Oracle® Identity Manager

Connector Guide for Oracle Identity Cloud Services

Release 11.1.1
E71438-05
May 2020

Oracle Identity Manager Connector Guide for Oracle Identity Cloud Services, Release 11.1.1

E71438-05

Primary Author: Gowri.G.R

Contributors: Alankrita Prakash

Contents

Preface

What’s New in Oracle Identity Manager Connector for Oracle Identity Cloud Service?

1 About the Oracle Identity Cloud Service Connector

2 Deploying the Oracle Identity Cloud Service Connector

3 Using the Oracle Identity Cloud Service Connector

4 Extending the Functionality of the Oracle Identity Cloud Service Connector

A Files and Directories on the Installation Media

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Oracle Identity Cloud Services.

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

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

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

Conventions

The following text conventions are used in this document:

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

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

What’s New in Oracle Identity Manager Connector for Oracle Identity Cloud Service?

This chapter provides an overview of the updates made to the software and documentation for the Oracle Identity Cloud Services connector in release 11.1.1.5.0.

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

- Software Updates

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

- Documentation-Specific Updates

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

Software Updates

These are the updates made to the connector software.

Software Updates in Release 11.1.1.5.0

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

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 11.1.1.5.0

The following documentation-specific update has been made in revision "5" of this guide:

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

The following documentation-specific update has been made in revision "4" of this guide:

All instances of "IDCS Connectors" is replaced with "Oracle Identity Cloud Service connectors" throughout the guide.

The following documentation-specific update has been made in revision “3” of this guide:

The "Oracle Identity Manager" row of Table 1-1, "Certified Components" has been renamed as "Oracle Identity Governance or Oracle Identity Manager" and has been updated for Oracle Identity Governance for 12*c* (12.2.1.3.0) certification.

The following documentation-specific update has been made in revision “2” of this guide:

The description of the parameter “baseURI” in Table 2-1 has been modified.

1 About the Oracle Identity Cloud Service Connector

The Oracle Identity Cloud Service connector integrates Oracle Identity Manager (OIM) with Oracle Identity Cloud Service.

Oracle Identity Manager is a centralized identity management solution that provides self service, compliance, provisioning and password management services for applications residing on-premise or on the Cloud. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. The Oracle Identity Cloud Service connector enables you to use Oracle Identity Cloud Service as a managed (target) resource Oracle Identity Manager.

> **Note:**
>
> In this guide, the term **target system** is sometimes used to refer to Oracle Identity Cloud Service.

The following topics provide a high-level overview of the Oracle Identity Cloud Service connector:

- Introduction to the Oracle Identity Cloud Service Connector
- Certified Components for the Oracle Identity Cloud Service Connector
- Certified Languages for the Oracle Identity Cloud Service Connector
- Connector Architecture
- Use Cases Supported by the Oracle Identity Cloud Service Connector
- Features of the Connector
- Lookup Definitions Used During Connector Operations
- Connector Objects Used During Target Resource Reconciliation
- Connector Objects Used During Provisioning
- Roadmap for Deploying and Using the Connector

1.1 Introduction to the Oracle Identity Cloud Service Connector

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

In the account management (target resource) mode of the connector, the data about the users created or modified directly on the target system can be reconciled into

Oracle Identity Manager. This data is used to provision (allocate) new resources or update resources already assigned to Oracle Identity Manager users. You can also use Oracle Identity Manager to provision or update Oracle Identity Cloud Service resources (accounts) assigned to Oracle Identity Manager users. These provisioning operations performed on Oracle Identity Manager translate into the creation or updates to target system accounts.

1.2 Certified Components for the Oracle Identity Cloud Service Connector

These are the software components and their versions required for installing and using the Oracle Identity Cloud Service connector.

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

Table 1-1 Certified Components

Item	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) and any later BP in this release track
Target System	Oracle Identity Cloud Service 16.3.6 or later
Connector Server	11.1.2.1.0
Connector Server JDK	JDK 1.6 or later

1.3 Certified Languages for the Oracle Identity Cloud Service Connector

The connector supports the following languages:

- Arabic
- Chinese Simplified
- Chinese Traditional
- Danish
- English
- French
- German
- Italian

- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

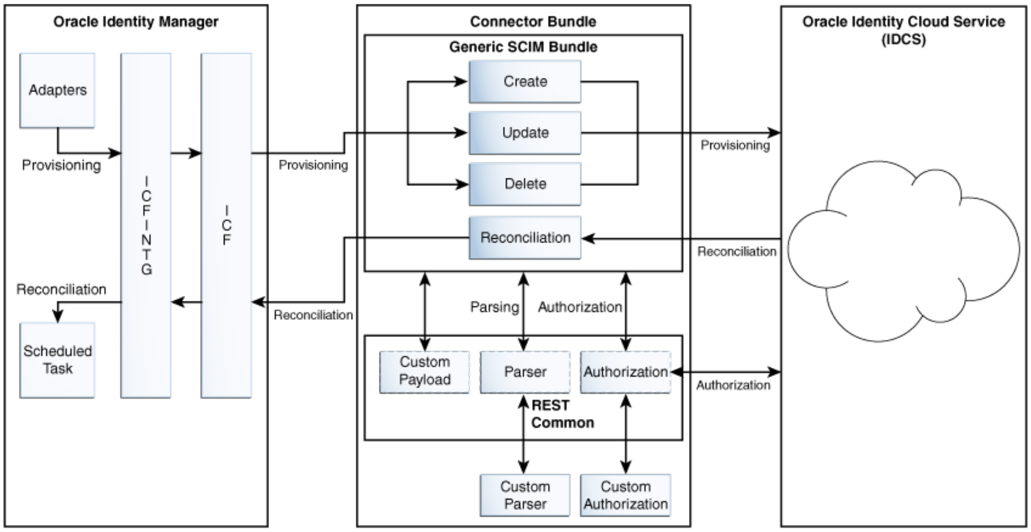
1.4 Architecture of the Oracle Identity Cloud Service Connector

The Oracle Identity Cloud Service connector is implemented by using the Identity Connector Framework (ICF).

The ICF is a component that provides basic reconciliation and provisioning operations that are common to all Oracle Identity Manager connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering. The ICF is shipped together with Oracle Identity Manager.

Figure 1–1 shows the integration of on-premise Oracle Identity Manager with the Identity Cloud Service. The Oracle Identity Cloud Service connector follows a hybrid data management system providing opportunities for organizations having roots in Oracle Identity Manager but with an intent of migrate to the Oracle Identity Cloud Service framework. As the diagram suggests, Oracle Identity Cloud Service connector can carry out provisioning and reconciliation operations on Oracle Identity Cloud Service. In the diagram, the connector bundle is responsible for interacting with Oracle Identity Cloud Service, which is a SCIM compliant target. Therefore, the connector package uses the Generic SCIM bundle. Parsing and authorization is handled by the REST common bundle, which is a part of the Generic SCIM bundle. By default, it supports OAuth 2.0 Resource Owner Password authentication. In addition, custom parser and custom authorization can be implemented to enhance the connector.

Figure 1-1 Connector Architecture



1.5 Use Cases Supported by the Oracle Identity Cloud Service Connector

The promise of simplified deployment, reduced acquisition costs, reduced management overhead and quick time to value are driving organizations to adopt SaaS applications to meet the various business needs. Since recently, very large number of applications are being developed in the cloud. Oracle Identity Cloud Service provides a set of foundational services for Oracle’s Public Cloud applications and their customers by delivering simple, secure integration with Oracle and third party SaaS applications for customers interested in a Public Identity as a service offering from Oracle.

Similarly, many of Oracle’s existing customers using on-premise IDM are also moving their HCM, CRM, directories and other applications from on-premise to the Cloud. Customers also want to move their IDM services into cloud. To keep pace with the changing trends and to support customers who are adopting cloud, Oracle’s on-premise Identity Management software, Oracle Identity Manager provides a new integration called the Oracle Identity Cloud Service connector. This integration will not only facilitate customer’s migration from on-premise to cloud but it will also support the hybrid strategy where customers can have both on-premise IDM and cloud IDM working together to achieve greater value.

Let’s say ACME Corporation has been using Oracle Identity Manager for some time to manage its identities and various applications on premise. The long-term plan of ACME Corporation is to move into cloud but they want to achieve this in phases. At one point of time, they have both on-premise and cloud applications. As part of this move, they now have Oracle Identity Cloud Service to manage cloud applications but for the time being, they want to use only Oracle Identity Manager to manage identities in their ecosystem.

Oracle Identity Cloud Service connector will facilitate ACME Corporation in achieving this use case by providing Oracle Identity Cloud Service user and group management for the cloud applications.

After installing the Oracle Identity Cloud Service connector, customer can manage complete lifecycle of the users and groups in Oracle Identity Cloud Service from Oracle Identity Manager. Using this integration, ACME Corporation can create, update, enable, and disable Oracle Identity Cloud Service users accessing the cloud applications. Also, it can assign or revoke Oracle Identity Cloud Service groups for a particular user accessing the cloud applications using Oracle Identity Manager.

With the RBAC policies defined in Oracle Identity Manager, granting or revoking appropriate groups using connector will ensure that user has proper, authorized access to the cloud applications registered with the Oracle Identity Cloud Service.

1.6 Features of the Oracle Identity Cloud Service Connector

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

- Support for Account and Group Provisioning
- Full and Incremental Reconciliation

- Limited Reconciliation
- Batched Reconciliation
- Transformation and Validation of Account Data
- Reconciliation of Deleted User Accounts and Groups
- Support for the Connector Server

1.6.1 Support for Account and Group Provisioning

You can use the connector to provision Oracle Identity Cloud Service user accounts and groups.

You can create a new user in Oracle Identity Manager by using the Create User page. The connector provides separate process forms and resource objects for user account and group operations.

1.6.2 Full and Incremental Reconciliation

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

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

1.6.3 Limited Reconciliation

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

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

1.6.4 Support for Batched Reconciliation

Depending on the number of records to be reconciled, a batched reconciliation operation can be configured.

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

1.6.5 Transformation and Validation of Account Data

Transformation and validation of account data can be configured during reconciliation and provisioning operations.

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. The following sections provide more information:

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

1.6.6 Reconciliation of Deleted User Accounts and Groups

You can configure the connector to fetch details of deleted target system users and groups in the target resource mode.

You can configure the connector for reconciliation of deleted user accounts and groups. In target resource mode, if a user record is deleted or a token is unassigned on the target system, then the corresponding Oracle Identity Cloud Service resource is revoked from the Oracle Identity Manager User.

See IDCS Delete User Reconciliation and IDCS Delete Group Reconciliation for more information about scheduled jobs used for reconciling deleted user records and groups.

1.6.7 Support for the Connector Server

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

> **See Also:**
>
> Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about the installation options for this connector

1.7 Lookup Definitions Used During Connector Operations

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

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

- Lookup Definitions Synchronized With the Target System
- Preconfigured Lookup Definitions

1.7.1 Lookup Definitions Synchronized With the Target System

During a provisioning operation, you use a lookup field on the process form to select a single value from a set of values. For example, you may want to select a group from the Groups lookup field to specify the group being assigned to the user. 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 specific fields in the target system to lookup definitions in Oracle Identity Manager.

After you deploy the connector, the following lookup definitions, which are used as an input source for lookup fields, are automatically created in Oracle Identity Manager:

- Lookup.IDCS.Groups
- Lookup.IDCS.Managers

The Lookup.IDCS.Groups and Lookup.IDCS.Managers lookup definitions are populated with values fetched from the target system by the scheduled jobs for lookup field synchronization.

During a provisioning operation, you use the Group lookup field on the process form to specify a group and the Managers lookup definition to specify users already assigned as managers. The Groups and Managers lookup fields are populated with values from the Lookup.IDCS.Groups and Lookup.IDCS.Managers lookup definitions, which are automatically created on Oracle Identity Manager when you deploy the connector.

By default, these lookup definitions are empty. They are populated with values fetched from the target system when you run the scheduled jobs for lookup field synchronization. For example, when you run the scheduled job, all groups on the target system are fetched to Oracle Identity Manager and populated in the Lookup.IDCS.Groups lookup definition.

After synchronization, the data in each of the lookup definitions is stored in the following format:

- **Code Key:** *<IT_RESOURCE_KEY>~<FIELD_VALUE_ID>*

  In this format:

  - *IT_RESOURCE_KEY* is the numeric code assigned to an IT resource in Oracle Identity Manager.
  - *FIELD_VALUE_ID* is the ID of the target system field value.

    For example, for the Lookup.IDCS.Groups lookup definition, the code key value for one of its entries is `89~1b5d6697-f4a6-4f03-8df7-4fae1512fd16`. In this example, `89` is the numeric code assigned to the IT resource associated with the target system and `1b5d6697-f4a6-4f03-8df7-4fae1512fd16` is the ID of the Group in the target system.

- **Decode:** *<IT_RESOURCE_NAME>~<FIELD_VALUE>*

  In this format:

  - *IT_RESOURCE_NAME* is the name of the IT resource in Oracle Identity Manager.
  - *FIELD_VALUE* is the value of the field in the target system.

    For example, for the Lookup.IDCS.Groups lookup definition, the decode value for one of its entries is `IDCS~HR`. In this example, `IDCS` is the name of the IT resource and `HR` is the value of the Group field in the target system.

Table 1-2 shows sample entries in the Lookup.IDCS.Groups lookup definition.

Table 1-2 Sample Entries in the Lookup.IDCS.Groups Lookup Definition

Code Key	Decode
IDCS~Finance	89~9b3b3faf-e7fb-427e-8038-b8021cfbab30
IDCS~HR	89~eb1b204e-2de0-41ec-98e9-1c33684d698a
IDCS~ISP	89~4457f158-d1ec-47f2-aeb4-79d5a2be0e38

1.7.2 Preconfigured Lookup Definitions

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

The other lookup definitions are as follows:

- Lookup.IDCS.Configuration
- Lookup.IDCS.GM.Configuration
- Lookup.IDCS.GM.ProvAttrMap
- Lookup.IDCS.GM.ReconAttrMap
- Lookup.IDCS.UM.Configuration
- Lookup.IDCS.UM.ProvAttrMap
- Lookup.IDCS.UM.ReconAttrMap
- Lookup.IDCS.UserTypes
- Lookup.IDCS.Organizations

1.7.2.1 Lookup.IDCS.Configuration

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

> **Note:**
>
> The values for these lookup definitions are preconfigured and cannot be modified.

Table 1-3 lists the default entries in this lookup definition.

Table 1-3 Entries in the Lookup.IDCS.Configuration lookup definition

Code	Decode	Description
Any Incremental Recon Attribute Type	true	By default, during incremental reconciliation, Oracle Identity Manager accepts time stamp information sent from the target system only in Long datatype format. A decode value of True for the Incremental Recon Attribute Type entry indicates that Oracle Identity Manager will accept time stamp information in any datatype format.

Table 1-3 (Cont.) Entries in the Lookup.IDCS.Configuration lookup definition

Code	Decode	Description
attrToOClassMapping	"__ACCOUNT__.groups=Groups"	This entry denotes that the groups attribute of the __ACCOUNT__ object class is mapped to the Groups object class on the target.
Bundle Name	org.identityconnectors.genericscim	This entry holds the name of the connector bundle package.
Bundle Version	1.0.1115	This entry holds the version of the connector bundle.
Connector Name	org.identityconnectors.genericscim.GenericSCIMConnector	This entry holds the name of the connector class.
customPayload	"__ACCOUNT__.password.UpdateOp={\"userName\":\"$(__ACCOUNT__.userName)$\",\"password\":\"$(__ACCOUNT__.password)$\",\"schemas\":[\"urn:ietf:params:scim:schemas:oracle:idcs:UserPasswordChanger\"]}","__ACCOUNT__.groups.AddOp={\"schemas\":[\"urn:ietf:params:scim:api:messages:2.0:PatchOp\"],\"Operations\":[{\"op\":\"add\",\"path\":\"members\",\"value\":[{\"value\":\"$(__ACCOUNT__.__UID__)$\"}]}]}"	This entry holds the payloads for all operations that are not in the standard format.
Group Configuration Lookup	Lookup.IDCS.GM.Configuration	This entry holds the name of the lookup definition that contains group-specific configuration properties.
httpOperationTypes	"__ACCOUNT__.password.UpdateOp=PUT"	This entry indicates that for a Password Update operation, the target needs a PUT operation instead of PATCH.
jsonResourcesTag	Resources	This JSON tag value is used during reconciliation for parsing multiple entries in a single response payload.
nameAttributes	"Users=userName","Groups=displayName"	This entry indicates which attributes need to be treated as the __NAME__ attribute for which Object class.
passwordAttributes	"Users=password"	This entry indicates which attributes need to be treated as the __PASSWORD__ attribute for which object class.

Table 1-3 (Cont.) Entries in the Lookup.IDCS.Configuration lookup definition

Code	Decode	Description
relURLs	"__ACCOUNT__.password.UpdateOp=/UserPasswordChanger/$(__ACCOUNT__.__UID__)$"	This entry holds the relative URL of every object class supported by this connector and the connector operations that can be performed on these object classes. This entry indicates that for a Password Update operation, the /UserPasswordChanger endpoint needs to be hit, instead of the default /Users end point.
scimVersion	17	This indicates the SCIM version on which the target is implemented.
statusAttributes	"Users=active"	This entry lists the name of the target system attribute that holds the status of an account. This entry indicates the status field: The __ENABLE__ field on the target for which object class.
uidAttributes	"Users=id","Groups=id"	"This entry holds the UID attribute for the object which are handled by the connectors. For example for User accounts the UID attribute is ID.
reconSortByAttrs	"Users=id","Groups=id"	This entry holds the attribute used for sorting the records during a reconciliation operation.
User Configuration Lookup	Lookup.IDCS.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties.

1.7.2.2 Lookup.IDCS.GM.Configuration

The Lookup.IDCS.GM.Configuration lookup definition holds configuration entries that are specific to the group object type.

This lookup definition is used during group management operations when your target system is configured as a target resource.

Table 1-4 lists the default entries in this lookup definition.

Table 1-4 Lookup.IDCS.GM.Configuration lookup definition

Code	Decode	Description
Provisioning Attribute Map	Lookup.IDCS.GM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.IDCS.GM.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.IDCS.GM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.IDCS.GM.ReconAttrMap for more information about this lookup definition.

1.7.2.3 Lookup.IDCS.GM.ProvAttrMap

The Lookup.IDCS.GM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes.

This lookup definition is preconfigured and used during group provisioning operations. Table 1-13 lists the default entries.

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

1.7.2.4 Lookup.IDCS.GM.ReconAttrMap

The Lookup.IDCS.GM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes.

This lookup definition is preconfigured and used during target resource reconciliation of groups. Table 1-9 lists the default entries.

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

1.7.2.5 Lookup.IDCS.UM.Configuration

The Lookup.IDCS.UM.Configuration lookup definition holds configuration entries that are specific to the user object type.

This lookup definition is used during user management operations when your target system is configured as a target resource.

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

Table 1-5 Entries in the Lookup.IDCS.UM.Configuration Lookup Definition

Code	Decode	Description
Provisioning Attribute Map	Lookup.IDCS.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.IDCS.UM.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.IDCS.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.IDCS.UM.ReconAttrMap for more information about this lookup definition.

1.7.2.6 Lookup.IDCS.UM.ProvAttrMap

The Lookup.IDCS.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes.

This lookup definition is preconfigured and used during provisioning. Table 1-12 lists the default entries.

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

1.7.2.7 Lookup.IDCS.UM.ReconAttrMap

The Lookup.IDCS.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes.

This lookup definition is preconfigured used during target resource reconciliation. Table 1-8 lists the default entries.

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

1.7.2.8 Lookup.IDCS.UserTypes

The Lookup.IDCS.UserTypes lookup definition holds the list of user types.

This is a static lookup definition. You cannot modify or add entries in this lookup definition.

Table 1-6 lists the default entries in this lookup definition.

Table 1-6 Entries in the Lookup.IDCS.UserTypes Lookup Definition

Code Key	Decode
contractor	CONTRACTOR

Table 1-6 (Cont.) Entries in the Lookup.IDCS.UserTypes Lookup Definition

Code Key	Decode
employee	EMPLOYEE
external	EXTERNAL
intern	INTERN
service	SERVICE
temp	TEMP

1.7.2.9 Lookup.IDCS.Organizations

The Lookup.IDCS.Organizations lookup definition holds the list of organizations.

This is a static lookup definition. The entries of this lookup needs to be updated manually based on the Organizations on the target.

Table 1-7 lists the default entry in this lookup definition.

Table 1-7 Entries in the Lookup.IDCS.Organizations Lookup Definition

Code Key	Decode
Xellerate Users	Xellerate Users

1.8 Connector Objects Used During Target Resource Reconciliation

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

The IDCS Target Resource User Reconciliation scheduled job is used to initiate a reconciliation run. This scheduled job is discussed in Reconciliation Scheduled Jobs for Oracle Identity Cloud Service Connector.

> **See Also:**
>
> Managing Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for generic information about connector reconciliation

This section contains the following topics related to connector objects:

- User Fields for Target Resource Reconciliation
- Group Fields for Reconciliation
- Reconciliation Rules for Target Resource Reconciliation
- Reconciliation Action Rules for Oracle Identity Cloud Service

1.8.1 User Fields for Target Resource Reconciliation

The Lookup.IDCS.UM.ReconAttrMap lookup definition maps resource object fields with target system attributes.

These lookup definitions are used for performing target resource reconciliation runs.

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

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

Table 1-8 lists the entries in the Lookup.IDCS.UM.ReconAttrMap lookup definition.

Table 1-8 Entries in the Lookup.IDCS.UM.ReconAttrMap Lookup Definition

Code Key	Decode
Email	__ACCOUNT__.emails.value,type:work,primary:true
Employee Number	employeeNumber
First Name	name.givenName
Groups~Group Value[LOOKUP]	__ACCOUNT__.groups~__ACCOUNT__.groups~value
Id	__UID__
Last Name	name.familyName
Manager[LOOKUP]	manager.value
Middle Name	name.middleName
Organization	organization
Status	__ENABLE__
User Name	__NAME__
User Type	userType

1.8.2 Group Fields for Reconciliation

The Lookup.IDCS.GM.ReconAttrMap lookup definition maps group resource object fields and target system attributes.

This lookup definition is used for performing target resource group reconciliation runs.

Table 1-9 lists the entries in the Lookup.IDCS.GM.ReconAttrMap lookup definition.

Table 1-9 Entries in the Lookup.IDCS.GM.ReconAttrMap Lookup Definition

Code Key	Decode
Description	description
Group Id	__UID__
Group Name	__NAME__
OIM Organization Name	OIM Organization Name

1.8.3 Reconciliation Rules for Target Resource Reconciliation

The reconciliation engine uses rules to determine the identity to which Oracle Identity Manager must assign a newly discovered account on the target system.

This section discuss the following topics related to users and groups reconciliation rule for target resource reconciliation:

- Reconciliation Rule for Users
- Reconciliation Rule for Groups
- Viewing Reconciliation Rules in the Design Console

1.8.3.1 Reconciliation Rule for Users

The Oracle Identity Cloud Service connector can perform reconciliation of both users and groups. Therefore, the connector has reconciliation rules defined specifically for users.

Rule name: IDCS User Recon Rule

Rule element: User Login Equals User Name

In this rule:

- `User Login` is the User ID field of the Oracle Identity Manager User form.
- `User Name` is the Username attribute for users on the target.

1.8.3.2 Reconciliation Rule for Groups

The Oracle Identity Cloud Service connector can perform reconciliation of both users and groups. Therefore, the connector has reconciliation rules defined specifically for groups.

Rule name: IDCS Groups Recon Rule

Rule element: Organization Name Equals OIM Org Name.

In this rule:

- `Organization Name` is the Organization Name field of the Oracle Identity Manager User form.
- `OIM Org Name` is the organization name of the groups in Oracle Identity Manager. OIM Org Name is the value specified in the Organization Name attribute of the IDCS Group Recon scheduled job.

1.8.3.3 Viewing Reconciliation Rules in the Design Console

After you deploy the connector, you can view the reconciliation rules for users and groups on the Reconciliation Rule Builder form in Oracle Identity Manager Design Console.

To view the reconciliation rule for target resource reconciliation of users and groups:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tool**s and then double-click **Reconciliation Rules.**

3. Search for and open one of the following:
    - For Users: **IDCS User Recon Rule**
    - For Groups: **IDCS Groups Recon Rule**

1.8.4 Reconciliation Action Rules for Oracle Identity Cloud Service

Reconciliation action rules specify the actions that the connector must perform depending on whether or not matching Oracle Identity Cloud Service resources or Oracle Identity Manager Users are found when the reconciliation rule is applied.

> **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.

The following sections provide information about the action rules for this connector:

- Reconciliation Action Rules
- Viewing Reconciliation Action Rules Reconciliation in Design Console

1.8.4.1 Reconciliation Action Rules

Reconciliation action rules specify the actions the connector must perform based on the result of the processing of a reconciliation event. The reconciliation action rules for both users and groups are the same.

Table 1-10 lists the action rules for target resource reconciliation.

Table 1-10   Action Rules for Reconciliation for Target

Rule Condition	Action
No matches found	None
One entity match found	Establish link
One process match found	Establish link

1.8.4.2 Viewing Reconciliation Action Rules Reconciliation in Design Console

After you deploy the connector, you can view the reconciliation action rules for users and groups reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects.**
3. Search for and open one of the following resource objects:
    - For Users: **IDCS User**
    - For Groups: **IDCS Group**

4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules that are defined for this connector.

1.9 Connector Objects Used During Provisioning

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

This section provides information related to connector objects used during a provisioning operation:

- Provisioning Functions
- User Fields for Provisioning
- Group Fields for Provisioning

1.9.1 Provisioning Functions

These are the supported provisioning functions and the adapters that perform these functions for the Oracle Identity Cloud Service connector.

The Adapter column in Table 1-11 provides the name of the adapter that is used when the function is performed.

> **See Also:**
>
> Types of Adapters in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for generic information about process tasks and adapters

Table 1-11 Provisioning Functions

Function	Adapter
Disable a user	adpADIDCDISABLEUSER
Add child data	adpIDCSADDCHILDDATA
Bulk update adapter	adpIDCSBULKUPDATEADAPTER
Create object	adpIDCSCREATEOBJECT
Delete object	adpIDCSDELETEOBJECT
Enable user	adpIDCSENABLEUSER
Prepopulate adapter	adpIDCSPREPOPULATEADAPTER
Remove child data	adpIDCSREMOVECHILDDATA
Update child data	adpIDCSUPDATECHILDDATA
Update object	adpIDCSUPDATEOBJECT

Note:

The password update task does not work with the parent form. It works only with the reset password operation.

1.9.2 User Fields for Provisioning

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

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

- **Code Key:** Name of the process form field
- **Decode:** Name of the target system user attribute

Table 1-12 lists default entries in the Lookup.IDCS.UM.ProvAttrMap lookup definition.

Table 1-12 Entries in the Lookup.IDCS.UM.ProvAttrMap lookup definition

Code	Decode
Creation Mechanism	creationMechanism
Email	__ACCOUNT__.emails.value,type:work,primary:true
Employee Number	employeeNumber
First Name	name.givenName
Id	__UID__
Last Name	name.familyName
Manager[LOOKUP]	manager.value
Middle Name	name.middleName
Organization	organization
Password	__PASSWORD__
Status	__ENABLE__
UD_IDCS_UGP~Group Value[LOOKUP]	__ACCOUNT__.groups~__ACCOUNT__.groups~value
User Name	__NAME__
User Type	userType

1.9.3 Group Fields for Provisioning

The Lookup.IDCS.GM.ProvAttrMap lookup definition maps user resource object fields and target system attributes. This lookup definition is used for performing group provisioning operations.

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

- **Code Key:** Name of the process form field
- **Decode:** Name of the target system group attribute

Table 1-13 lists default entries in the Lookup.IDCS.GM.ProvAttrMap lookup definition.

Table 1-13   Entries in the Lookup.IDCS.GM.ProvAttrMap lookup definition

Code	Decode
Description	description
Group Id	__UID__
Group Name	__NAME__
OIM Organization Name	OIM Organization Name

1.10 Roadmap for Deploying and Using the Connector

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

- Deploying the Oracle Identity Cloud Service Connector describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Using the Oracle Identity Cloud Service Connector describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Extending the Functionality of the Oracle Identity Cloud Service Connector describes procedures that you can perform if you want to extend the functionality of the connector.
- Files and Directories on the Installation Media lists the files and directories that comprise the connector installation media.

2

Deploying the Oracle Identity Cloud Service Connector

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

The following topics provide details on these stages:

- Preinstallation
- Installation
- Postinstallation

2.1 Preinstallation

Preinstallation for the Oracle Identity Cloud Service connector involves registering and generating a client application (that is, the Oracle Identity Cloud Service connector) with the target system so that the connector can access Oracle Identity Cloud Service Graph APIs. It also involves creating a target system account for connector operations.

Preinstallation involves performing the following tasks on the target system:

1. Register and generate an application. Because the connector operates as a multitarget environment, the application needs to be registered on the Oracle Identity Cloud Service environment for authentication.
2. Specify the permissions to choose an application type to configure your own application in the cloud. To do so:
    a. Select **Resource Owner** as the allowed grant type for this application.
    b. Select the **Client has Access to Identity Cloud Service Admin APIs** checkbox.
    c. Select **Identity Domain Administrator** and **Me**. This provides administrator permissions to any third-party client using this application to perform identity operations such as User and Group management.
    d. In the Register the Resource of the Application page, select the **Register Resources** radio button.
3. Create a target system account with administrative privileges to enable connector operations such as reconciliation and provisioning.

2.2 Installation

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

The following topics discuss installing the Oracle Identity Cloud Service connector:

- Understanding Installation

- Running the Connector Installation
- Configuring the IT Resource for the Target System
- Deploying the Connector in a Connector Server

2.2.1 Understanding Installation of the Oracle Identity Cloud Service Connector

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

Depending on where you want to run the generated connector, the connector provides the following installation options:

- Run the connector code locally in Oracle Identity Manager. To run the connector code locally in Oracle Identity Manager, perform the procedure described in Installing the Connector in Oracle Identity Manager. In this scenario, you deploy the connector in Oracle Identity Manager.
- Run the connector code remotely in a Connector Server. To run the connector code remotely in a Connector Server, perform the procedures described in Installing the Connector in Oracle Identity Manager and Deploying the Connector in a Connector Server. In this scenario, you deploy the connector in Oracle Identity Manager, and then, deploy the connector bundle in a Connector Server. For information about installing, configuring, and running the Connector Server, and then installing the connector in a Connector Serve, see Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* .

2.2.2 Installing the Connector in Oracle Identity Manager

Installation on Oracle Identity Manager consists of the following procedures:

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

2.2.2.1 Running the Connector Installer

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

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory: `OIM_HOME/server/ConnectorDefaultDirectory`.
2. Log in to Oracle Identity System Administration.
3. From the left pane, expand the **Provisioning Configuration** tab and click **Manage Connector.**
4. In the Manage Connector page, click **Install.**
5. From the Connector List, select **IDCS Connector *RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files

you copy into the default connector installation directory mentioned in the *OIM_HOME/server/ConnectorDefaultDirectory.*

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

a. In the **Alternative Directory** field, enter the full path and name of that directory.
b. To repopulate the list of connectors in the Connector List list, click **Refresh.**
c. From the Connector List, select **IDCS 11.1.1.5.0.**

6. Click **Load.**
7. To start the installation process, click **Continue.**

   The following tasks are performed in sequence:

   a. Configuration of connector libraries
   b. Import of the connector XML files (by using the Deployment Manager)
   c. Compilation of adapters

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

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

8. Click **Exit** to finish the installation procedure.

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

   a. Make sure that the prerequisites for using the connector are addressed.

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

   b. Configure the IT resource for the connector.

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

   c. Configure the scheduled jobs.

      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 A-1

2.2.2.2 Configuring the IT Resource for the Target System

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

This section contains the following topics:

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

2.2.2.2.1 IT Resource Parameters

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

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

- Connection-related parameters
- Authentication parameters

Connection Parameters

Table 2-1 lists the connection-related parameters.

Table 2-1 Connection IT Resource Parameters

Parameter	Description
host	The host name or IP address of the computer hosting the target system. Sample value: `www.example.com`
port	The port number at which the target system is listening. Sample value: `80`
baseURI	The base URI is the base relative URL of the Oracle Identity Cloud Service target system. Sample value: http://host:port/admin/v1, then baseURI is /admin/v1
Configuration Lookup	The name of the lookup definition that stores configuration information used during reconciliation and provisioning. Default value for Oracle Identity Cloud Service: `Lookup.IDCS.Configuration`
Connector Server Name	If you have deployed the Oracle Identity Cloud Service connector in a Java Connector Server, then enter the name of the IT resource for the Connector Server.

Table 2-1 (Cont.) Connection IT Resource Parameters

Parameter	Description
acceptType	The accept type for the header denotes how the request body must be parsed. The request body should only be parsed as JSON if the Content-Type header is application/json.
sslEnabled	If the target system requires SSL connectivity, set the value of this parameter to true. Otherwise, set the value to false.
grantType	The type of authentication used by your target system. The default value is: `password`
scope	Scope is required to authenticate request based on 'OAuth2.0 Resource Owners Password or Client Credentials' authentication type
contentType	The content type for the header denotes the format of the request being sent to the target system. The request body should only be parsed as JSON if the Content-Type header is application or JSON.

Table 2-2 lists authentication parameters.

Table 2-2 Basic Authentication IT Resource Parameters

Parameter	Description
username	The user name or User ID used if authentication type is “basic” or “password”. Sample value: `johnsmith`
password	The password used if authentication type is “basic” or “password”. Sample value: `password`
authenticationServerUrl	The URL of the authentication server if authentication type is “BASIC”. Sample value: `https://api.example.com/oauth2/token`

customAuthHeaders	Authorization=Basic
	`“<Base64 Encode ClientID:ClientSecret>”`

2.2.2.2.2 Specifying Values for the IT Resource Parameters

The IT resource for the target system contains connection information about the target system. Oracle Identity Manager uses this information during provisioning and reconciliation. When you run the metadata generator, the IT resource corresponding to this connector is automatically created in Oracle Identity Manager.

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

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **IT Resource.**
3. In the IT Resource Name field on the Manage IT Resource page, enter `Identity Cloud Services`, and then click **Search.**
4. Click the edit icon for the IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the IT resource.
7. To save the values, click **Update.**

2.2.3 Deploying the Connector in a Connector Server

In this scenario, you deploy the connector in Oracle Identity Manager, and then, deploy the connector bundle in a Connector Server.

For information about installing, configuring, and running the Connector Server, and then installing the connector in a Connector Server, see Using an Identity Connector Server in *Developing and Customizing Applications for Oracle Identity Manager*.

2.3 Postinstallation

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

Postinstallation steps are detailed in the following sections:

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

2.3.1 Postinstallation on Oracle Identity Manager

Configuring Oracle Identity Manager involves performing the following procedures:

- Configuring Oracle Identity Manager
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Managing Logging for Oracle Identity Cloud Service Connector
- Localizing Field Labels in UI Forms
- Configuring SSL for Oracle Identity Cloud Service

2.3.1.1 Configuring Oracle Identity Manager

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

These procedures are described in the following sections:

- Creating and Activating a Sandbox

- Creating a New UI Form
- Creating an Application Instance
- Publishing a Sandbox
- Harvesting Entitlements and Sync Catalog
- Updating an Existing Application Instance with a New Form

2.3.1.1.1 Creating and Activating a Sandbox

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

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

2.3.1.1.2 Creating a New UI Form

You can use Form Designer in Oracle Identity System Administration to create and manage application instance forms. See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

While creating the UI form, ensure that you select the resource object corresponding to the Oracle Identity Cloud Service connector that you want to associate the form with. In addition, select the **Generate Entitlement Forms** check box.

2.3.1.1.3 Creating an Application Instance

Create an application instance as follows:

1. In the left pane of the System Administration console, under Configuration, click **Application Instances.** The Application Instances page appears.
2. From the Actions menu, select **Create.** Alternatively, click Create on the toolbar. The Create Application Instance page appears.
3. Enter appropriate values for the fields displayed on the Attributes form and click **Save.**
4. Click **Save.** The application instance is created.
5. Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See Publishing an Application Instance to Organizations in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

2.3.1.1.4 Publishing a Sandbox

After you publish a sandbox, it is difficult to revert changes. Therefore, before you publish a sandbox, perform the following procedure to validate all sandbox changes made until this stage:

1. In the System Administration console, deactivate the sandbox.
2. Log out of the System Administration console.
3. Log in to the Self Service console using the xelsysadm user credentials, and then activate the sandbox that you deactivated in Step 1.

4. In the catalog, ensure that the Oracle Identity Cloud Service application instance form appears with the correct fields.
5. After you Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

2.3.1.1.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync the catalog:

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

> **See Also:**
>
> For a description of the Entitlement List and Catalog Synchronization Job scheduled jobs, see Predefined Scheduled Tasks in *Administering Oracle Identity Manager*

2.3.1.1.6 Updating an Existing Application Instance with a New Form

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

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

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

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

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

1. In a command window, switch to the *OIM_HOME*/server/bin directory.
2. Enter one of the following commands:

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

- **On Microsoft Windows:** `PurgeCache.bat All`
- **On UNIX:** `PurgeCache.sh All`

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

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

In this format:

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

  You can use the PurgeCache utility to purge the cache for any content category. See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

2.3.1.3 Managing Logging for Oracle Identity Cloud Service Connector

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

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

2.3.1.3.1 Understanding Log Levels

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

ODL is the principle logging service used by Oracle Identity Manager and is based on java.util.Logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.
- SEVERE

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

  This level enables logging of information about potentially harmful situations.
- INFO

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

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

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

These log levels are mapped to ODL message type and level combinations as shown in Table 2-3.

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

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

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

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

2.3.1.3.2 Enabling Logging

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

a. Add the following blocks in the file:

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

 <logger name='ORG.IDENTITYCONNECTORS.GENERICSCIM' level='TRACE:32'
useParentHandlers='false'>
     <handler name='idcs-handler'/>
     <handler name='console-handler'/>
   </logger>
```

b. Replace both occurrences of **`[LOG_LEVEL]`** with the ODL message type and level combination that you require. Table 2-3 lists the supported message type and level combinations.

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

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

```
<log_handler name='idcs-handler' level='TRACE:32'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path'
  value='/scratch/IDCS/Logs/IDCS.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>
</log_handlers>

 <logger name='ORG.IDENTITYCONNECTORS.GENERICSCIM' level='TRACE:32'
useParentHandlers='false'>
     <handler name='idcs-handler'/>
     <handler name='console-handler'/>
   </logger>
```

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

2. Save and close the file.

3. Set the following environment variable to redirect the server logs to a file:

   - **For Microsoft Windows:**

     ```
     set WLS_REDIRECT_LOG=FILENAME
     ```

   - **For UNIX:**

     ```
     export WLS_REDIRECT_LOG=FILENAME
     ```

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

4. Restart the application server.

2.3.1.4 Localizing Field Labels in UI Forms

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

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

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open one of the following files in a text editor:
   - For Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0):

     ```
     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime
     \BizEditorBundle_ en.xlf
     ```

   - For releases prior to Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0):

     ```
     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime
     \BizEditorBundle. xlf
     ```

6. Edit the BizEditorBundle.xlf file in the following manner:
   a. Search for the following text:

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

   b. Replace with the following text:

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

      In this text, replace *LANG_CODE* with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

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

c. Search for the application instance code. This procedure shows a sample edit for Oracle Identity Cloud Service application instance. The original code is:

```
<trans-unit
id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResource
Bundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.us
erEO.UD_ACMEGSAP_APP_DFLT_HOME__c_description']}">
<source>APP_DFLT_HOME</source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.ACMEFORM.entity.ACME
FORMEO.UD_ACMEGSAP_APP_DFLT_HOME__c_LABEL">
<source>APP_DFLT_HOME</source>
<target/>
</trans-unit>
```

d. Open the properties file created in Step 1 and get the value of the attribute, for example, `global.udf.D_ACMEGSAP_APP_DFLT_HOME=\u4567d`.

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResource
Bundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.us
erEO.UD_ACMEGSAP_APP_DFLT_HOME__c_description']}">
<source>APP_DFLT_HOME</source>
<target>\u4567d</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.ACMEFORM.entity.ACME
FORMEO.UD_ACMEGSAP_APP_DFLT_HOME__c_LABEL">
<source>APP_DFLT_HOME</source>
<target>\u4567d</target>
</trans-unit>
```

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

g. Save the file as BizEditorBundle_*LANG_CODE*.xlf. In this file name, replace *LANG_CODE* with the code of the language to which you are localizing.

   Sample file name: BizEditorBundle_ja.xlf.

7. Repackage the ZIP file and import it into MDS.

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

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

2.3.1.5 Configuring SSL for Oracle Identity Cloud Service

Configure SSL to secure data communication between Oracle Identity Manager and Oracle Identity Cloud Service.

Oracle Identity Cloud Service validates the client system dates to be in sync with the SSL certificate (the certificate issued by Oracle Identity Cloud Service application) date. If there is any deviation, then the target system might throw an error. The client machine date must be in sync with the certificate timestamp range. Obtain SSL certificate from the target system.

Importing the Certificate

Use the keytool command to import the SSL certificate from the target system into the identity keystore in Oracle Identity Manager.

```
keytool -import -alias alias -trustcacerts -file file-to-import -keystore
keystore-name -storepass keystore-password
```

In this example, the certificate file `supportcert.pem` is imported to the identity keystore `client_store.jks` with password `weblogic1`:

```
keytool -import -alias serverwl -trustcacerts -file supportcert.pem -
keystore client_store.jks -storepass weblogic1
```

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

2.3.2 Creating the IT Resource for the Connector Server

You must create an IT resource for the Connector Server if you have deployed the Oracle Identity Cloud Service connector in the Connector Server.

To create the IT resource for the Connector Server, perform the following procedure:

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

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

     Log in to Oracle Identity System Administration
2. If you are using Oracle Identity Manager release 11.1.1, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Create IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.2.*x,* then:

   a. In the left pane under Configuration, click **IT Resource.**

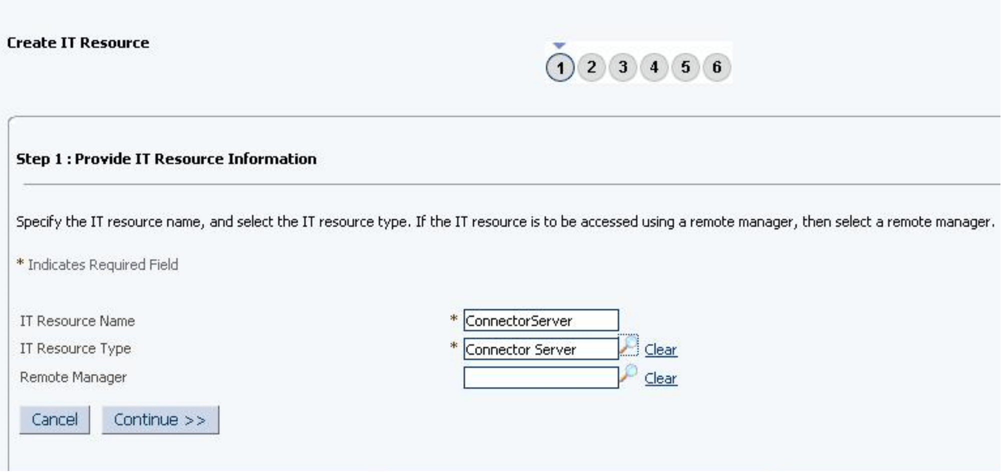
   b. In the Manage IT Resource page, click **Create IT Resource.**

4. On the Step 1: Provide IT Resource Information page, perform the following steps:

   - **IT Resource Name**: Enter a name for the IT resource.
   - **IT Resource Type**: Select **Connector Server** from the IT Resource Type list.
   - **Remote Manager**: Do not enter a value in this field.

5. Click **Continue**. Figure 1 shows the IT resource values added on the Create IT Resource page.

Figure 2-1 Step 1: Provide IT Resource Information



Create IT Resource

Step 1 : Provide IT Resource Information

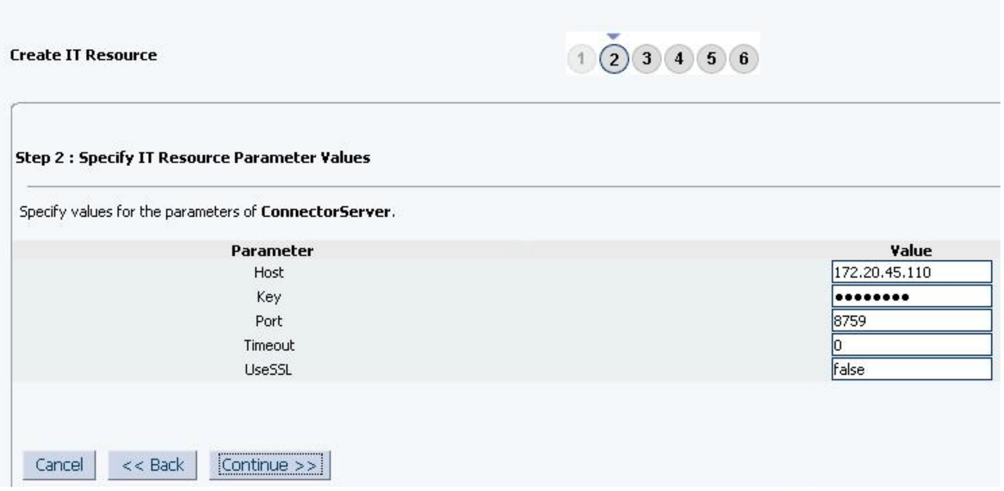
Specify the IT resource name, and select the IT resource type. If the IT resource is to be accessed using a remote manager, then select a remote manager.

* Indicates Required Field

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

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

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



Create IT Resource

Step 2 : Specify IT Resource Parameter Values

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

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

Figure 2-5 provides information about the parameters of the IT resource and Table 2-4 lists values to be specified for the parameters of the IT resource.

Table 2-4 IT Resource Parameters

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

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

   Note:

   This step is optional.

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

   a. Click **Assign Group.**

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

   c. Click **Assign**.

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

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

a. Click **Update Permissions.**

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

c. Click **Update**.

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

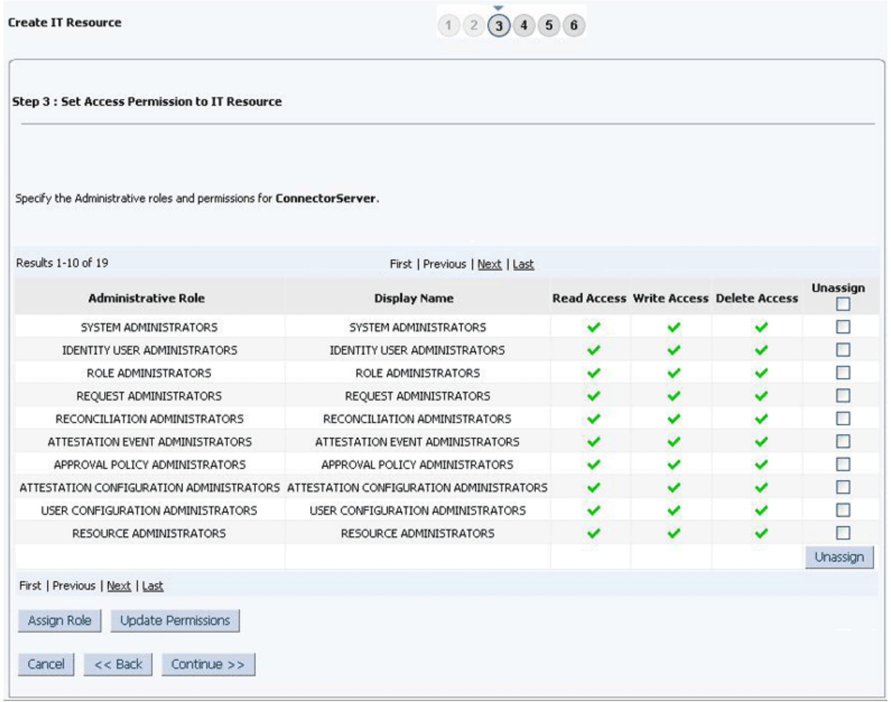
> **Note:**
>
> - This step is optional.
> - You cannot unassign the `SYSTEM ADMINISTRATORS` group. You can unassign only other groups that you assign to the IT resource.

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

b. Click **Unassign**.

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

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



Step 3 : Set Access Permission to IT Resource

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

Results 1-10 of 19

First | Previous | Next | Last

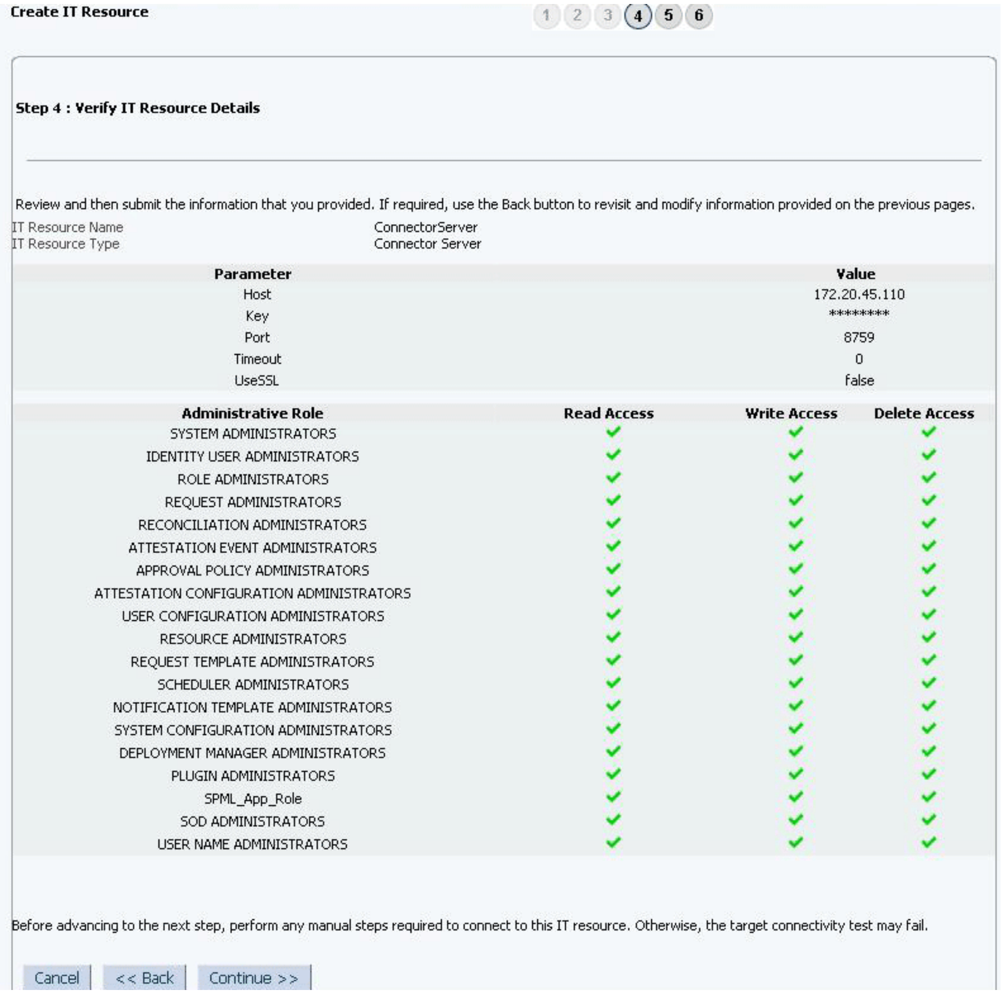
Administrative Role	Display Name	Read Access	Write Access	Delete Access	Unassign □
SYSTEM ADMINISTRATORS	SYSTEM ADMINISTRATORS	✓	✓	✓	□
IDENTITY USER ADMINISTRATORS	IDENTITY USER ADMINISTRATORS	✓	✓	✓	□
ROLE ADMINISTRATORS	ROLE ADMINISTRATORS	✓	✓	✓	□
REQUEST ADMINISTRATORS	REQUEST ADMINISTRATORS	✓	✓	✓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

First | Previous | Next | Last

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

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

Figure 2-4   Step 4: Verify IT Resource Details



Step 4 : Verify IT Resource Details

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

IT Resource Name	ConnectorServer
IT Resource Type	Connector Server

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

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

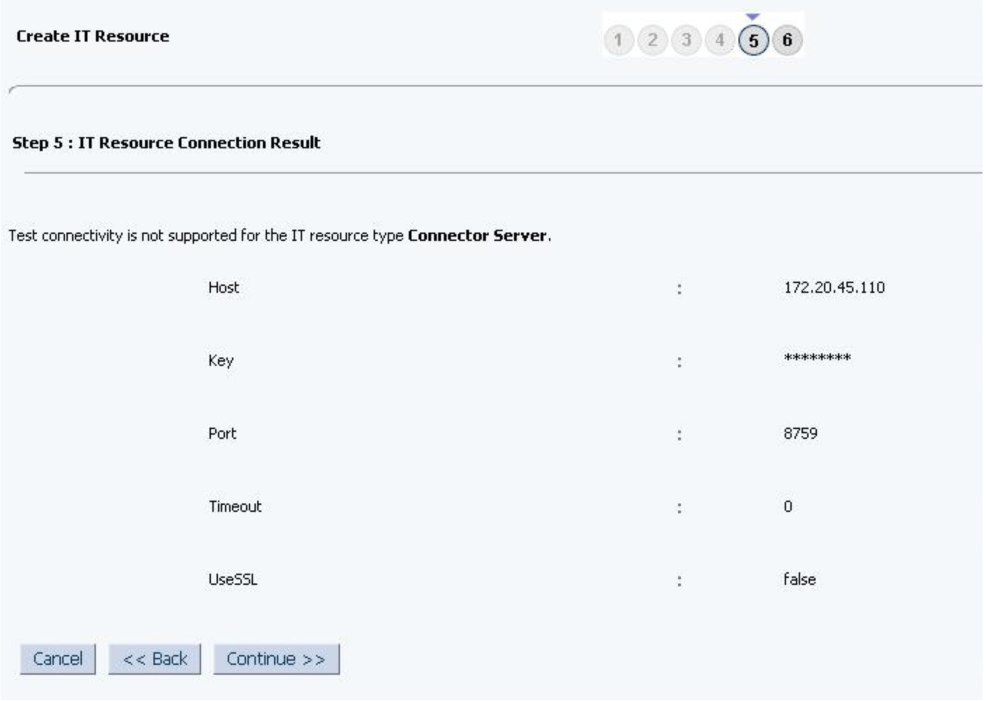
Before advancing to the next step, perform any manual steps required to connect to this IT resource. Otherwise, the target connectivity test may fail.

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

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

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

Figure 2-5   Step 5: IT Resource Connection Result



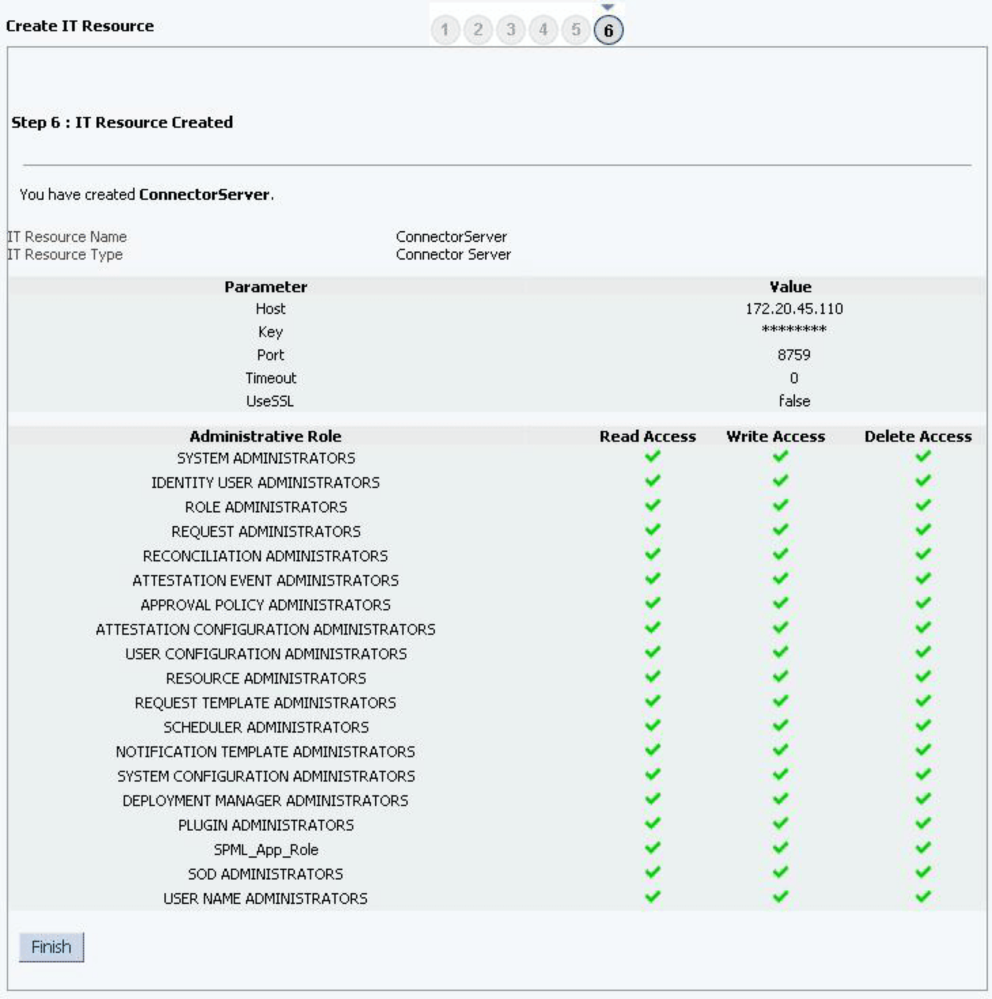
Step 5 : IT Resource Connection Result

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

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

14. Click **Finish**. Figure 6 shows the IT Resource Created Page.

Figure 2-6   Step 6: IT Resource Created



Step 6 : IT Resource Created

You have created **ConnectorServer**.

IT Resource Name	ConnectorServer
IT Resource Type	Connector Server

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

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

3

Using the Oracle Identity Cloud Service Connector

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

This chapter contains the following topics related to using the Oracle Identity Cloud Service connector:

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

3.1 Scheduled Job for Lookup Field Synchronization for Oracle Identity Cloud Service Connector

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

The following scheduled jobs are used for lookup fields synchronization:

- IDCS Groups Lookup Reconciliation
- IDCS Managers Lookup Reconciliation

You must specify values for the attributes of these scheduled jobs. Table 3-1 describes the attributes of the scheduled job for lookup field synchronization.

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

Attribute	Description
Code Key Attribute	Name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: `__UID__` **Note:** Do *not* change the value of this attribute.
Decode Attribute	Name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: `__NAME__` **Note:** Do *not* change the value of this attribute.
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value:`Identity Cloud Services`
Lookup Name	Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. Depending on the scheduled job that you are using, the default values are as follows: • For Groups Lookup Reconciliation: `Lookup.IDCS.Groups` • For Managers Lookup Reconciliation: `Lookup.IDCS.Managers`
Object Type	Enter the type of object you want to reconcile. Depending on the scheduled job that you are using, the default values are as follows: • For Groups Lookup Reconciliation: `Groups` • For Managers Lookup Reconciliation: `__ACCOUNT__`

3.2 Configuring Reconciliation for Oracle Identity Cloud Service Connector

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

This section discusses the following topics related to configuring reconciliation:

- Performing Full Reconciliation
- Performing Limited Reconciliation
- Performing Batched Reconciliation
- Reconciliation Scheduled Jobs for Oracle Identity Cloud Service Connector

3.2.1 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, ensure that no values are specified for the Latest Token and Filter attributes of the scheduled jobs for reconciling user records.

At the end of the reconciliation run, the Latest Token attribute of the scheduled job for user record reconciliation is automatically set to the time stamp at which the run ended. From the next reconciliation run onward, only records created or modified after this time stamp are considered for reconciliation. This is incremental reconciliation.

> **Note:**
>
> Incremental reconciliation reflects changes or modifications made in the target system when a change or modification is made in the incremental reconciliation attribute. For example, during user reconciliation, changes like updates to all the fields on the Authentication Settings page (including radius profiles) and group updates will not be reconciled as a part of incremental reconciliation, and a full reconciliation has to be performed in order to reconcile these changes into Oracle Identity Manager.

3.2.2 Performing Batched Reconciliation

This topic discusses the Batch Size, Batch Start, and Number of Batches attributes of the scheduled jobs for target resource reconciliation.

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure batched reconciliation to avoid such problems.

Batch Start is an attribute that can be used to configure batched reconciliation. This attribute is used to specify the record number from which batched reconciliation must begin.

Set the value of this attribute to 0 to begin reconciliation from the first record in the target system. Similarly, set the value of this attribute to 1 to begin reconciliation from the second record in the target system and so on.

> **Note:**
>
> See Reconciliation Scheduled Jobs for Oracle Identity Cloud Service Connector for more information about the IDCS User Target Recociliation and IDCS Group Target Recociliation scheduled jobs.

3.2.3 Performing Limited Reconciliation

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

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

> **Note:**
>
> If you are using filters in reconciliation as described in this section, be consistent and always use the same filters for delete and normal reconciliation. By using the same filters, you will maintain consistency of the data and will ensure that you work with the same user base in all reconciliation operations.

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

See ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about ICF Filters.

3.2.4 Reconciliation Scheduled Jobs for Oracle Identity Cloud Service Connector

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

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

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

- IDCS User Reconciliation
- IDCS Delete User Reconciliation
- IDCS Group Reconciliation
- IDCS Delete Group Reconciliation

3.2.4.1 IDCS User Reconciliation

You use the IDCS User Reconciliation scheduled job to reconcile user account data from the target system.

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

Table 3-2 Attributes of the IDCS User Reconciliation Scheduled Job

Attribute	Description
Filter	Enter the search filter for fetching records from the target system during a reconciliation run. See Performing Full Reconciliation for more information about filtered reconciliation.
Incremental Recon Attribute	Attribute that holds the date on which the token record was modified. Default value: `meta.lastModified` **Note:** Do *not* change the value of this attribute.

Table 3-2 (Cont.) Attributes of the IDCS User Reconciliation Scheduled Job

Attribute	Description
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `Identity Cloud Services`
Latest Token	This attribute holds the value of the target system attribute that is specified as the value of the Incremental Recon Attribute attribute. The Latest Token attribute is used for internal purposes. By default, this value is empty. **Note:** Do *not* enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute. Sample value: `<String>2016-10-19T07:24:49Z</String>`
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `User` **Note:** User is the only object that is supported. Therefore, do *not* change the value of this attribute.
Resource Object Name	This attribute holds the name of the resource object used for reconciliation. Default value: `IDCS User` Do *not* change the value of this attribute.

3.2.4.2 IDCS Delete User Reconciliation

You use the IDCS Delete User Reconciliation scheduled job to reconcile deleted user account data from the target system.

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

Table 3-3   Attributes of the IDCS Delete User Reconciliation Scheduled Job

Attribute	Description
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `Identity Cloud Services`
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `User` **Note:** User is the only object that is supported. Therefore, do *not* change the value of this attribute.
Resource Object Name	This attribute holds the name of the resource object used for reconciliation. Default value: `IDCS User`

3.2.4.3 IDCS Group Reconciliation

You use the IDCS Group Reconciliation scheduled job to reconcile group data from the target system.

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

Table 3-4   Attributes of the Group Reconciliation Scheduled Job

Attribute	Description
Filter	Enter the search filter for fetching records from the target system during a reconciliation run. See Performing Full Reconciliation for more information about filtered reconciliation.

Table 3-4 (Cont.) Attributes of the Group Reconciliation Scheduled Job

Attribute	Description
Incremental Recon Attribute	Attribute that holds the date on which the token record was modified. Default value: `meta.lastModified` **Note:** Do *not* change the value of this attribute.
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `Identity Cloud Services`
Latest Token	This attribute holds the value of the attribute that is specified as the value of the Incremental Recon Attribute. The Latest Token attribute is used for internal purposes. By default, this value is empty. **Note:** Do *not* enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute. Sample value: `<String>2016-10-19T07:24:49Z</String>`

Table 3-4 (Cont.) Attributes of the Group Reconciliation Scheduled Job

Attribute	Description
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `Group` **Note:** Group is the only object that is supported. Therefore, do *not* change the value of this attribute.
OIM Organization Name	Name of the organization that is used for reconciliation.
Resource Object Name	This attribute holds the name of the resource object used for reconciliation. Default value: `IDCS Group`

3.2.4.4 IDCS Delete Group Reconciliation

You use the IDCS Delete Group Reconciliation scheduled job to reconcile deleted group data from the target system.

Table 3-5 describes the attributes of this scheduled job.

Table 3-5 Attributes of the Delete Group Reconciliation Scheduled Job

Attribute	Description
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `Identity Cloud Services`

Table 3-5 (Cont.) Attributes of the Delete Group Reconciliation Scheduled Job

Attribute	Description
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: `Group` **Note:** User is the only object that is supported. Therefore, do *not* change the value of this attribute.
OIM Organization Name	Name of the organization that is used for delete reconciliation.
Resource Object Name	This attribute holds the name of the resource object used for reconciliation. Default value: `IDCS Group`

3.3 Configuring Scheduled Jobs

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

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

To configure a scheduled job:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **Scheduler.**
3. Search for and open the scheduled task as follows:
   a. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the following parameters:
   - **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
   - **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

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

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

   > **Note:**
   >
   > - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
   > - Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.
   > - Attributes of the scheduled job are discussed in Scheduled Jobs.

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

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

3.4 Performing Provisioning Operations

You create a new user in Oracle Identity Self Service by using the Create User page. You provision or request for accounts on the Accounts tab of the User Details page.

To perform provisioning operations in Oracle Identity Manager:

1. Log in to Oracle Identity Administrative and User console.
2. Create a user as follows:
   a. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
   b. From the Actions menu, select **Create**. Alternatively, you can click **Create** on the toolbar. The Create User page is displayed with input fields for user profile attributes.
   c. Enter details of the user in the Create User page.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance created in Step 3, and then click **Checkout.**
5. Specify value for fields in the application form.

6. Specify value for fields in the application form and then click **Ready to Submit.**
7. Click **Submit.**
8. If you want to provision entitlements, then:
   a. On the Entitlements tab, click **Request Entitlements.**
   b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout.**
   c. Click **Submit.**

3.5 Uninstalling the Connector

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

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

4

Extending the Functionality of the Oracle Identity Cloud Service Connector

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

This chapter discusses the following topics related to extending the functionality of the Oracle Identity Cloud Service connector:

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

- Adding New User or Group Attributes for Reconciliation
- Adding New User or Group Attributes for Provisioning
- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring Transformation of Data During User Reconciliation
- Configuring the Connector for Multiple Installations of the Target System
- Defining the Connector

4.1 Adding New User or Group Attributes for Reconciliation

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

The default attribute mappings for reconciliation are listed in Table 1-8 and Table 1-9.

> **Note:**
>
> - This connector supports configuration of already existing (standard) attributes of Oracle Identity Cloud Service for reconciliation.
> - Only single-valued attributes can be mapped for reconciliation.

This section contains the following topics related to adding new attributes for users or groups:

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

4.1.1 Adding New Attributes on the Process Form

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

To add a new attribute on the process form:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open one of the following process forms:
   - For Users: **UD_IDCS_USR**
   - For Groups: **UD_IDCS_GRP**
4. Click **Create New Version**, and then click **Add**.
5. Enter the details of the field.

   For example, if you are adding the PREFIX field, enter `UD_IDCS_USR_PREFIX` in the Name field and then enter other details such as Variable Type, Length, Field Label, and Field Type.
6. Click the Save icon, and then click **Make Version Active**. The following screenshot shows the new field added to the process form.

Figure 4-1 Form Designer

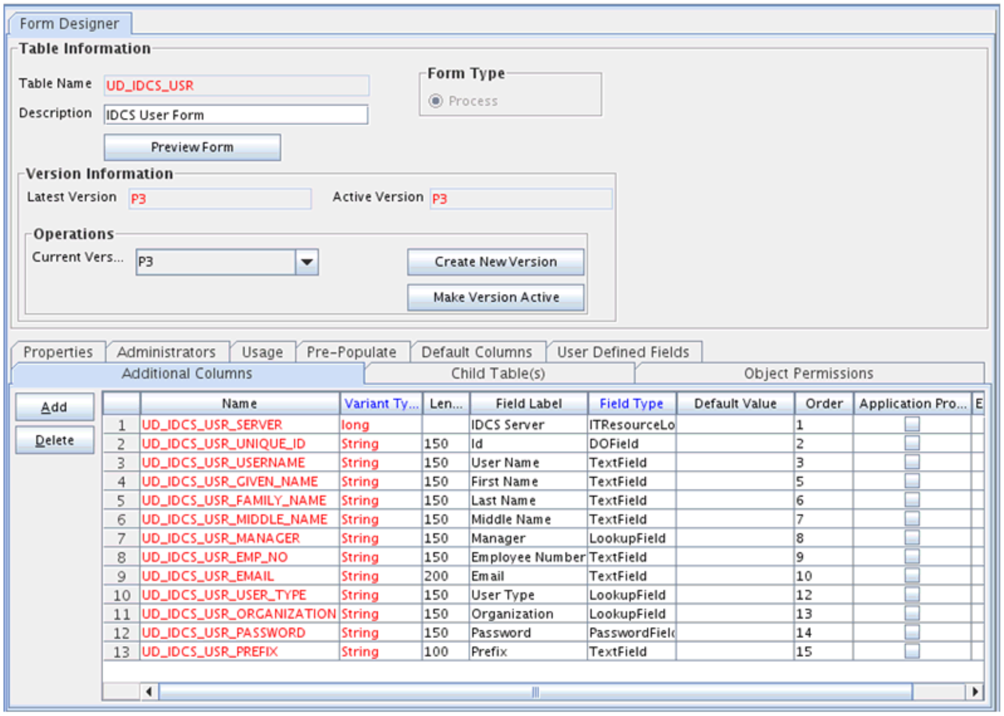


Table Name: UD_IDCS_USR
Description: IDCS User Form
Form Type: ● Process
Latest Version: P3
Active Version: P3
Current Vers...: P3

	Name	Variant Ty...	Len...	Field Label	Field Type	Default Value	Order	Application Pro...	E
1	UD_IDCS_USR_SERVER	long		IDCS Server	ITResourceLo		1	□	
2	UD_IDCS_USR_UNIQUE_ID	String	150	Id	DOField		2	□	
3	UD_IDCS_USR_USERNAME	String	150	User Name	TextField		3	□	
4	UD_IDCS_USR_GIVEN_NAME	String	150	First Name	TextField		5	□	
5	UD_IDCS_USR_FAMILY_NAME	String	150	Last Name	TextField		6	□	
6	UD_IDCS_USR_MIDDLE_NAME	String	150	Middle Name	TextField		7	□	
7	UD_IDCS_USR_MANAGER	String	150	Manager	LookupField		8	□	
8	UD_IDCS_USR_EMP_NO	String	150	Employee Number	TextField		9	□	
9	UD_IDCS_USR_EMAIL	String	200	Email	TextField		10	□	
10	UD_IDCS_USR_USER_TYPE	String	150	User Type	LookupField		12	□	
11	UD_IDCS_USR_ORGANIZATION	String	150	Organization	LookupField		13	□	
12	UD_IDCS_USR_PASSWORD	String	150	Password	PasswordFielc		14	□	
13	UD_IDCS_USR_PREFIX	String	100	Prefix	TextField		15	□	

4.1.2 Adding Attributes to Reconciliation Fields

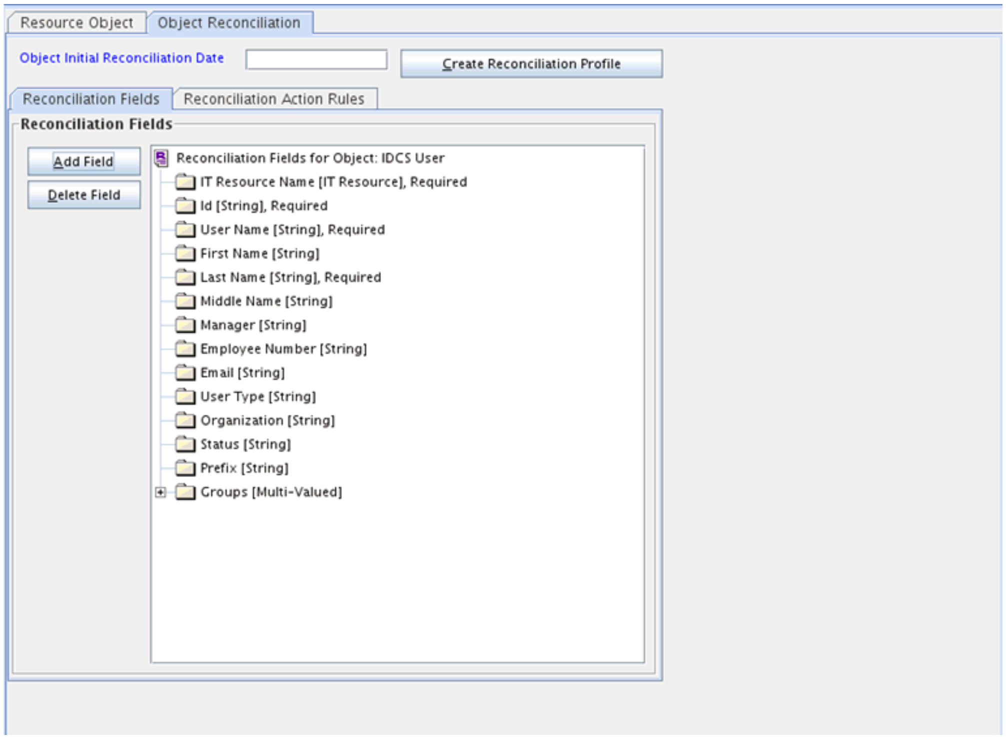
You can add the new attribute to the resource object in the Resource Objects section of Oracle Identity Manager Design Console.

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

1. Expand **Resource Management**, and double-click **Resource Objects**.
2. Search for and open one of the following resource objects:
   - For Users: **IDCS User**
   - For Groups: **IDCS Group**
3. On the Object Reconciliation tab, click **Add Field**.
4. Enter the details of the field.

   For example, enter `ALIAS` in the **Field Name** field and select **String** from the **Field Type** list.
5. Click the Save icon. The following screenshot shows the new reconciliation field added to the resource object:

Figure 4-2 Object Reconciliation Tab



Reconciliation Fields for Object: IDCS User
- IT Resource Name [IT Resource], Required
- Id [String], Required
- User Name [String], Required
- First Name [String]
- Last Name [String], Required
- Middle Name [String]
- Manager [String]
- Employee Number [String]
- Email [String]
- User Type [String]
- Organization [String]
- Status [String]
- Prefix [String]
- Groups [Multi-Valued]

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

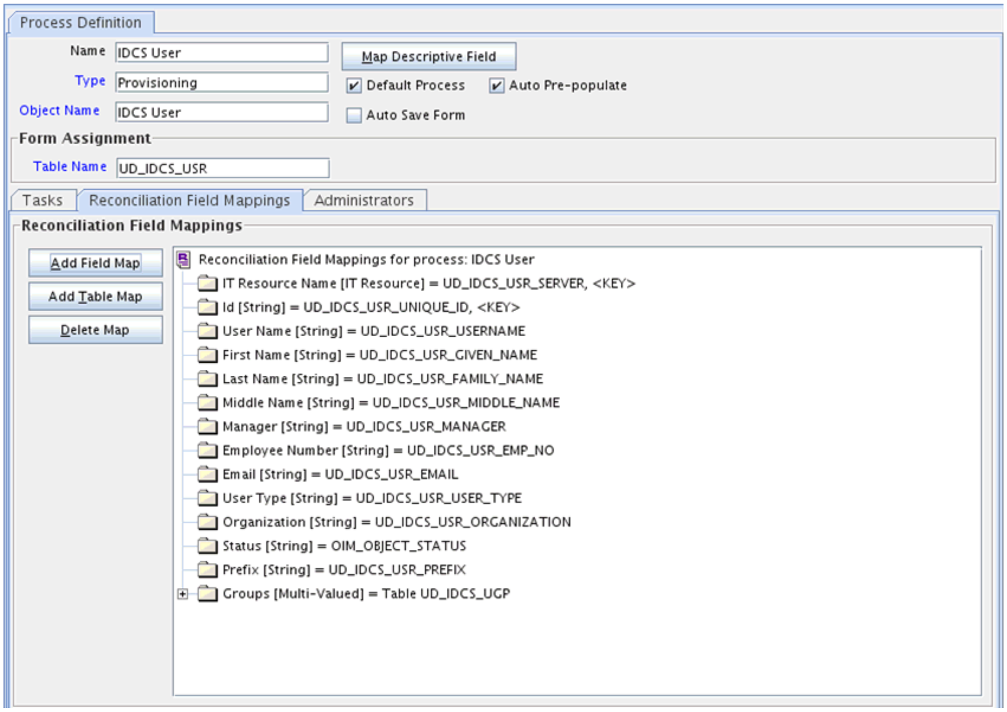
4.1.3 Creating Reconciliation Field Mapping

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

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

1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open one of the following process definitions:
   - For Users: **IDCS User**
   - For Groups: **IDCS Group**
3. On the Reconciliation Field Mappings tab of the **IDCS User** process definition, click **Add Field Map**.
4. From the Field Name list, select the field that you want to map.
5. Double-click the **Process Data Field** field, and then select the column for the attribute. For example, select **UD_IDCS_USR_PREFIX**.
6. Click the **Save** icon. The following screenshot shows the new reconciliation field mapped to a process data field in the process definition:

Figure 4-3 Process Definition Tab



Name: IDCS User
Type: Provisioning
Object Name: IDCS User
☑ Default Process ☑ Auto Pre-populate
□ Auto Save Form

Form Assignment
Table Name: UD_IDCS_USR

Reconciliation Field Mappings

- Reconciliation Field Mappings for process: IDCS User
  - IT Resource Name [IT Resource] = UD_IDCS_USR_SERVER, <KEY>
  - Id [String] = UD_IDCS_USR_UNIQUE_ID, <KEY>
  - User Name [String] = UD_IDCS_USR_USERNAME
  - First Name [String] = UD_IDCS_USR_GIVEN_NAME
  - Last Name [String] = UD_IDCS_USR_FAMILY_NAME
  - Middle Name [String] = UD_IDCS_USR_MIDDLE_NAME
  - Manager [String] = UD_IDCS_USR_MANAGER
  - Employee Number [String] = UD_IDCS_USR_EMP_NO
  - Email [String] = UD_IDCS_USR_EMAIL
  - User Type [String] = UD_IDCS_USR_USER_TYPE
  - Organization [String] = UD_IDCS_USR_ORGANIZATION
  - Status [String] = OIM_OBJECT_STATUS
  - Prefix [String] = UD_IDCS_USR_PREFIX
  - Groups [Multi-Valued] = Table UD_IDCS_UGP

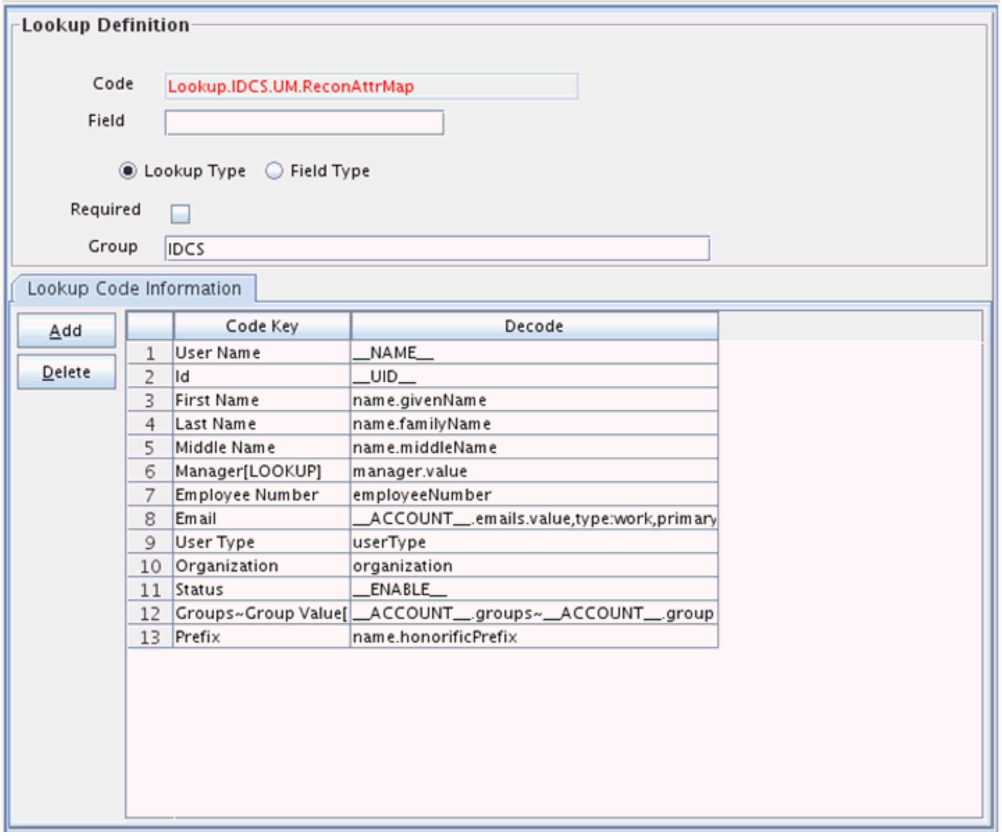
4.1.4 Creating Entries in Lookup Definitions

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

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

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

Figure 4-4 Lookup Definition Page



Lookup Definition

Code	Lookup.IDCS.UM.ReconAttrMap
Field	
● Lookup Type ○ Field Type	
Required	□
Group	IDCS

	Code Key	Decode
1	User Name	__NAME__
2	Id	__UID__
3	First Name	name.givenName
4	Last Name	name.familyName
5	Middle Name	name.middleName
6	Manager[LOOKUP]	manager.value
7	Employee Number	employeeNumber
8	Email	__ACCOUNT__.emails.value,type:work,primary
9	User Type	userType
10	Organization	organization
11	Status	__ENABLE__
12	Groups~Group Value[	__ACCOUNT__.groups~__ACCOUNT__.group
13	Prefix	name.honorificPrefix

4.1.5 Performing Changes in a New UI Form

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

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

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

4.2 Adding New User or Group Attributes for Provisioning

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

The default attribute mappings for provisioning are listed in Table 1-12 and Table 1-13. If required, you can map additional user attributes for provisioning.

This section contains the following topics related to adding new user or group attributes for provisioning:

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

4.2.1 Adding New Attributes for Provisioning

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

> **Note:**
>
> If you have already added an attribute for reconciliation, then you need not repeat steps performed as part of that procedure.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open one of the following the process form.
   - For Users: **UD_IDCS_USR**
   - For Groups: **UD_IDCS_GRP**
4. Click **Create New Version**, and then click **Add**.
5. Enter the details of the attribute.

   For example, if you are adding the PREFIXfield, enter `UD_IDCS_USR_PREFIX` in the Name field, and then enter the rest of the details of this field.
6. Click the Save icon, and then click **Make Version Active**.

   The following screenshot shows the new field added to the process form:

Figure 4-5   New Field Added to the Process Form

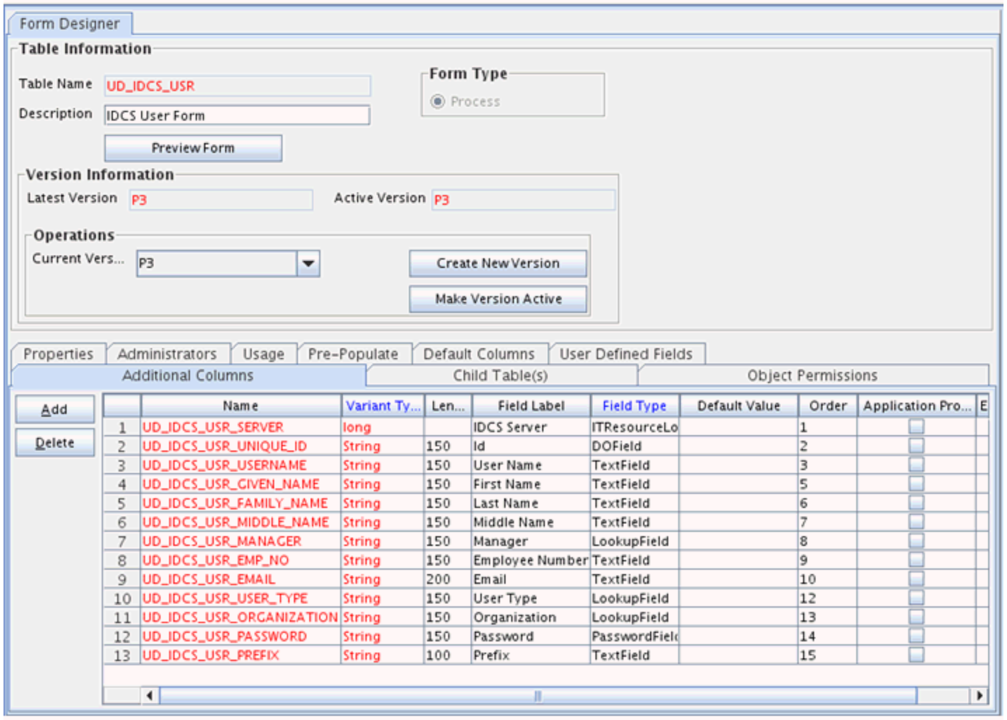


Table Name: UD_IDCS_USR
Description: IDCS User Form
Form Type: ● Process
Latest Version: P3
Active Version: P3
Current Vers...: P3

	Name	Variant Ty...	Len...	Field Label	Field Type	Default Value	Order	Application Pro...	E
1	UD_IDCS_USR_SERVER	long		IDCS Server	ITResourceLo		1	□	
2	UD_IDCS_USR_UNIQUE_ID	String	150	Id	DOField		2	□	
3	UD_IDCS_USR_USERNAME	String	150	User Name	TextField		3	□	
4	UD_IDCS_USR_GIVEN_NAME	String	150	First Name	TextField		5	□	
5	UD_IDCS_USR_FAMILY_NAME	String	150	Last Name	TextField		6	□	
6	UD_IDCS_USR_MIDDLE_NAME	String	150	Middle Name	TextField		7	□	
7	UD_IDCS_USR_MANAGER	String	150	Manager	LookupField		8	□	
8	UD_IDCS_USR_EMP_NO	String	150	Employee Number	TextField		9	□	
9	UD_IDCS_USR_EMAIL	String	200	Email	TextField		10	□	
10	UD_IDCS_USR_USER_TYPE	String	150	User Type	LookupField		12	□	
11	UD_IDCS_USR_ORGANIZATION	String	150	Organization	LookupField		13	□	
12	UD_IDCS_USR_PASSWORD	String	150	Password	PasswordFiel		14	□	
13	UD_IDCS_USR_PREFIX	String	100	Prefix	TextField		15	□	

4.2.2 Creating Entries in Lookup Definitions for Provisioning

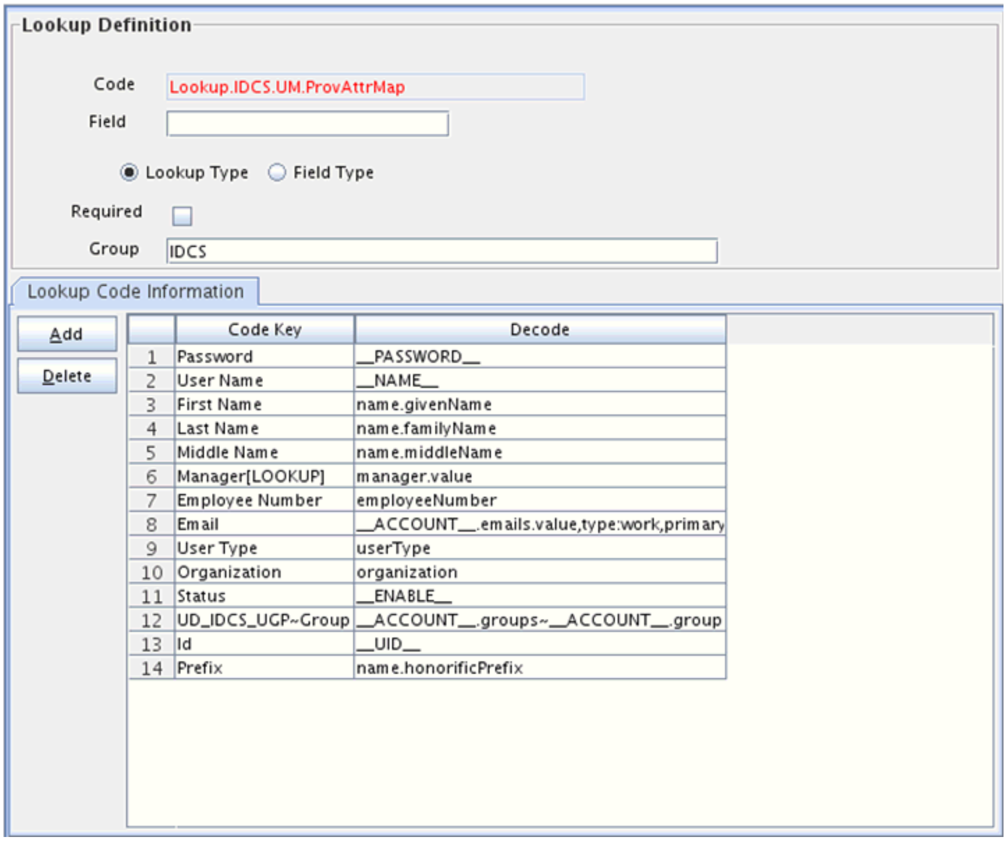
You create an entry for the newly added attribute in the lookup definition that holds attribute mappings for provisioning.

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

1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open one of the following lookup definitions.
   - For Users: **Lookup.IDCS.UM.ProvAttrMap**
   - For Groups: **Lookup.IDCS.GM.ProvAttrMap**
4. Click **Add** and then enter the Code Key and Decode values for the attribute.

   For example, enter `Prefix` in the Code Key column and then enter `name.honorificPrefix` in the Decode column. The following screenshot shows the entry added to the lookup definition:

Figure 4-6   Entry Added to the Lookup Definition



Code: Lookup.IDCS.UM.ProvAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: IDCS

	Code Key	Decode
1	Password	__PASSWORD__
2	User Name	__NAME__
3	First Name	name.givenName
4	Last Name	name.familyName
5	Middle Name	name.middleName
6	Manager[LOOKUP]	manager.value
7	Employee Number	employeeNumber
8	Email	__ACCOUNT__.emails.value,type:work,primary
9	User Type	userType
10	Organization	organization
11	Status	__ENABLE__
12	UD_IDCS_UGP~Group	__ACCOUNT__.groups~__ACCOUNT__.group
13	Id	__UID__
14	Prefix	name.honorificPrefix

4.2.3 Creating a Task to Enable Update Operations

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

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

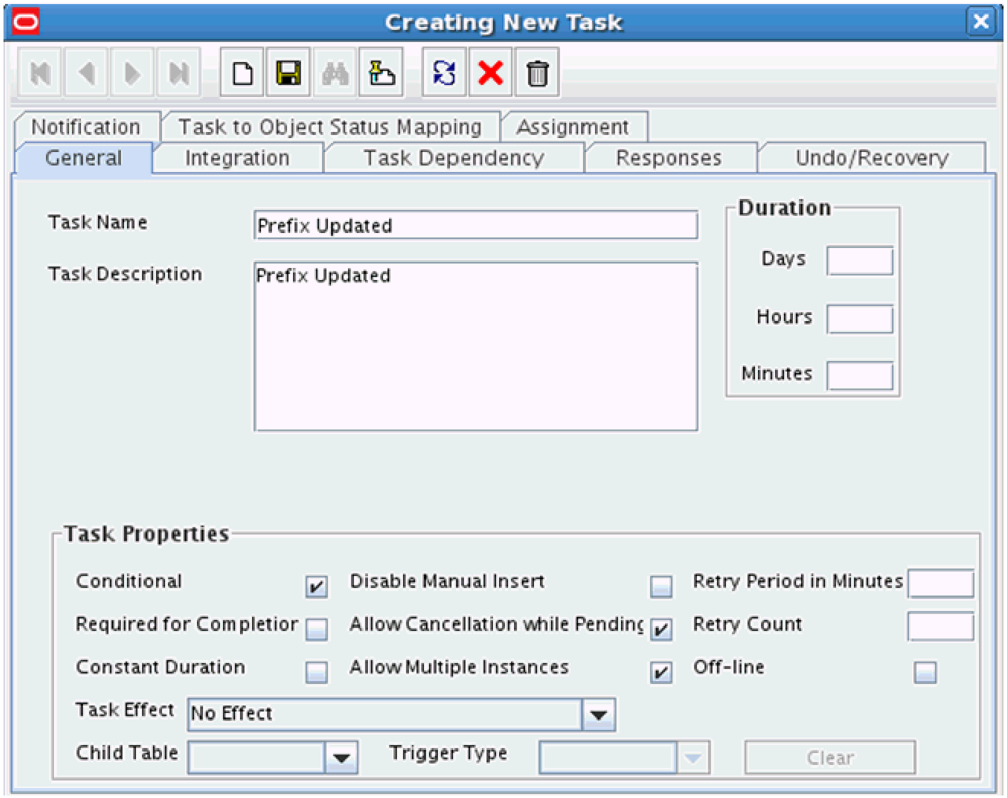
To enable the update of the attribute during provisioning operations, add a process task for updating the new user or group attribute as follows:

> **See Also:**
>
> Developing Provisioning Processes in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open one of the following process definitions.
   - For Users: **IDCS User**
   - For Groups: **IDCS Group**
3. Click **Add.**

4. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:
   - Conditional
   - Allow Cancellation while Pending
   - Allow Multiple Instances
5. Click the Save icon. The following screenshot shows the new task added to the process definition:

Figure 4-7 New Task Added to the Process Definition



Task Name: Prefix Updated

Task Description: Prefix Updated

Duration

Days:

Hours:

Minutes:

Task Properties

Conditional	☑	Disable Manual Insert	□	Retry Period in Minutes	
Required for Completion	□	Allow Cancellation while Pending	☑	Retry Count	
Constant Duration	□	Allow Multiple Instances	☑	Off-line	□

Task Effect: No Effect

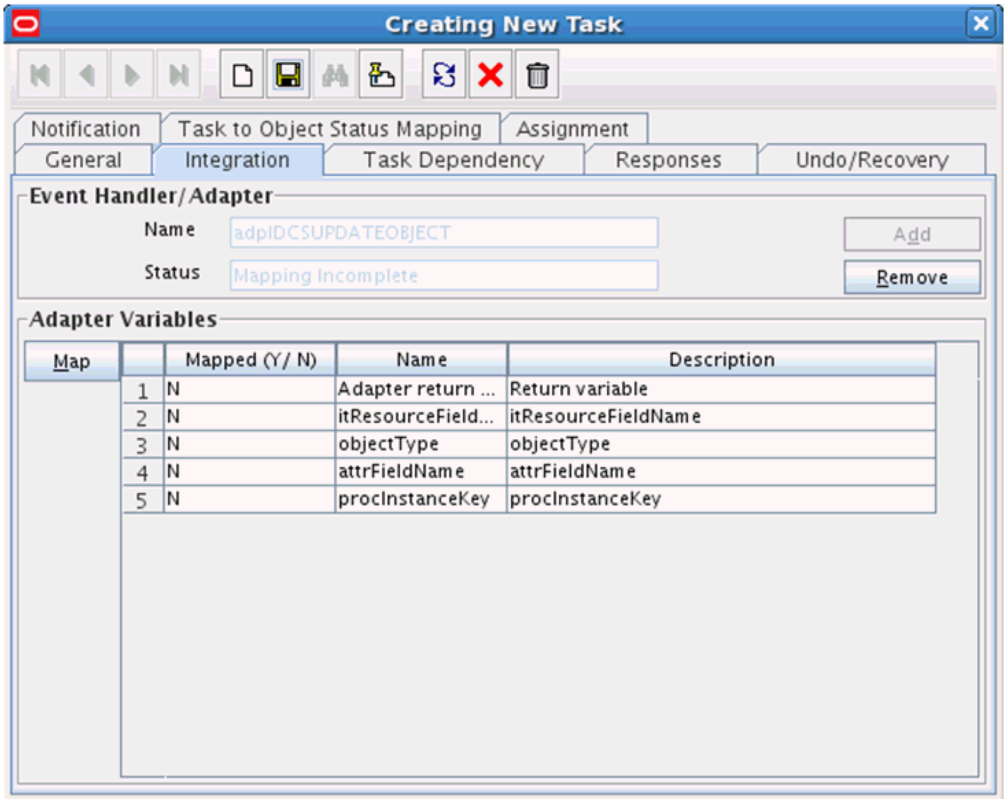
Child Table:

Trigger Type:

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

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

Figure 4-8 List of Adapter Variables



Name: adpIDCSUPDATEOBJECT

Status: Mapping Incomplete

	Mapped (Y/ N)	Name	Description
1	N	Adapter return ...	Return variable
2	N	itResourceField...	itResourceFieldName
3	N	objectType	objectType
4	N	attrFieldName	attrFieldName
5	N	procInstanceKey	procInstanceKey

7. In the Adapter Variables region, click the **ParentFormProcessInstanceKey** variable.
8. In the dialog box that is displayed, create the following mapping:
   - **Variable Name:** ParentFormProcessInstanceKey
   - **Map To:** Process Data
   - **Qualifier:** Process Instance
9. Click Save and close the dialog box.
10. If you are enabling update provisioning operations for a User attribute, then repeat Steps 7 through 9 for the remaining variables listed in the Adapter Variables region.

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

Variable	Map To	Qualifier	Literal Value
Adapter Return Value	Response Code	NA	NA
Object Type	Literal	String	User
itResourceFieldName	Literal	String	UD_IDCS_USR_SERVER
attributeFieldName	Literal	String	Prefix

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

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

Variable	Map To	Qualifier	Literal Value
ParentFormProcessInstanceKey	Process Data	Process Instance	NA
Adapter Return Value	Response Code	NA	NA
Object Type	Literal	String	Group
itResourceFieldName	Literal	String	UD_IDCS_GRP_SERVER
attributeFieldName	Literal	String	<NAME_OF_THE_NEW_GROUP_ATTRIBUTE>

12. On the Responses tab, click **Add** to add at least the SUCCESS response code, with Status C. This ensures that if the task is successfully run, then the status of the task is displayed as `Completed`.
13. Click the Save icon and close the dialog box, and then save the process definition.

4.2.4 Replicating Form Designer Changes to a New UI Form

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

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

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

4.3 Configuring Validation of Data During Reconciliation and Provisioning

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

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

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

To configure validation of data:

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

   The validation class must implement validate method with the following method signature:

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

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

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

```
                }
        return valid;
                      }
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file to Oracle Identity Manager database.

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

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

   - **For Microsoft Windows:** `OIM_HOME/server/bin/UploadJars.bat`
   - **For UNIX:** `OIM_HOME/server/bin/UploadJars.sh`

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.
4. If you created the Java class for validating a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Create a lookup definition named **Lookup.IDCS.UM.ReconValidation**.
   c. In the Code Key column, enter `username`. In the Decode column, enter `org.identityconnectors.IDCS.extension.IDCSValidator`.
   d. Save the changes to the lookup definition.
   e. Search for and open the Lookup.IDCS.UM.Configuration lookup definition.
   f. In the Code Key column, enter `Recon Validation Lookup`. In the Decode column, enter `Lookup.IDCS.UM.ReconValidation`.
   g. Save the changes to the lookup definition.
5. If you created the Java class for validating a process form field for provisioning, then:
   a. Log in to the Design Console.
   b. Create a lookup definition named Lookup.IDCS.UM.ProvValidation.
   c. In the Code Key column, enter the process form field name. In the Decode column, enter the class name.
   d. Save the changes to the lookup definition.
   e. Search for and open the Lookup.IDCS.UM.Configuration lookup definition.
   f. In the Code Key column, `Provisioning Validation Lookup`. In the Decode column, enter `Lookup.IDCS.UM.ProvValidation`.

g. Save the changes to the lookup definition.

h. Purge the cache to ensure that the changes are reflected in Oracle Identity Manager. See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager* .

4.4 Configuring Transformation of Data During User Reconciliation

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

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

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

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

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

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

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

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

   ```
   package oracle.iam.connectors.common.transform;
   import java.util.HashMap;
   public class TransformAttribute {
   /*
   Description:Abstract method for transforming the attributes
   param hmUserDetails< String,Object>
   HashMap containing parent data details
   param hmEntitlementDetails < String,Object>
   HashMap containing child data details
   */
   public Object transform(HashMap hmUserDetails, HashMap
   hmEntitlementDetails,String sField) {
   /*
   *    You must write code to transform the attributes. Parent data
   attribute values can be fetched by using hmUserDetails.get("Field
   Name").
   ```

```
*To fetch child data values, loop through the
*    ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
*    Return the transformed attribute.
*/
String sUserName= (String)hmUserDetails.get("User Name"); String
sLastName= (String)hmUserDetails.get("Last Name"); String
sFullName=sUserName+"."+sLastName;
return sFullName;
}
}
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file to Oracle Identity Manager database.

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

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

   - **For Microsoft Windows:** `*OIM_HOME*/server/bin/UploadJars.bat`
   - **For UNIX:** `*OIM_HOME*/server/bin/UploadJars.sh`

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.
4. If you created the Java class for transforming a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Create a lookup definition named **Lookup.IDCS.UM.ReconTransformation**.
   c. In the Code Key column, enter the resource object field name on which you want to apply transformation. For example, User Name. In the Decode column, enter the name of the class that implements the transformation logic. For example, `oracle.iam.connectors.common.transform.TransformAttribute`.
   d. Save the changes to the lookup definition.
5. Add an entry in the **Lookup.IDCS.UM.Configuration** lookup definition to enable transformation as follows:
   a. Expand Administration, and then double-click **Lookup Definition**.
   b. Search for and open the **Lookup.IDCS.UM.Configuration** lookup definition.
   c. In the Code Key column, enter `Recon Transformation Lookup`. In the Decode column, enter `Lookup.Office365.UM.ReconTransformation`.

   d. Save the changes to the lookup definition.
   e. Purge the cache to ensure that the changes are reflected in Oracle Identity Manager. See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

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 must create copies of the connector. See Cloning Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4.6 Defining the Connector

You can define a customized or reconfigured connector using the Oracle Identity System Administration. Defining a connector is equivalent to registering the connector with Oracle Identity Manager.

A connector is automatically defined when you install it using the Install Connectors feature or when you upgrade it using the Upgrade Connectors feature. You must manually define a connector if:

- You import the connector by using the Deployment Manager.
- You customize or reconfigure the connector.
- You upgrade Oracle Identity Manager.

The following events take place when you define a connector:

- A record representing the connector is created in the Oracle Identity Manager database. If this record already exists, then it is updated.
- The status of the newly defined connector is set to Active. In addition, the status of a previously installed release of the same connector automatically is set to Inactive.

See Defining Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

A
Files and Directories on the Installation Media

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

Table A-1   Files and Directories on the Installation Media

File in the Installation Media Directory	Description
org.identityconnectors.genericscim-1.0.1115.jar	This JAR is the ICF connector bundle.
configuration/IDCS-CI.xml	This XML file contains configuration information that is used during the connector installation process.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the Oracle Identity Manager database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that include GUI element labels and messages.
xml/IDCS-ConnectorConfig.xml	This XML file contains definitions for the following connector objects: • Resource objects • IT resource types • IT resource instance • Process forms • Process tasks and adapters • Process definition • Prepopulate rules • Lookup definitions • Reconciliation rules • Scheduled jobs

Index