lookup.DBUM.Sybase.Configuration Lookup Definition

Code Key	Decode	Description
Reserved Words List	NODATA	List of reserve words that are not supported in the OIM User process form fields during provisioning operations.
Resource Exclusion Column Key	UD_DB_SYB_L_LOGIN	Name of the process form field that is excluded during provisioning operations.
Resource Exclusion List Lookup	Lookup.DBUM.Sybase.ExclusionList	See for more information about this lookup definition.
Status Reconciliation Class Name	NODATA	You must enter a value for this entry only if your target system does not contain a column from which you can retrieve the status of a target system account. In Microsoft SQL server, the <code>is_disabled</code> column holds the status of the target system account. Therefore, <i>do not</i> enter any value for this entry.
Target Date Format	NODATA	Enter the format in which date values are stored on the target system.
Unsupported Special Characters	NODATA	Enter the list of special characters that are not supported in the process form fields during provisioning operations.
Use Status Reconciliation	No	Specifies whether you want to run reconciliation for the status of a target system user account. Note: Do not change the value of this entry.
Use Validation For Provisioning	Yes	Specifies whether you want to enable validation of user attributes during provisioning operations. See Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning" for information about configuring data validation during provisioning operations.

A.4.2 Lookup.DBUM.Sybase.Error.Mapping

The Lookup.DBUM.Sybase.Error.Mapping lookup definition maps error codes displayed by the database with error messages to be displayed on the OIM User form during provisioning operations.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** SQL error code returned by the database
- **Decode:** Corresponding error message to be displayed on the OIM User process form

If you want to add or modify entries in this lookup definition, then specify the values in the format specified in the preceding paragraph.

[Table A–61](#) lists the default entries in this lookup definition.

Table A–61 Entries in the *Lookup.DBUM.Sybase.Error.Mapping* Lookup Definition

Code Key	Decode
102	INCORRECT_SYNTAX
900	INVALID_SQL
15006	INVALID_CHARACTERS
15023	USER_ALREADY_EXIST
15025	LOGIN_ALREADY_EXIST
15118	PASSWORD_POLICY_NOT_MATCH
15247	PERMISSION_DENIED

A.4.3 Lookup.DBUM.Sybase.ExclusionList

The Lookup.DBUM.Sybase.ExclusionList lookup definition holds user attributes of the target system accounts for which you do not want to perform target resource reconciliation and provisioning.

For target system accounts on which you do not want to perform provisioning operations, the following is the format of the Code Key and Decode values:

- **Code Key:** Name of the process form field
- **Decode:** Process form field values separated by the tilde (~) character

For target system accounts that must not be reconciled during a target resource reconciliation run, the following is the format of the Code Key and Decode values:

- **Code Key:** Resource object attribute name
- **Decode:** Resource object attribute values separated by the tilde (~) character

[Table A–28](#) lists the default entry in this lookup definition.

See Also: [Section 3.1.3, "Setting Up the ExclusionList Lookup Definition"](#) for information about adding or modifying entries in this lookup definition

Table A–62 Entries in the *Lookup.DBUM.Sybase.ExclusionList* Lookup Definition

Code Key	Decode
UD_DB_SYB_L_LOGIN	sa
Login Name	sa
User Name	sa

A.4.4 Lookup.DBUM.Sybase.Parameter.Configuration

The Lookup.DBUM.Sybase.Parameter.Configuration lookup definition maps identifiers of stored procedures and SQL statements (defined in the Lookup.DBUM.Sybase.Query.Configuration lookup definition) with names of the process form fields.

This connector uses stored procedures and SQL statements to perform provisioning operations. The data that you enter on the process form while performing provisioning operations are stored in the corresponding process form fields in the Design Console. The process form field is mapped to the identifiers of stored procedures or SQL

statements that are defined in the `Lookup.DBUM.Sybase.Query.Configuration` lookup definition.

See Also: [Section A.4.6, "Lookup.DBUM.Sybase.Query.Configuration"](#) for more information about the `Lookup.DBUM.Sybase.Query.Configuration` lookup definition

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Identifier in the stored procedure or SQL statement used for provisioning operations
- **Decode:** Combination of the following elements separated by the tilde (~) character:

`PF_FIELD_NAME~PF_DATA_TYPE~PARAMETER_TYPE~QUOTE_TYPE~EXCLUDE_VALIDATION~UPPERCASE`

In this format:

- `PF_FIELD_NAME` is process form field name
- `PF_DATA_TYPE` is process form field data type
- `PARAMETER_TYPE` specifies whether the value in the process form field is of type input or output.

If the value in the process form field is used as an input parameter, for example, as an input to a variable in the SQL statement, then use `IN`. Otherwise, use `OUT`.

- `QUOTE_TYPE` specifies whether the value from the process form field that is passed to the SQL statement must be enclosed in a single quotation mark or double quotation mark. The `QUOTE_TYPE` element is optional.

If you want to enclose the value in single quotation marks, then use `SINGLE_QUOTE`. If you want to enclose the value in double quotation marks, then use `DOUBLE_QUOTE`.

- `EXCLUDE_VALIDATION` is an optional element. It is used in the following scenario:

Suppose you specify values for the Reserved Words List or Unsupported Special Characters entries of the `Lookup.DBUM.Sybase.Configuration` lookup definition. During provisioning operations, the connector checks whether the OIM User process form fields contain any of the values specified in the Reserved Words List or Unsupported Special Characters entries. If such values are found, then no provisioning operations are performed on that record. If you do not want the connector to perform this check on a particular field on the OIM User process form, then include `EXCLUDE_VALIDATION` along with the name of that process form field.

For example, the

`UD_DB_SYB_R_ROLE~varchar2~IN~EXCLUDE_VALIDATION` Decode values specifies that during a particular provisioning operation, the connector does not check whether the Role field contains any of the values specified in the Reserved Words List or Unsupported Special Characters entries of the `Lookup.DBUM.Sybase.Configuration` lookup definition.

- UPPERCASE element is an optional element. You use this element if you want to save on the target system the value entered in the process form field in upper case

[Table A-63](#) lists the default entries in this lookup definition.

Table A-63 *Entries in the Lookup.DBUM.Sybase.Parameter.Configuration Lookup Definition*

Code Key	Decode
syb_defdb	UD_DB_SYB_L_DEFDB~varchar2~IN~EXCLUDE_VALIDATION
syb_deflang	UD_DB_SYB_L_DEFAULTLANG~varchar2~IN~EXCLUDE_VALIDATION
syb_fullname	UD_DB_SYB_L_FULLNAME~varchar2~IN
syb_group	UD_DB_SYB_U_DBGROUP~varchar2~IN~EXCLUDE_VALIDATION
syb_login	UD_DB_SYB_L_LOGIN~varchar2~IN
syb_old_pass	UD_DB_SYB_L_OLD_PASSWORD~varchar2~IN
syb_pass	UD_DB_SYB_L_PASSWORD~varchar2~IN
syb_role	UD_DB_SYB_R_ROLE~varchar2~IN~EXCLUDE_VALIDATION
syb_user_id	UD_DB_SYB_U_USERNAME~varchar2~IN
syb_user_login	UD_DB_SYB_U_LOGINNAME~varchar2~IN

A.4.5 Lookup.DBUM.Sybase.Provisioning.Validation

The Lookup.DBUM.Sybase.Provisioning.Validation lookup definition is used to store the mapping between the attribute for which validation has to be applied and the validation implementation class.

The Lookup.DBUM.Sybase.Provisioning.Validation lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.4.6 Lookup.DBUM.Sybase.Query.Configuration

As mentioned in one of the sections in this chapter, this connector uses stored procedures and SQL statements to perform provisioning operations.

The Lookup.DBUM.Sybase.Query.Configuration lookup definition contains stored procedures and SQL statements that are used to perform provisioning operations.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the stored procedure or SQL statement
- **Decode:** Corresponding stored procedure or SQL statement

Depending on the provisioning operations that you are performing, adapters run the appropriate stored procedures or SQL statements on the target system.

[Table A-64](#) lists the default entries in this lookup definition.

Table A–64 Entries in the *Lookup.DBUM.Sybase.Query.Configuration* Lookup Definition

Code Key	Decode
SYB_ADD_ROLE	{CALL sp_role('grant',:syb_role,:syb_login)}
SYB_CREATE_LOGIN	{CALL sp_addlogin(:syb_login,:syb_pass,:syb_defdb,:syb_deflang,:syb_fullname)}
SYB_CREATE_USER	{CALL sp_adduser(:syb_user_login,:syb_user_id,:syb_group)}
SYB_DELETE_LOGIN	{CALL sp_droplogin(:syb_login)}
SYB_DELETE_USER	{CALL sp_dropuser(:syb_user_id)}
SYB_DISABLE_LOGIN	{CALL sp_locklogin(:syb_login,'lock')}
SYB_ENABLE_LOGIN	{CALL sp_locklogin(:syb_login,'unlock')}
SYB_REVOKE_ROLE	{CALL sp_role('revoke',:syb_role,:syb_login)}
SYB_UPDATE_DEFDB	{CALL sp_modifylogin(:syb_login,'defdb',:syb_defdb)}
SYB_UPDATE_DEFLANG	{CALL sp_modifylogin(:syb_login,'deflanguage',:syb_deflang)}
SYB_UPDATE_FULLNAME	{CALL sp_modifylogin(:syb_login,'fullname',:syb_fullname)}
SYB_UPDATE_GROUP	{CALL sp_changegroup(:syb_group,:syb_user_id)}
SYB_UPDATE_LOGIN_PASSWORD	{CALL sp_password(:syb_old_pass,:syb_pass,:syb_login)}
SYB_GET_USER	select u.name from sysusers u, sysusers g, master.dbo.syslogins m where u.name=:syb_user_id and u.suid *= m.suid and u.gid *= g.uid and ((u.uid < @@mingroupid and u.uid != 0) or (u.uid > @@maxgroupid))
SYB_GET_LOGIN	select name from master.dbo.syslogins where name=:syb_login

A.4.7 Lookup.DBUM.Sybase.TargetRecon.Delete.Login.Mapping

The Lookup.DBUM.Sybase.TargetRecon.Delete.Login.Mapping lookup definition maps the resource object field with the primary key column name used in the reconciliation query. Note that this resource object field is the key field for reconciliation matching.

The Lookup.DBUM.Sybase.TargetRecon.Delete.Login.Mapping lookup definition is used during delete login target reconciliation runs.

During a delete login reconciliation run, the resource object field that you specify in this lookup definition is used for comparing target system login entity records with existing target system resource assigned to OIM Users. During this comparison process, if no match is found between the target system login entity record and the resource provisioned to the OIM User, then the database user resource is revoked from the OIM User.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the resource object field, which is the key field for reconciliation matching
- **Decode:** Primary key column name used in the reconciliation query for performing delete user reconciliation

Table A–65 lists the default entry in this lookup definition.

Table A–65 Entries in the Lookup.DBUM.Sybase.TargetRecon.Delete.Login.Mapping Lookup Definition

Code Key	Decode
Login Name	LoginName

A.4.8 Lookup.DBUM.Sybase.TargetRecon.Delete.User.Mapping

The Lookup.DBUM.Sybase.TargetRecon.Delete.User.Mapping lookup definition maps the resource object field with the primary key column name used in the reconciliation query. Note that this resource object field is the key field for reconciliation matching.

The Lookup.DBUM.Sybase.TargetRecon.Delete.User.Mapping lookup definition is used during delete user target reconciliation runs.

During a delete user reconciliation run, the resource object field that you specify in this lookup definition is used for comparing target system user entity records with existing target system resource assigned to OIM Users. During this comparison process, if no match is found between the target system user entity record and the resource provisioned to the OIM User, then the database user resource is revoked from the OIM User.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the resource object field, which is the key field for reconciliation matching
- **Decode:** Primary key column name used in the reconciliation query for performing delete user reconciliation

Table A–66 lists the default entry in this lookup definition.

Table A–66 Entries in the Lookup.DBUM.Sybase.TargetRecon.Delete.User.Mapping Lookup Definition

Code Key	Decode
User Name	UserName

A.4.9 Lookup.DBUM.Sybase.TargetRecon.Login.Mapping

The Lookup.DBUM.Sybase.TargetRecon.Login.Mapping lookup definition maps resource object fields with column names used in the stored procedure or SQL query for reconciliation. This lookup definition is used for performing target resource login reconciliation runs.

In this lookup definition, the Code Key contains the reconciliation field of the resource object.

For Code Key columns that store single-valued attributes, the Decode value can be in one of the following formats:

- COL_NAME or COL_NAME_ALIAS

In this format, *COL_NAME* is the target system column name used in the reconciliation query. *COL_NAME_ALIAS* is the alias of the target system column names used in the reconciliation query.

You use this format if the target system contains a column corresponding to the resource object attribute.

For example, consider the Login Name attribute, which is a single-valued attribute on the resource object. The target system contains Loginame, which is a column corresponding to the Login Name attribute. Therefore, the mapping is as follows:

Code Key: Login Name

Decode: Loginame

- *CONSTANT~CONSTANT_VALUE*

In this format, *CONSTANT* specifies that the data in this column is constant. *CONSTANT_VALUE* is value that you want to be displayed in the corresponding field of the OIM User form in the Administrative and User Console.

You use this format if you want to set a constant value for a particular field on the OIM User form.

For example, consider the Password attribute of the resource object. The Decode value of this attribute is set to *CONSTANT~Dummy*. This implies that the Password field on the OIM User form displays Dummy for all records reconciled from the target system.

- *COLUMN_NAME~LOOKUP_NAME*

In this format, *COLUMN_NAME* is the target system column name from which value is fetched. *LOOKUP_NAME* is the name of the lookup definition that maps values fetched from the target system with values to be displayed in the OIM User form field.

You use this format if you want values fetched from the target system to be displayed in a format that is accepted by Oracle Identity Manager.

For example, consider the Status attribute of the resource object. This is a single-valued attribute. The target system contains Locked, which is a column corresponding to the Status attribute of the resource object. However, we do not map the Status resource object attribute to the Locked column for the following reason:

The status of an account in the target system can be reconciled from the Locked column, which can contain only the following values:

- YES
- NO

However, these statuses cannot be displayed in the Status field of the OIM User form. This is because Oracle Identity Manager accepts only one of the following values as the status of a user account:

- Active
- Disabled
- Disabled Until Start Date
- Deleted

Therefore, in order to display the status retrieved from the Locked column in a format that is accepted by Oracle Identity Manager, the Status resource object attribute has been mapped to

`Locked~Lookup.DBUM.TargetRecon.StatusMapping`.

This implies that in the Code Key column of the `Lookup.DBUM.TargetRecon.StatusMapping` lookup definition, the connector searches for the value that is fetched from the Locked column of the target system.

Then, the corresponding Decode value is displayed as the status of the user account in Oracle Identity Manager. This is illustrated by the following example:

Suppose the value fetched from the Locked column for a particular user account on the target system is NO. In the Code Key column of the Lookup.DBUM.TargetRecon.StatusMapping lookup definition, the connector searches for the value NO. The Decode value of the No Code Key is Enabled. Therefore, in Oracle Identity Manager, the connector displays Enabled as the status of the user account.

See Also: [Section A.5.1, "Lookup.DBUM.TargetRecon.StatusMapping"](#)

■ LOOKUP~COL_NAME

In this format:

- LOOKUP specifies that the data retrieved from the target system is lookup data.
- COL_NAME is the corresponding column name or column name alias used in the reconciliation query

You use this format if process form field corresponding to the Code Key value is a lookup type field.

For Code Key columns that store multivalued attributes, the Decode value is specified in one of the following formats:

CHILD~MULTIVALUED_ATTR_CONFIG_LOOKUP

In this format:

- CHILD specifies that the data in this column is the child attribute data
- MULTIVALUED_ATTR_CONFIG_LOOKUP is name of the lookup definition that holds configurable entries for the multivalued attribute.

For example, Role List is a multivalued attribute. The Decode value of the Role List Code Key value is CHILD~Lookup.DBUM.Sybase.TargetRecon.Role.Mapping.

See Also: [Section A.4.10, "Lookup.DBUM.Sybase.TargetRecon.Login.Transformation"](#)

You can add to or remove entries in the Lookup.DBUM.Oracle.TargetRecon.Mapping lookup definition. See [Section 4.2, "Adding or Removing Attributes for Reconciliation"](#) for information about adding or modifying entries in this lookup definition.

[Table A-67](#) lists the default entries in this lookup definition, and the descriptions for some of the lookup entries.

Table A-67 Entries in the Lookup.DBUM.Sybase.TargetRecon.Login.Mapping Lookup Definition

Code Key	Decode
Default Database Name	Lookup~Default Database
Default Language	Lookup~Default Language
Full Name	Fullname
Login Name	Loginame

Table A–67 (Cont.) Entries in the Lookup.DBUM.Sybase.TargetRecon.Login.Mapping Lookup Definition

Code Key	Decode
Password	CONSTANT~Dummy
Role List	CHILD~Lookup.DBUM.Sybase.TargetRecon.Role.Mapping
Status	Locked~Lookup.DBUM.TargetRecon.StatusMapping

A.4.10 Lookup.DBUM.Sybase.TargetRecon.Login.Transformation

The Lookup.DBUM.Sybase.TargetRecon.Login.Transformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during target resource reconciliation of login entities.

The Lookup.DBUM.Sybase.TargetRecon.Login.Transformation lookup definition is empty by default.

See [Section 4.9, "Configuring Transformation of Data During Reconciliation"](#) for information about adding entries to this lookup definition.

A.4.11 Lookup.DBUM.Sybase.TargetRecon.Login.Validation

The Lookup.DBUM.Sybase.TargetRecon.Login.Validation lookup definition is used to configure validation of login entity attribute values that are fetched from the target system during target resource reconciliation.

The Lookup.DBUM.Sybase.TargetRecon.Login.Validation lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.4.12 Lookup.DBUM.Sybase.TargetRecon.QueryFilter

The Lookup.DBUM.Sybase.TargetRecon.QueryFilter lookup definition holds information about the filter parameters that you want to use while running the SQL query for target resource reconciliation.

The Lookup.DBUM.Sybase.TargetRecon.QueryFilter lookup definition is empty by default.

See [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#) for information about adding entries to this lookup definition.

A.4.13 Lookup.DBUM.Sybase.TargetRecon.Role.Mapping

The Lookup.DBUM.Sybase.TargetRecon.Role.Mapping lookup definition holds mapping between the Role multivalued attribute and the corresponding column name used in the stored procedure for target resource reconciliation.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Attribute name of the multivalued attribute
- **Decode:** The value can be specified in one of the following formats:
 - LOOKUP~COL_NAME

In this format:

- LOOKUP specifies that the data retrieved from the target system is lookup data.
- *COL_NAME* is the corresponding column name or column name alias used in the reconciliation query

You use this format if process form field corresponding to the Code Key value is a lookup type field.

- *COL_NAME*

This is the column name used in the reconciliation query corresponding to the value in the code key column.

If you want to add or modify the entries in this lookup definition, then you must specify values in the format described in this section.

Table A-68 lists the default entry in this lookup definition.

Table A-68 *Entries in the Lookup.DBUM.Sybase.TargetRecon.Role.Mapping Lookup Definition*

Code Key	Decode
Role	RoleName

A.4.14 Lookup.DBUM.Sybase.TargetRecon.User.Mapping

The Lookup.DBUM.Sybase.TargetRecon.User.Mapping lookup definition maps resource object fields with column names used in the stored procedure or SQL query for reconciliation. This lookup definition is used for performing target resource user reconciliation runs.

In this lookup definition, the Code Key contains the reconciliation field of the resource object.

For Code Key columns that store single-valued attributes, the Decode value can be one of the following formats:

- *COL_NAME* or *COL_NAME_ALIAS*

In this format, *COL_NAME* is the target system column name used in the reconciliation query. *COL_NAME_ALIAS* is the alias of the target system column names used in the reconciliation query.

You use this format if the target system contains a column corresponding to the resource object attribute that you added.

- *CONSTANT~CONSTANT_VALUE*

In this format, *CONSTANT* specifies that the data in this column is constant. *CONSTANT_VALUE* is value to be displayed in the corresponding OIM User form field in the Administrative and User Console.

You use this format if you want to display in a particular process form field, a constant value for all records.

- *COLUMN_NAME~LOOKUP_NAME*

In this format, *COLUMN_NAME* is the target system column name from which value is fetched. *LOOKUP_NAME* is the name of the lookup definition that maps values fetched from the target system with values that must be displayed in the process form field.

You use this format if you want to specify the format in which values fetched from the target system must be displayed in the process form field. By default, this lookup definition does not contain entries in this format. See [Section A.3.11, "Lookup.DBUM.Oracle.TargetRecon.Mapping"](#) for an example an using this format.

- `LOOKUP~COL_NAME`

In this format:

- `LOOKUP` specifies that the data retrieved from the target system is lookup data.
- `COL_NAME` is the corresponding column name or column name alias used in the reconciliation query

You use this format if process form field corresponding to the Code Key value is a lookup type field.

For Code Key columns that store multivalued attributes, the Decode value is specified in the following format:

`CHILD~MULTIVALUED_ATTR_CONFIG_LOOKUP`

In this format:

- `CHILD` specifies that the data in this column is the child attribute data
- `MULTIVALUED_ATTR_CONFIG_LOOKUP` is name of the lookup definition that holds configurable entries for the multivalued attribute.

By default, this lookup definition does not contain entries in this format. See [Section A.3.11, "Lookup.DBUM.Oracle.TargetRecon.Mapping"](#) for an example an using this format.

[Table A-69](#) lists the default entries in this lookup definition.

Table A-69 Entries in the *Lookup.DBUM.Sybase.TargetRecon.User.Mapping* Lookup Definition

Code Key	Decode
Database Group	DatabaseGroup
Database Name	DatabaseName
IT Resource	Sybase
Login Name	ParentLoginName
User Name	UserName

A.4.15 Lookup.DBUM.Sybase.TargetRecon.User.Transformation

The *Lookup.DBUM.Sybase.TargetRecon.User.Transformation* lookup definition is used to configure transformation of user entity attribute values that are fetched from the target system during target resource reconciliation.

The *Lookup.DBUM.Sybase.TargetRecon.Login.Transformation* lookup definition is empty by default.

See [Section 4.9, "Configuring Transformation of Data During Reconciliation"](#) for information about adding entries to this lookup definition.

A.4.16 Lookup.DBUM.Sybase.TargetRecon.User.Validation

The Lookup.DBUM.Sybase.TargetRecon.User.Validation lookup definition is used to configure validation of user entity attribute values that are fetched from the target system during target resource reconciliation.

The Lookup.DBUM.Sybase.TargetRecon.User.Validation lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.4.17 Lookup.DBUM.Sybase.TrustedRecon.Configuration

The Lookup.DBUM.Sybase.TrustedRecon.Configuration lookup definition holds connector configuration entries that are used during trusted source reconciliation.

[Table A-70](#) lists the default entries in this lookup definition.

Note: You cannot add entries to this lookup definition. However, you can modify the Decode values of the existing entries.

Table A-70 Entries in the Lookup.DBUM.Sybase.TrustedRecon.Configuration Lookup Definition

Code Key	Decode	Description
Reconciliation Class Name	oracle.iam.connectors.dbum.tasks.impl.DBUMSybaseReconciliationImpl	Name of the class that implements the logic for trusted source reconciliation.
Reconciliation Query Property File	Enter a value	Enter the full path and name of the file containing queries that must be run during reconciliation.
Reconciliation SQL Injection Keywords	NODATA	Enter the list of SQL keywords (separated by the tilde (~) character) that must not be used in the reconciliation query. The connector does not run a query (used for trusted source reconciliation) that contains any of the keywords listed in the Decode column.
Resource Exclusion List Lookup	Lookup.DBUM.Sybase.TrustedRecon.ExclusionList	See Section A.4.19, "Lookup.DBUM.Sybase.TrustedRecon.ExclusionList" for more information about this lookup definition.
Status Reconciliation Class Name	NODATA	You must enter a value for this entry only if your target system does not contain a column from which you can retrieve the status of a target system account. In Sybase, the Locked column holds the status of the target system account. Therefore, <i>do not</i> enter any value for this entry.
Target Date Format	NODATA	Enter the format in which date values are stored on the target system.
Use Status Reconciliation	No	Specifies whether you want to run reconciliation for the status of a target system user account. Note: Do not change the value of this entry.

A.4.18 Lookup.DBUM.Sybase.TrustedRecon.Delete.Mapping

The Lookup.DBUM.Sybase.TrustedRecon.Delete.Mapping lookup definition maps the resource object field with the primary key column name used in the reconciliation query (for retrieving all login entities from the target system). Note that this resource object field is the key field for reconciliation matching.

The Lookup.DBUM.Sybase.TrustedRecon.Delete.Mapping lookup definition is used during delete login trusted reconciliation runs.

During a delete login reconciliation run, the resource object field that you specify in this lookup definition is used for comparing target system accounts with existing OIM Users. During this comparison process, if no match is found between the target system account and OIM User, then the OIM User is deleted.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the resource object field, which is the key field for reconciliation matching
- **Decode:** Primary key column name used in the reconciliation query for performing delete login reconciliation

[Table A-71](#) lists the default entry in this lookup definition.

Table A-71 Entries in the Lookup.DBUM.Sybase.TrustedRecon.Delete.Mapping Lookup Definition

Code Key	Decode
User Login	Loginame

A.4.19 Lookup.DBUM.Sybase.TrustedRecon.ExclusionList

The Lookup.DBUM.Sybase.TrustedRecon.ExclusionList lookup definition holds user attributes of target system accounts that must not be reconciled during trusted source reconciliation.

The following is the format of the Code Key and Decode values for this lookup definition:

- **Code Key:** Resource object field name
- **Decode:** Resource object field values separated by the tilde (~) character

[Table A-39](#) lists the default entry in this lookup definition.

See Also: [Section 3.1.3, "Setting Up the ExclusionList Lookup Definition"](#) for information about adding or modifying entries in this lookup definition

Table A-72 Entries in the Lookup.DBUM.Sybase.TrustedRecon.ExclusionList Lookup Definition

Code Key	Decode
User Login	sa

A.4.20 Lookup.DBUM.Sybase.TrustedRecon.Mapping

The Lookup.DBUM.Sybase.TrustedRecon.Mapping lookup definition maps the fields of the OIM User form with corresponding column names used in the reconciliation query. This lookup definition is used for performing trusted source reconciliation.

In this lookup definition, the Code Key contains names of the fields on the OIM User form. The Decode value can be in one of the following formats:

- `COL_NAME` or `COL_NAME_ALIAS`

In this format, *COL_NAME* is the target system column name used in the reconciliation query. *COL_NAME_ALIAS* is the alias of the target system column name used in the reconciliation query.

You use this format if the target system contains a column corresponding to the resource object attribute.

For example, consider the User Login attribute on the resource object. The target system contains Loginame, which is a column corresponding to the User Login attribute. Therefore, the mapping is as follows:

Code Key: User Login

Decode: Loginame

- `CONSTANT~CONSTANT_VALUE`

In this format:

- `CONSTANT` specifies that the data in this column is constant.
- `CONSTANT_VALUE` is the value that must be displayed in the corresponding field of the OIM User form in the Administrative and User Console.

You this format if you want to set a constant value for a particular field on the OIM User form.

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 `CONSTANT~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.

By default, in this lookup definition, the Decode values for the Employee Type, Organization, and User Type Code Key columns have been set to constant values Full-Time, Xellerate Users, and End-User, respectively. However, depending on your requirement, you can change these values to one of the following:

- For the Employee Type Code Key, you can set one of the following constant values:
 - Full-Time
 - Part-Time
 - Temp
 - Intern
 - Consultant
- For the Organization Code Key, you can set one of the following constant values:

- Xellerate Users
 - Requests
- For the User Type Code Key, you can set one of the following constant values:
 - End-User
 - End-User Administrator
- *COLUMN_NAME~LOOKUP_NAME*
In this format:
 - *COLUMN_NAME* is the target system column name from which value is fetched.
 - *LOOKUP_NAME* is the name of the lookup definition that maps values fetched from the target system with values to be displayed in the OIM User form field.

You use this format if you want values fetched from the target system to be displayed in a format that is accepted by Oracle Identity Manager.

For example, consider the Status attribute of the resource object. The target system contains Locked, which is a column corresponding to the Status attribute of the resource object. However, we do not map the Status attribute to the Locked column for the following reason:

The status of an account in the target system can be reconciled from the Locked column, which can contain only the following values:

- YES
- NO

However, these statuses cannot be displayed in the Status field of the OIM User form. This is because Oracle Identity Manager accepts only one of the following values as the status of a user account:

- Active
- Disabled
- Disabled Until Start Date
- Deleted

Therefore, in order to display the status retrieved from the Locked column in a format that is accepted by Oracle Identity Manager, the Status resource object attribute has been mapped to

`Locked~Lookup.DBUM.TrustedRecon.StatusMapping`.

This implies that in the Code Key column of the `Lookup.DBUM.TrustedRecon.StatusMapping` lookup definition, the connector searches for the value that is fetched from the Locked column of the target system. Then, the corresponding Decode value is displayed as the status of the user account in Oracle Identity Manager. This is illustrated by the following example:

Suppose the value fetched from the Locked column for a particular user account on the target system is YES. In the Code Key column of the `Lookup.DBUM.TrustedRecon.StatusMapping` lookup definition, the connector searches for the value YES. The Decode value of the YES Code Key is Disabled. Therefore, in Oracle Identity Manager, the connector displays Disabled as the status of the user account.

See Also: [Section A.5.2,](#)
["Lookup.DBUM.TrustedRecon.StatusMapping"](#)

You can add to or remove entries in the Lookup.DBUM.Oracle.TrustedRecon.Mapping lookup definition. See [Section 4.2, "Adding or Removing Attributes for Reconciliation"](#) for information about adding or modifying entries in this lookup definition.

[Table A-73](#) lists the default entries in this lookup definition.

Table A-73 *Entries in the Lookup.DBUM.Sybase.TrustedRecon.Mapping Lookup Definition*

Code Key	Decode
Employee Type	CONSTANT~Full-Time
First Name	Loginame
Last Name	Loginame
Organization	CONSTANT~Xellerate Users
Status	Locked~Lookup.DBUM.TrustedRecon.StatusMapping
User Login	Loginame
User Type	CONSTANT~End-User

A.4.21 Lookup.DBUM.Sybase.TrustedRecon.QueryFilter

The Lookup.DBUM.Sybase.TrustedRecon.QueryFilter lookup definition is used for configuring limited reconciliation if your target system is configured as a trusted source. This lookup definition holds information about the filter parameters that you want to use while running the SQL query or stored procedure for trusted source reconciliation.

The Lookup.DBUM.Sybase.TargetRecon.QueryFilter lookup definition is empty by default.

See [Section 3.4.4.2, "Adding a Filter Parameter in the Reconciliation Query"](#) for information about adding entries to this lookup definition.

A.4.22 Lookup.DBUM.Sybase.TrustedRecon.Transformation

The Lookup.DBUM.Sybase.TrustedRecon.Transformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during trusted source reconciliation.

The Lookup.DBUM.Sybase.TrustedRecon.Transformation lookup definition is empty by default.

See [Section 4.9, "Configuring Transformation of Data During Reconciliation"](#) for information about adding entries to this lookup definition.

A.4.23 Lookup.DBUM.Sybase.TrustedRecon.Validation

The Lookup.DBUM.Sybase.TrustedRecon.Validation lookup definition is used to configure validation of attribute values that are fetched from the target system during trusted source reconciliation.

The Lookup.DBUM.Sybase.TrustedRecon.Validation lookup definition is empty by default.

See [Section 4.8, "Configuring Validation of Data During Reconciliation and Provisioning"](#) for information about adding entries to this lookup definition.

A.5 Other Lookup Definitions

This section discusses the following lookup definitions that are common to all target systems:

- [Section A.5.1, "Lookup.DBUM.TargetRecon.StatusMapping"](#)
- [Section A.5.2, "Lookup.DBUM.TrustedRecon.StatusMapping"](#)

A.5.1 Lookup.DBUM.TargetRecon.StatusMapping

The Lookup.DBUM.TargetRecon.StatusMapping lookup definition maps statuses of users accounts in the target system with the corresponding statuses to be displayed in the Status field of the OIM User form. This lookup definition is used for target system configured as a target resource.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Status of the user account fetched from the target system
- **Decode:** Corresponding status to be displayed in the Status field of the OIM User form

If you want to add or modify entries in this lookup definition, then you must specify entries in the format described in this section.

[Table A-74](#) lists the default entries in this lookup definition.

Table A-74 Entries in the Lookup.DBUM.TargetRecon.StatusMapping Lookup Definition

Code Key	Decode
0	Enabled
1	Disabled
EXPIRED & LOCKED	Disabled
LOCKED	Disabled
NO	Enabled
OPEN	Enabled
YES	Disabled

A.5.2 Lookup.DBUM.TrustedRecon.StatusMapping

The Lookup.DBUM.TrustedRecon.StatusMapping lookup definition maps statuses of users accounts in the target system with the corresponding statuses to be displayed in the Status field of the OIM User form. This lookup definition is used for target system configured as a trusted source.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Status of the user account fetched from the target system
- **Decode:** Corresponding status to be displayed in the Status field of the OIM User form

If you want to add or modify entries in this lookup definition, then you must specify entries in the format described in this section.

[Table A-75](#) lists the default entries in this lookup definition.

Table A-75 *Entries in the Lookup.DBUM.TrustedRecon.StatusMapping Lookup Definition*

Code Key	Decode
0	Active
1	Disabled
EXPIRED	Disabled
EXPIRED & LOCKED	Disabled
LOCKED	Disabled
NO	Active
OPEN	Active
YES	Disabled

Index

A

additional files, 1-2
Administrative and User Console, 2-9
architecture, 1-2

B

batched reconciliation, 1-12

C

certified components, 1-1
certified languages, 1-2
changing input locale, 2-10
clearing server cache, 2-10
components, certified, 1-1
configuring connector
 database object-level privileges, 4-50
 database vault realms, 2-14, 4-60
configuring provisioning, 3-27
configuring SSL, 1-14, 2-15
configuring transformation, 1-13, 4-49
configuring validation, 1-13, 4-46
Connection Properties parameter, 2-20, 2-21, 2-22
connector architecture, 1-2
connector features, 1-10
connector files and directories
 description, 2-1
 installation media file, 2-1
Connector Installer, 2-6
connector installer, 2-6
connector release number, determining, 2-3

D

data encryption and integrity, 2-15, 2-16, 2-17, 2-19
Database URL parameter, 2-20, 2-21, 2-22
defining
 IT resources, 2-26
determining release number of connector, 2-3

E

enabling logging, 2-11
external code files, 1-2, 2-5
externally-authenticated users, 1-11, 1-15, 3-25, 3-26

F

features of connector, 1-10
files
 additional, 1-2
 external code, 1-2
 See also XML files
Files and Directories, 2-1
files and directories of the connector
 See connector files and directories
filtered reconciliation
 See limited reconciliation, 1-12
full reconciliation, 1-12

G

globalization features, 1-2
globally-authenticated users, 1-11, 1-15, 3-25

I

IBM DB2/UDB, 2-16, 2-19, 2-20
incremental reconciliation, 1-12
input locale changing, 2-10
installation, 2-6
 preinstallation, 2-1
installing connector, 2-1, 2-6, 2-8
IT resources
 defining, 2-26
 parameters, 2-26

L

limited reconciliation, 1-12
logging enabling, 2-11
lookup definitions
 Lookup.DBUM.DB2.Configuration, 1-18, 2-20, 2-28, 3-2, 4-28, A-2
 Lookup.DBUM.DB2.Error.Mapping, 1-18, A-2, A-3
 Lookup.DBUM.DB2.ExclusionList, 1-18, A-4
lookup field synchronization, 1-15, 3-1, 3-4
lookup fields, 1-15, 3-1, 3-4

M

Microsoft SQL Server, 2-17, 2-21

multilanguage support, 1-2
multiple trusted source reconciliation, 4-45

O

object-level privileges, 1-11, 4-50
Oracle Database, 2-17, 2-22
Oracle Database Vault, 1-14, 2-14, 2-27, 4-60
Oracle Database Vault realms, 1-14
Oracle Identity Manager Administrative and User Console, 2-9
Oracle Identity Manager database table, 2-10

P

parameters of IT resources, 2-26
provider parameters
 Connection Properties, 2-20, 2-21, 2-22
 Database URL, 2-20, 2-21, 2-22
provisioning
 fields, 1-29, 1-32
 identity fields, 1-32
 module, 1-29
provisioning functions, 1-29
 IBM DB2 UDB, 1-29
 Microsoft SQL Server, 1-30
 Oracle Database, 1-31
 Sybase, 1-31

R

Reconciliation, 1-3
reconciliation
 batched, 1-12
 full, 1-12
 incremental, 1-12
reconciliation action rule
 target resource reconciliation, 1-27
 trusted source reconciliation, 1-27
reconciliation query
 configuring, 4-45
 modifying, 4-45
reconciliation rule
 target resource reconciliation, 1-26
 trusted source reconciliation, 1-26, 1-27
reconciliation scheduled tasks, 3-10
release number of connector, determining, 2-3

S

scheduled tasks
 defining, 3-19
 reconciliation, 3-10
server cache, clearing, 2-10
stages of connector deployment
 installation, 2-6
 postinstallation, 2-8
 preinstallation, 2-1
supported
 releases of Oracle Identity Manager, 1-2
 target systems, 1-2

SVP table, 2-10

T

target resource reconciliation, 1-21, 3-4
 adding new fields, 4-4, 4-7, 4-11, 5-13
 reconciliation action rule, 1-27
 reconciliation rule, 1-26
target system, multiple installations, 4-26
target systems
 child, 1-2
 master, 1-2
 supported, 1-2
temporary tables, 1-22
trusted resource reconciliation
 reconciliation rule, 1-26, 1-27
trusted source reconciliation, 4-45
 adding new fields, 4-4
 reconciliation action rule, 1-27