

Oracle® Identity Governance

Configuring the Oracle Identity Cloud Service Application



12c (12.2.1.3.0)

F12372-02

March 2020

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Oracle Identity Governance Configuring the Oracle Identity Cloud Service Application, 12c (12.2.1.3.0)

F12372-02

Copyright © 2018, 2020, Oracle and/or its affiliates.

Primary Author: Gowri.G.R

Contributors: Samriti Gupta

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	ix
Documentation Accessibility	ix
Related Documents	ix
Conventions	x

What's New in This Guide?

Software Updates	xi
Documentation-Specific Updates	xii

1 About the Identity Cloud Service Connector

1.1	Certified Components	1-2
1.2	Usage Recommendation	1-3
1.3	Certified Languages	1-4
1.4	Supported Connector Operations	1-4
1.5	Connector Architecture	1-5
1.6	Supported Use Cases	1-6
1.7	Supported Connector Features Matrix	1-7
1.8	Connector Features	1-7
1.8.1	Support for User and Group Provisioning	1-8
1.8.2	Support for Full and Incremental Reconciliation	1-8
1.8.3	Support for Limited Reconciliation	1-8
1.8.4	Support for Batched Reconciliation	1-8
1.8.5	Reconciliation of Deleted User and Group Records	1-8
1.8.6	Transformation and Validation of Account Data	1-9
1.8.7	Support for Cloning Applications and Creating Instance Applications	1-9
1.8.8	Secure Communication to the Target System	1-9
1.8.9	Support for the Connector Server	1-9

2	Creating an Application By Using the Identity Cloud Service Connector	
2.1	Process Flow for Creating an Application By Using the Connector	2-1
2.2	Prerequisites for Creating an Application By Using the Connector	2-3
2.2.1	Configuring the Target System	2-3
2.2.2	Downloading the Connector Installation Package	2-4
2.3	Creating an Application By Using the Connector	2-4
3	Configuring the Identity Cloud Service Connector	
3.1	Basic Configuration Parameters	3-1
3.2	Advanced Settings Parameters	3-2
3.3	Attribute Mappings	3-5
3.4	Correlation Rules, Situations, and Responses	3-8
3.5	Reconciliation Jobs	3-10
4	Performing the Postconfiguration Tasks for the Identity Cloud Service Connector	
4.1	Configuring Oracle Identity Governance	4-1
4.1.1	Creating and Activating a Sandbox	4-1
4.1.2	Creating a New UI Form	4-2
4.1.3	Publishing a Sandbox	4-2
4.1.4	Updating an Existing Application Instance with a New Form	4-2
4.2	Harvesting Entitlements and Sync Catalog	4-3
4.3	Managing Logging for the Connector Server	4-3
4.3.1	Understanding Log Levels	4-4
4.3.2	Enabling Logging	4-5
4.4	Configuring the IT Resource for the Connector Server	4-6
4.5	Localizing Field Labels in UI Forms	4-7
4.6	Configuring SSL for the Connector	4-9
5	Using the Identity Cloud Service Connector	
5.1	Configuring Reconciliation	5-1
5.1.1	Performing Full and Incremental Reconciliation	5-1
5.1.2	Performing Batched Reconciliation	5-2
5.1.3	Performing Limited Reconciliation	5-2
5.2	Configuring Reconciliation Jobs	5-3
5.3	Configuring Provisioning	5-4
5.3.1	Guidelines on Performing Provisioning Operations	5-4

5.3.2	Performing Provisioning Operations	5-4
5.4	Connector Objects Used For Group Management	5-5
5.4.1	Lookup Definitions for Group Management	5-5
5.4.2	Reconciliation Scheduled Jobs for Group Management	5-5
5.4.2.1	IDCS Group Reconciliation Job	5-6
5.4.2.2	IDCS Group Delete Reconciliation Job	5-7
5.4.3	Reconciliation Rules for Group Management	5-7
5.4.3.1	Reconciliation Rule for Groups	5-7
5.4.3.2	Viewing Reconciliation Rules in the Design Console	5-8
5.4.4	Reconciliation Action Rules for Group Management	5-8
5.4.4.1	Reconciliation Action Rules for Groups	5-8
5.4.4.2	Viewing Reconciliation Action Rules in Design Console	5-8
5.5	Uninstalling the Connector	5-9

6 Extending the Functionality of the Identity Cloud Service Connector

6.1	Adding New Group Attributes for Reconciliation	6-1
6.1.1	Adding New Attributes on the Process Form	6-2
6.1.2	Adding Attributes to Reconciliation Fields	6-2
6.1.3	Creating Reconciliation Field Mapping	6-3
6.1.4	Creating Entries in Lookup Definitions	6-4
6.1.5	Performing Changes in a New UI Form	6-5
6.2	Adding New Group Attributes for Provisioning	6-5
6.2.1	Adding New Attributes for Provisioning	6-6
6.2.2	Creating Entries in Lookup Definitions for Provisioning	6-6
6.2.3	Creating a Task to Enable Update Operations	6-7
6.2.4	Replicating Form Designer Changes to a New UI Form	6-10
6.3	Configuring Transformation and Validation of Data	6-10
6.4	Configuring Action Scripts	6-11
6.5	Configuring the Connector for Multiple Installations of the Target System	6-11

7 Upgrading the Identity Cloud Service Connector

7.1	Preupgrade Steps	7-1
7.2	Upgrade Steps	7-2
7.3	Postupgrade Steps	7-2

8 Troubleshooting the Identity Cloud Service Connector

9 Known Issues and Workarounds for the Identity Cloud Service Connector

A Files and Directories in the Identity Cloud Service Connector Package

List of Figures

1-1	Architecture of the Identity Cloud Service Connector	1-5
2-1	Overall Flow of the Process for Creating an Application By Using the Connector	2-2
3-1	Default Attribute Mappings for the Identity Cloud Service User Account	3-7
3-2	Default Attribute Mappings for the Identity Cloud Service Group Names	3-8
3-3	Simple Correlation Rule for an Identity Cloud Service Target Application	3-9
3-4	Default Situations and Responses for an Identity Cloud Service Target Application	3-9
6-1	Form Designer	6-2
6-2	Object Reconciliation Tab	6-3
6-3	Process Definition Tab	6-4
6-4	Lookup Definition Page	6-4
6-5	New Field Added to the Process Form	6-6
6-6	Entry Added to the Lookup Definition	6-7
6-7	New Task Added to the Process Definition	6-8
6-8	List of Adapter Variables	6-9

List of Tables

1-1	Certified Components	1-2
1-2	Supported Connector Operations	1-4
1-3	Supported Connector Features Matrix	1-7
3-1	Basic Configuration Parameters for Identity Cloud Service	3-1
3-2	Advanced Settings Parameters for Identity Cloud Service	3-3
3-3	Default Attribute Mappings for the Identity Cloud Service User Account	3-5
3-4	Default Attribute Mappings for the Identity Cloud Service Group Names	3-7
3-5	Predefined Identity Correlation Rule for an Identity Cloud Service Target Application	3-8
3-6	Predefined Situations and Responses for an Identity Cloud Service Target Application	3-9
3-7	Parameters of the IDCS Target Resource User Reconciliation Job	3-10
3-8	Parameters of the IDCS Target Resource User Delete Reconciliation Job	3-11
3-9	Parameters of the Reconciliation Jobs for Entitlements	3-12
4-1	Log Levels and ODL Message Type:Level Combinations	4-4
4-2	Parameters of the IT Resource for the Connector Server	4-6
5-1	Entries in the Lookup Definitions for Group Management	5-5
5-2	Attributes of the IDCS Group Reconciliation Scheduled Job	5-6
5-3	Attributes of the IDCS Group Delete Reconciliation Scheduled Job	5-7
5-4	Reconciliation Action Rules for Groups	5-8
8-1	Troubleshooting the Identity Cloud Service Connector	8-1
A-1	Files and Directories in the IDCS Connector Package	A-1

Preface

This guide describes the connector that is used to onboard Oracle Identity Cloud Service applications to Oracle Identity Governance.

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

<http://docs.oracle.com/middleware/12213/oig/index.html>

For information about installing and using Oracle Identity Manager 11.1.2.3, visit the following Oracle Help Center page:

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

For information about Oracle Identity Governance Connectors 12.2.1.3.0 documentation, visit the following Oracle Help Center page:

<http://docs.oracle.com/middleware/oig-connectors-12213/index.html>

For information about Oracle Identity Manager Connectors 11.1.1 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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in This Guide?

These are the updates made to the software and documentation for release 12.2.1.3.0 of Configuring the Oracle Identity Cloud Service Application.

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

- [Software Updates](#)

These include updates made to the connector software.

- [Documentation-Specific Updates](#)

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

Software Updates

These are the updates made to the connector software.

Software Updates in Release 12.2.1.3.0

The following are the software updates in release 12.2.1.3.0:

Support for Onboarding Applications Using the Connector

From this release onward, the connector bundle includes application onboarding templates required for performing connector operations on the Oracle Identity Cloud Service (IDCS) target system. This helps in quicker onboarding of the applications for this target system into Oracle Identity Governance by using an intuitive UI.

Support for Password Hashing and Deleting Users Associated with Entities

From this release onward, the connector enables hashing on the default password that is sent to the target system when a new account is created. This helps in provisioning accounts on IDCS with the password that is assigned to the corresponding Oracle Identity Governance Users. In addition, the account creation notification is not sent from IDCS and users do not need to reset password on first login.

The connector also supports deleting users that are associated with one or more entities (Groups or Applications) in IDCS.

For details on these features, see [Guidelines on Performing Provisioning Operations](#).

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 12.2.1.3.0

The following documentation-specific updates have been made in revision "02" of this guide:

- The "Oracle Identity Governance or Oracle Identity Manager" row of [Table 1-1](#) has been updated to include support for Oracle Identity Governance release 12c PS4 (12.2.1.4.0).
- All instances of "IDCS connectors" is replaced with "Oracle Identity Cloud Service connectors" throughout the guide.

1

About the Identity Cloud Service Connector

Oracle Identity Governance is a centralized identity management solution that provides self service, compliance, provisioning and password management services for applications residing on-premises or on the Cloud. Oracle Identity Governance connectors are used to integrate Oracle identity Governance with the external identity-aware applications.

The Oracle Identity Cloud Service connector lets you create and onboard Identity Cloud Service applications in Oracle Identity Governance.

Note:

In this guide, the connector that is deployed using the **Applications** option on the **Manage** tab of Identity Self Service is referred to as an **AOB application**. The connector that is deployed using the **Manage Connector** option in Oracle Identity System Administration is referred to as a **CI-based connector** (Connector Installer-based connector).

From Oracle Identity Governance release 12.2.1.3.0 onward, connector deployment is handled using the application onboarding capability of Oracle Identity Self Service. This capability lets business users to onboard applications with minimum details and effort. The connector installation package includes a collection of predefined templates (XML files) that contain all the information required for provisioning and reconciling data from a given application or target system. These templates also include basic connectivity and configuration details specific to your target system. The connector uses information from these predefined templates allowing you to onboard your applications quickly and easily using only a single and simplified UI.

Application onboarding is the process of registering or associating an application with Oracle Identity Governance and making that application available for provisioning and reconciliation of user information.

Note:

In this guide, Oracle Identity Cloud Service is sometimes referred to as the **target system**.

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

- [Certified Components](#)
- [Usage Recommendation](#)
- [Certified Languages](#)

- [Supported Connector Operations](#)
- [Connector Architecture](#)
- [Supported Use Cases](#)
- [Supported Connector Features Matrix](#)
- [Connector Features](#)

 **Note:**

In this guide, the term Oracle Identity Governance server refers to the computer on which Oracle Identity Governance is installed.

1.1 Certified Components

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

 **Note:**

If you are using Oracle Identity Manager release 11.1.x, then you can install and use the connector only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12.2.1.3.0 or later.

Table 1-1 Certified Components

Component	Requirement for AOB Application	Required for CI-Based Connector
Oracle Identity Governance or Oracle Identity Manager	<p>You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager:</p> <ul style="list-style-type: none"> • Oracle Identity Governance 12c (12.2.1.4.0) • Oracle Identity Governance 12c (12.2.1.3.0) <p>Note: If you are using Oracle Identity Governance 12c (12.2.1.3.0), then ensure to download and apply patches 26616250 and 25323654 from My Oracle Support.</p>	<p>You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager:</p> <ul style="list-style-type: none"> • Oracle Identity Governance 12c (12.2.1.4.0) • Oracle Identity Governance 12c (12.2.1.3.0) • Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0) and any later BP in this release track

Table 1-1 (Cont.) Certified Components

Component	Requirement for AOB Application	Required for CI-Based Connector
Target System	Oracle Identity Cloud Service 16.3.6 or later Note: It is recommended to use Oracle Identity Cloud Service 18.2.x or later because the new features (such as Password Hashing and Deleting Users Associated with Entities) are not supported in earlier versions.	Oracle Identity Cloud Service 16.3.6 or later Note: It is recommended to use Oracle Identity Cloud Service 18.2.x or later because the new features (such as Password Hashing and Deleting Users Associated with Entities) are not supported in earlier versions.
Connector Server	11.1.2.1.0 or later Note: It is recommended to use Connector Server 12.2.1.3.0 or later if you want to configure Transport Layer Security (TLS) 1.2 connection.	11.1.2.1.0 or later Note: It is recommended to use Connector Server 12.2.1.3.0 or later if you want to configure TLS 1.2 connection.
Connector Server JDK	JDK 1.7 or later	JDK 1.7 or later

1.2 Usage Recommendation

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

- If you are using Oracle Identity Governance release 12c (12.2.1.3.0) or later, then use the latest 12.2.1.x version of this connector. Deploy the connector using the **Applications** option on the **Manage** tab of Identity Self Service.
- If you are using any of the Oracle Identity Manager releases listed in the “Requirement for CI-Based Connector” column of [Certified Components](#), then use the 11.1.1.x version of the Identity Cloud Service connector. If you want to use the 12.2.1.x version of this connector, then you can install and use it only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12c (12.2.1.3.0) or later.

Note:

If you are using the latest 12.2.1.x version of the Identity Cloud Service connector in the CI-based mode, then see *Oracle Identity Manager Connector Guide for Oracle Identity Cloud Services*, Release 11.1.1 for complete details on connector deployment, usage, and customization.

1.3 Certified Languages

The connector supports the following languages:

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

1.4 Supported Connector Operations

These are the list of operations that the connector supports for your target system.

Table 1-2 Supported Connector Operations

Operation	Supported?
User Management	
Disable user	Yes
Add child data	Yes
Update object	Yes
Create object	Yes
Delete object	Yes
Enable user	Yes
Update child data	Yes
Remove child data	Yes
Group Management	
Add group	Yes
Update group	Yes
Remove group	Yes

Note:

All the connector artifacts required for managing groups (such as group attribute mappings, reconciliation rules, scheduled jobs, and so on) are available in the preconfigured templates (XML files) of the connector installation package. See [Connector Objects Used For Group Management](#).

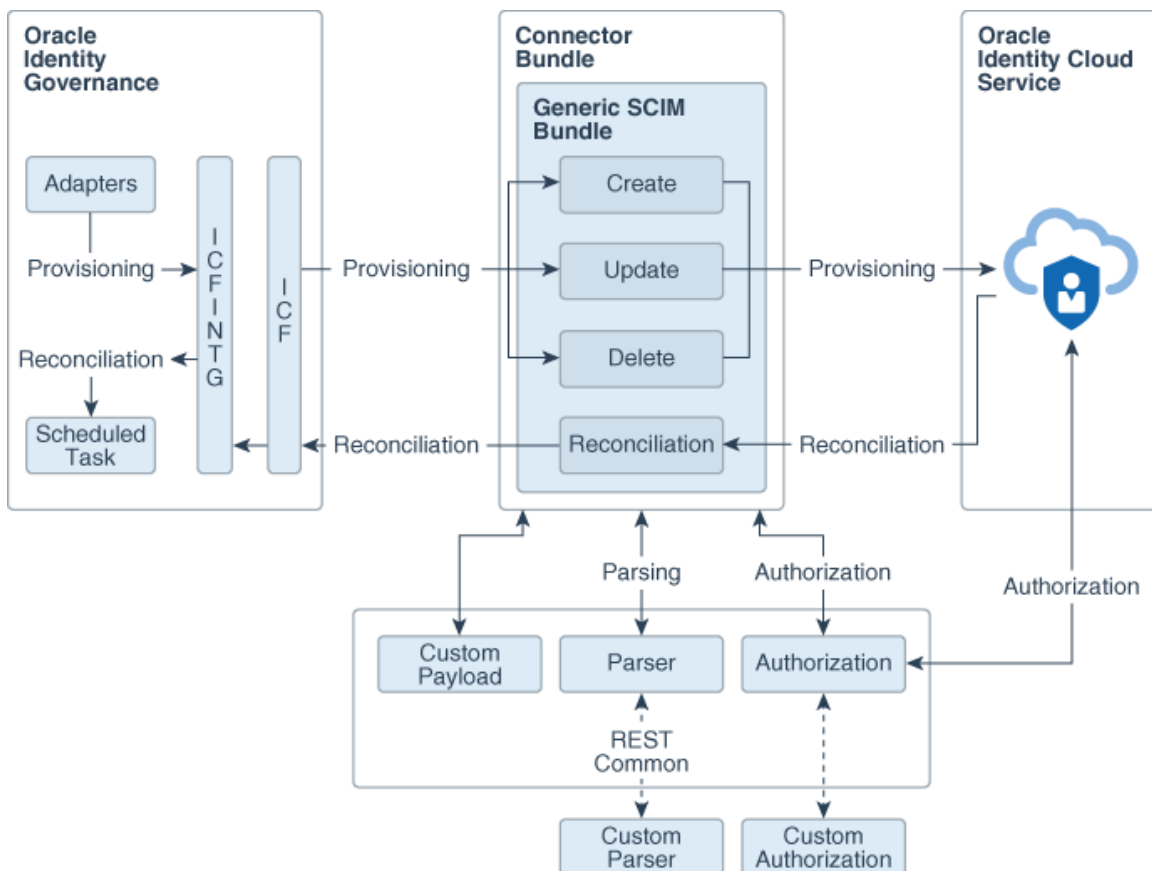
1.5 Connector Architecture

You can configure the Identity Cloud Service connector to run in the Target (or account management) mode, and is implemented using the Identity Connector Framework (ICF) component.

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

This connector enables management of target system accounts through Oracle Identity Governance. [Figure 1-1](#) shows the integration of on-premise Oracle Identity Governance with Oracle Identity Cloud Service.

Figure 1-1 Architecture of the Identity Cloud Service Connector



As shown in this figure, the Identity Cloud Service connector enables you to use the target system as a managed resource (target) of identity data for Oracle Identity Governance.

In the target mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Governance. In addition, you can use Oracle Identity Governance to perform provisioning operations on the target system.

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

The connector bundle is responsible for interacting with 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.

1.6 Supported Use Cases

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. 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 Governance provides a new integration called the 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 Governance 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 Identity Cloud Service to manage cloud applications but for the time being, they want to use only Oracle Identity Governance to manage identities in their ecosystem.

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

After installing the Identity Cloud Service connector, customer can manage complete lifecycle of the users and groups in Identity Cloud Service from Oracle Identity

Governance. Using this integration, ACME Corporation can create, update, enable, and disable the Identity Cloud Service users accessing the cloud applications. Also, it can assign or revoke Identity Cloud Service groups for a particular user accessing the cloud applications using Oracle Identity Governance.

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

1.7 Supported Connector Features Matrix

Provides the list of features supported by the AOB application and CI-based connector.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application	CI-Based Connector
Perform full and incremental reconciliation	Yes	Yes
Provision the Identity Cloud Service user and group accounts	Yes	Yes
Perform limited reconciliation	Yes	Yes
Perform batched reconciliation	Yes	Yes
Reconcile deleted user and group records into Oracle Identity Governance	Yes	Yes
Configure validation and transformation of account data	Yes	Yes
Clone applications or create new application instances	Yes	Yes
Use connector server	Yes	Yes
Provide secure communication to the target system through SSL	Yes	Yes

1.8 Connector Features

The features of the connector include support for provisioning user and group accounts, target resource reconciliation, reconciliation of all existing or modified account data, reconciliation of deleted user and group records, limited and batched reconciliation, transformation and validation of account data during reconciliation and provisioning, support for the connector server, multiple installations of the target system, secure communication to the target system through SSL, and so on.

- [Support for User and Group Provisioning](#)
- [Support for Full and Incremental Reconciliation](#)
- [Support for Limited Reconciliation](#)
- [Support for Batched Reconciliation](#)

- [Reconciliation of Deleted User and Group Records](#)
- [Transformation and Validation of Account Data](#)
- [Support for Cloning Applications and Creating Instance Applications](#)
- [Secure Communication to the Target System](#)
- [Support for the Connector Server](#)

1.8.1 Support for User and Group Provisioning

You can use the connector for provisioning user and group accounts.

You perform provisioning operations in Oracle Identity Governance by using the Create User page. See [Creating a User in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance](#) for details about the fields on the Create User page.

1.8.2 Support for Full and Incremental Reconciliation

After you create the application, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Governance. After the first full reconciliation run, incremental reconciliation is automatically enabled from the next run of the user reconciliation.

You can perform a full reconciliation run at any time. See [Performing Full and Incremental Reconciliation](#).

1.8.3 Support for Limited Reconciliation

You can set a reconciliation filter as the value of the Filter attribute of the scheduled tasks.

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

1.8.4 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](#).

1.8.5 Reconciliation of Deleted User and Group Records

You can use the connector to reconcile user and group records that are deleted on the target system into Oracle Identity Governance.

For more information about reconciliation jobs used for reconciling these deleted records, see [IDCS Target Resource User Delete Reconciliation Job](#) and [IDCS Group Delete Reconciliation Job](#).

1.8.6 Transformation and Validation of Account Data

You can configure transformation and validation of account data that is brought into or sent from Oracle Identity Governance during reconciliation and provisioning operations by writing Groovy scripts while creating your application.

For more information, see *Validation and Transformation of Provisioning and Reconciliation Attributes in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.8.7 Support for Cloning Applications and Creating Instance Applications

You can configure this connector for multiple installations of the target system by cloning applications or by creating instance applications.

When you clone an application, all the configurations of the base application are copied into the cloned application. When you create an instance application, it shares all configurations as the base application.

For more information about these configurations, see *Cloning Applications and Creating Instance Applications in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.8.8 Secure Communication to the Target System

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

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

See [Configuring SSL for the Connector](#).

1.8.9 Support for the Connector Server

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

A Java connector server is useful when you do not wish to execute a Java connector bundle in the same VM as your application. It can be beneficial to run a Java connector on a different host for performance improvements.

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 Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

2

Creating an Application By Using the Identity Cloud Service Connector

Learn about onboarding applications using the connector and the prerequisites for doing so.

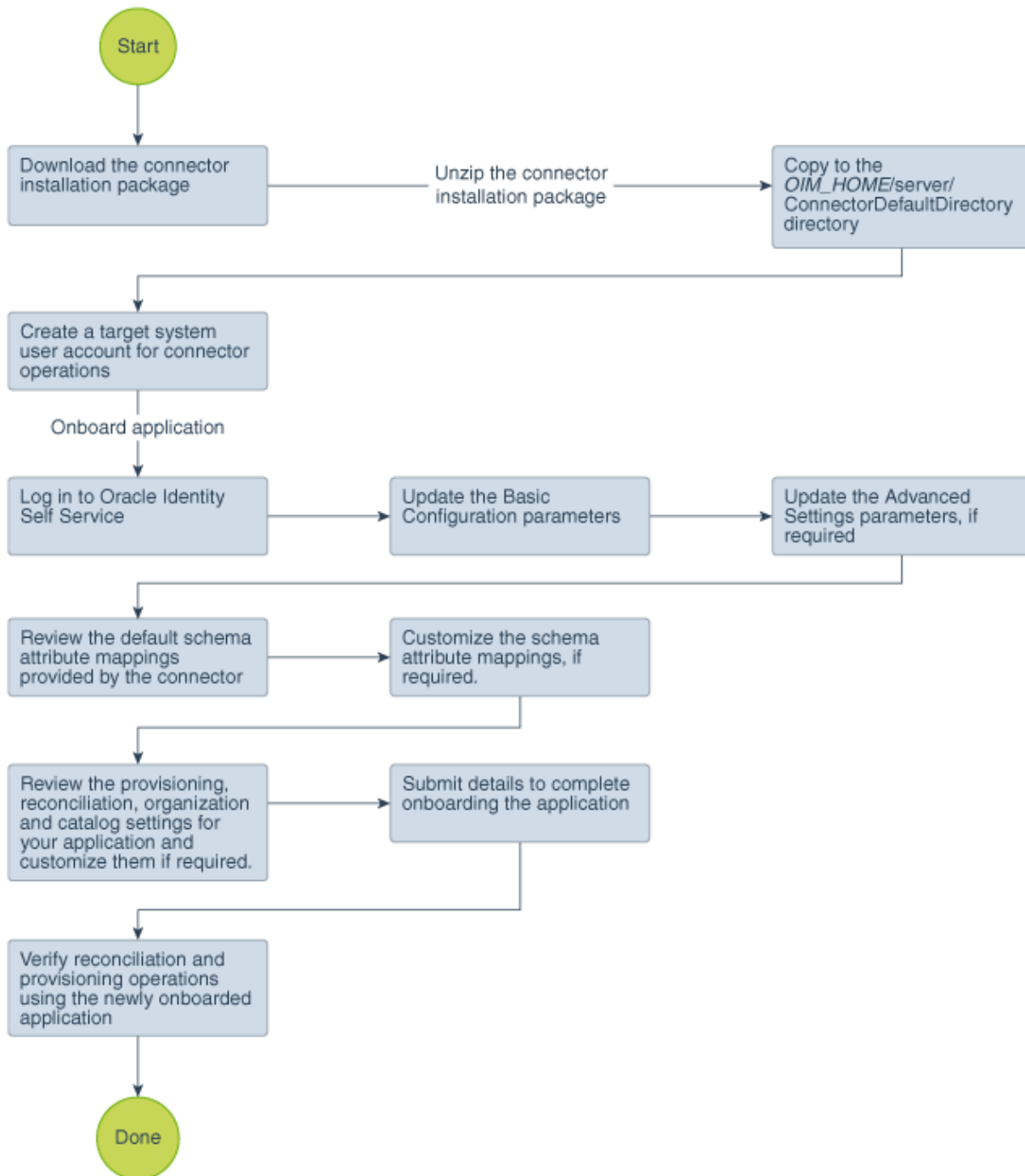
- [Process Flow for Creating an Application By Using the Connector](#)
- [Prerequisites for Creating an Application By Using the Connector](#)
- [Creating an Application By Using the Connector](#)

2.1 Process Flow for Creating an Application By Using the Connector

From Oracle Identity Governance release 12.2.1.3.0 onward, connector deployment is handled using the application onboarding capability of Identity Self Service.

[Figure 2-1](#) is a flowchart depicting high-level steps for creating an application in Oracle Identity Governance by using the connector installation package.

Figure 2-1 Overall Flow of the Process for Creating an Application By Using the Connector



2.2 Prerequisites for Creating an Application By Using the Connector

Learn about the tasks that you must complete before you create the application.

- [Configuring the Target System](#)
- [Downloading the Connector Installation Package](#)

2.2.1 Configuring the Target System

Configuring the target system involves registering and generating a client application so that the connector can access Identity Cloud Service APIs. It also involves creating a target system account for connector operations.

 **Note:**

The detailed instructions for performing these tasks are available in the target system documentation. See *Adding a Trusted Application in Oracle Cloud Administering Oracle Identity Cloud Service*.

To configure the target system:

1. Add a trusted application in Identity Cloud Service. Because the connector operates as a multitarget environment, the application needs to be registered on the 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 **Grant the client 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. On 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.
4. Activate the application.

The client ID and client secret values are displayed. You provide these values for the `customAuthHeaders` parameter (by creating a Base64 encoded string) in [Basic Configuration Parameters](#).

2.2.2 Downloading the Connector Installation Package

You can obtain the installation package for your connector on the Oracle Technology Network (OTN) website.

To download the connector installation package:

1. Navigate to the OTN website at <http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html>.
2. Click **OTN License Agreement** and read the license agreement.
3. Select the **Accept License Agreement** option.

You must accept the license agreement before you can download the installation package.

4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.
5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named `CONNECTOR_NAME-RELEASE_NUMBER`.
6. Copy the `CONNECTOR_NAME-RELEASE_NUMBER` directory to the `OIG_HOME/server/ConnectorDefaultDirectory` directory.

2.3 Creating an Application By Using the Connector

You can onboard an application into Oracle Identity Governance from the connector package by creating a Target application. To do so, you must log in to Identity Self Service and then choose the **Applications** box on the **Manage** tab.

The following is the high-level procedure to create an application by using the connector:

Note:

For detailed information on each of the steps in this procedure, see *Creating Applications of Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1. Create an application in Identity Self Service. The high-level steps are as follows:
 - a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.
 - b. Ensure that the **Connector Package** option is selected when creating an application.
 - c. Update the basic configuration parameters to include connectivity-related information.
 - d. If required, update the advanced setting parameters to update configuration entries related to connector operations.

- e. Review the default user account attribute mappings. If required, add new attributes or you can edit or delete existing attributes.
- f. Review the provisioning, reconciliation, organization, and catalog settings for your application and customize them if required. For example, you can customize the default correlation rules for your application if required.
- g. Review the details of the application and click **Finish** to submit the application details.

The application is created in Oracle Identity Governance.

- h. When you are prompted whether you want to create a default request form, click **Yes** or **No**.

If you click **Yes**, then the default form is automatically created and is attached with the newly created application. The default form is created with the same name as the application. The default form cannot be modified later. Therefore, if you want to customize it, click **No** to manually create a new form and attach it with your application.

2. Verify reconciliation and provisioning operations on the newly created application.

 **See Also:**

- [Configuring the Identity Cloud Service Connector](#) for details on basic configuration and advanced settings parameters, default user account attribute mappings, default correlation rules, and reconciliation jobs that are predefined for this connector
- [Configuring Oracle Identity Governance](#) for details on creating a new form and associating it with your application, if you chose not to create the default form

3

Configuring the Identity Cloud Service Connector

While creating an application, you must configure connection-related parameters that the connector uses to connect Oracle Identity Governance with your target system and perform connector operations. In addition, you can view and edit attribute mappings between the process form fields in Oracle Identity Governance and target system columns, predefined correlation rules, situations and responses, and reconciliation jobs.

- [Basic Configuration Parameters](#)
- [Advanced Settings Parameters](#)
- [Attribute Mappings](#)
- [Correlation Rules, Situations, and Responses](#)
- [Reconciliation Jobs](#)

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to the Identity Cloud Service.

Table 3-1 Basic Configuration Parameters for Identity Cloud Service

Parameter	Mandatory?	Description
acceptType	Yes	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. Sample value: application/json
authenticationServerUrl	Yes	The URL of the authentication server if authentication type is "BASIC". Sample value: https://api.example.com/oauth2/token
baseURI	Yes	The base URI is the base relative URL of the Identity Cloud Service target system. Sample value: If the target system URL is http://host:port/admin/v1, then the base URI is /admin/v1.
contentType	Yes	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. Sample value: application/json

Table 3-1 (Cont.) Basic Configuration Parameters for Identity Cloud Service

Parameter	Mandatory?	Description
customAuthHeaders	Yes	<p>Client identifier and client secret values used for authorization with your target system.</p> <p>Enter a value for this parameter in the following format: "Authorization=Basic <Base64 Encode ClientID:ClientSecret>"</p> <p>In this format, replace <Base64 Encode ClientID:ClientSecret> with the Base64 encoded string. You create this string by using the client ID and client secret values generated while registering your client application. See Configuring the Target System.</p> <p>Sample value: "Authorization=Basic AbC123XY1aBCXYZxYZabC123XyzabCABCXYZ123AbC1XY1aBCXYZxYZabC123XyzabCABCXYZ123"</p>
grantType	Yes	<p>Type of authentication used by your target system.</p> <p>Sample value: password or client_credentials</p>
host	Yes	<p>Host name or IP address of the computer hosting the target system.</p> <p>Sample value: www.example.com</p>
port	Yes	<p>Port number at which the target system is listening.</p> <p>Sample value: 80</p>
scope	Yes	<p>Scope is required to authenticate request based on "OAuth2.0 Resource Owners Password or Client Credentials" authentication type.</p> <p>Sample value: urn:opc:idm:__myscopes__</p>
sslEnabled	Yes	<p>If the target system requires SSL connectivity, set the value of this parameter to true. Otherwise, set the value to false.</p>
Connector Server Name	No	<p>Name of the IT resource of type "Connector Server".</p> <p>By default, this field is blank. If you have deployed the connector in a Java Connector Server, then enter the name of the IT resource for the Connector Server.</p>
username	No	<p>User name or User ID used if authentication type is "basic" or "password".</p> <p>Sample value: johnsmith</p>
password	No	<p>Password used if authentication type is "basic" or "password".</p> <p>Sample value: password</p>

3.2 Advanced Settings Parameters

These are the configuration-related entries that the connector uses during reconciliation and provisioning operations.

Table 3-2 Advanced Settings Parameters for Identity Cloud Service


Parameter	Mandatory ?	Description
relURLs	No	<p>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.</p> <p>Default value: "__ACCOUNT__.password.UpdateOp=/Users/\$(__ACCOUNT__.__UID__)\$"</p>
<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>You can update this parameter to delete a user that is associated with one or more entities (Groups or Applications) in Identity Cloud Service. To do so, add the "__ACCOUNT__.DeleteOp=/Users/\$(__ACCOUNT__.__UID__)\$?forceDelete=true" value at the end of this entry.</p> <p>The updated sample value is: "__ACCOUNT__.password.UpdateOp=/Users/\$(__ACCOUNT__.__UID__)\$", "__ACCOUNT__.DeleteOp=/Users/\$(__ACCOUNT__.__UID__)\$?forceDelete=true".</p> <p>If you do not update this entry and try to delete the user, an error message is displayed. For details on the error message, see Troubleshooting the Identity Cloud Service Connector.</p> </div>		
Bundle Name	No	<p>This entry holds the name of the connector bundle package.</p> <p>Default value: org.identityconnectors.genericscim</p>
Bundle Version	No	<p>This entry holds the version of the connector bundle.</p> <p>Default value: 12.3.0</p>
Connector Name	No	<p>This entry holds the name of the connector class.</p> <p>Default value: org.identityconnectors.genericscim.GenericSCIMConnector</p>
nameAttributes	Yes	<p>This entry indicates the attributes that need to be treated as the __NAME__ attribute for an Object class.</p> <p>Default value: "Users=username", "Groups=displayName"</p>
uidAttributes	Yes	<p>This entry holds the UID attribute for the objects that are handled by the connector. For example, the UID attribute is ID for User accounts.</p> <p>Default value: "Users=id", "Groups=id"</p>
statusAttributes	No	<p>This entry lists the name of the target system attribute that holds the status of an account.</p> <p>This entry indicates the status field: The __ENABLE__ field on the target for an object class.</p> <p>Default value: "Users=active"</p>

Table 3-2 (Cont.) Advanced Settings Parameters for Identity Cloud Service

Parameter	Mandatory ?	Description
passwordAttributes	No	This entry indicates the attributes that need to be treated as the <code>__PASSWORD__</code> attribute for an object class. Default value: "Users=password"
attrToOClassMapping	No	This entry denotes that the groups attribute of the <code>__ACCOUNT__</code> object class is mapped to the Groups object class on the target. Default value: " __ACCOUNT__.groups=Groups"
scimVersion	Yes	This indicates the SCIM version on which the target is implemented. Default value: 17
jsonResourcesTag	No	This JSON tag value is used during reconciliation for parsing multiple entries in a single response payload. Default value: Resources
customPayload	No	This entry holds the payloads for all operations that are not in the standard format. Default value: " __ACCOUNT__.password.UpdateOp={\"Operations\": [{\"op\": \"replace\", \"path\": \"password\", \"value\": \"\${__ACCOUNT__.password}\"}], \"schemas\": [\"urn:ietf:params:scim:api:messages:2.0:PatchOp\"]}, \"__ACCOUNT__.groups.AddOp={\"schemas\": [\"urn:ietf:params:scim:api:messages:2.0:PatchOp\"], \"Operations\": [{\"op\": \"add\", \"path\": \"members\", \"value\": [{\"value\": \"\${__ACCOUNT__.__UID}\"}]}] }"
Any Incremental Recon Attribute Type	No	By default, during incremental reconciliation, Oracle Identity Governance 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 Governance will accept time stamp information in any datatype format. Default value: true
httpOperationTypes	No	This entry indicates that for a Password Update operation, the target needs a PUT operation instead of PATCH. Default value: " __ACCOUNT__.password.UpdateOp=PATCH"
reconSortByAttrs	No	This entry holds the attribute used for sorting the records during a reconciliation operation. Default value: "Users=id", "Groups=id"
managedObjectClasses	No	This entry holds the value of object classes used by the target system. Operations related to users and groups use this parameter to store the corresponding object classes of the target system. Default value: "Users", "Groups"

Table 3-2 (Cont.) Advanced Settings Parameters for Identity Cloud Service

Parameter	Mandatory ?	Description
hashPasswordEnabled	No	<p>This entry specifies whether hashing must be enabled on the default password that is sent to the target system when a new account is created.</p> <p>Default value: <code>false</code></p> <p>This implies that hashing is not enabled and the default password is sent in a plain text format.</p> <p>Note: To enable hashing on the default password, set the value of this parameter to <code>true</code>.</p> <p>For more information on enabling hashing during the Create User provisioning operation, see Guidelines on Performing Provisioning Operations.</p>
hashAlgorithm	No	<p>This entry holds the value of hash algorithm that the connector uses if the <code>hashPasswordEnabled</code> parameter is set to <code>true</code>.</p> <p>Default value: <code>PBKDF2WithHmacSHA256</code></p> <p>The supported algorithms are:</p> <ul style="list-style-type: none"> • <code>PBKDF2WithHmacSHA1</code> • <code>PBKDF2WithHmacSHA256</code> • <code>PBKDF2WithHmacSHA384</code> • <code>PBKDF2WithHmacSHA512</code>

3.3 Attribute Mappings

The Schema page for a Target application displays the default schema (provided by the connector) that maps Oracle Identity Governance attributes to target system attributes. The connector uses these mappings during reconciliation and provisioning operations.

Identity Cloud Service User Account Attributes

[Table 3-3](#) lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and Identity Cloud Service attributes. The table also lists whether a specific attribute is used during provisioning or reconciliation and whether it is a matching key field for fetching records during reconciliation.

If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in *Creating a Target Application of Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-3 Default Attribute Mappings for the Identity Cloud Service User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive ?
Id	__UID__	String	No	Yes	Yes	Yes	Not Applicable
User Name	__NAME__	String	Yes	Yes	Yes	No	Not Applicable

Table 3-3 (Cont.) Default Attribute Mappings for the Identity Cloud Service User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
First Name	name.givenName	String	Yes	Yes	Yes	No	Not Applicable
Last Name	name.familyName	String	Yes	Yes	Yes	No	Not Applicable
Middle Name	name.middleName	String	No	Yes	Yes	No	Not Applicable
Manager	manager.value	String	No	Yes	Yes	No	Not Applicable
Employee Number	employeeNumber	String	No	Yes	Yes	No	Not Applicable
Email	__ACCOUNT__.emails.value,type:work,primary:true	String	Yes	Yes	Yes	No	Not Applicable
User Type	userType	String	No	Yes	Yes	No	Not Applicable
Organization	organization	String	No	Yes	Yes	No	Not Applicable
Password	__PASSWORD__	String	No	Yes	No	No	Not Applicable
Creation Mechanism	creationMechanism	String	No	Yes	No	No	Not Applicable
Status	__ENABLE__	String	No	Yes	Yes	No	Not Applicable

Figure 3-1 shows the default user account attribute mappings.

Figure 3-1 Default Attribute Mappings for the Identity Cloud Service User Account

Application Attribute				Provisioning Property		Reconciliation Properties			
Identity Attribute	Display Name	Target Attribute	Data Type	Mandatory	Provision Field	Recon Field	Key Field	Case Insensitive	
Enter a value	Id	__UID__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	✕
Enter a value	User Name	__NAME__	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕
Enter a value	First Name	name.givenName	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕
Enter a value	Last Name	name.familyName	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕
Enter a value	Middle Name	name.middleName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕
Enter a value	Manager	manager.value	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕
Enter a value	Employee Numbe	employeeNumber	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕
Enter a value	Email	__ACCOUNT__emails.value,...	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕
Enter a value	User Type	userType	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕
Enter a value	Organization	organization	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕
Enter a value	Password	__PASSWORD__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕
Enter a value	Creation Mechani	creationMechanism	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕
Enter a value	Status	__ENABLE__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕

Group Names Child Attributes

Table 3-4 lists the attribute mappings for group names between the process form fields in Oracle Identity Governance and Identity Cloud Service attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in *Creating a Target Application of Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-4 Default Attribute Mappings for the Identity Cloud Service Group Names

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Group Value	__ACCOUNT__ _groups~__A CCOUNT__.gr oups~value	String	No	Yes	Yes	Not Applicable

Figure 3-2 shows the default group name attribute mappings.

Figure 3-2 Default Attribute Mappings for the Identity Cloud Service Group Names

Groups

+ Add Attribute Delete Form Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties			
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive	
Group Value	__ACCOUNT__groups~__ACC	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	X ☰

3.4 Correlation Rules, Situations, and Responses

Learn about the predefined rules, responses and situations for an Identity Cloud Service Target application. The connector use these rules and responses for performing reconciliation.

Predefined Identity Correlation Rules

By default, the Identity Cloud Service connector provides a simple correlation rule when you create a Target application. The connector uses this correlation rule to compare the entries in Oracle Identity Governance repository and the target system repository, determine the difference between the two repositories, and apply the latest changes to Oracle Identity Governance.

If required, you can edit the default correlation rule or add new rules. You can create simple correlation rules also. For more information about adding or editing simple or complex correlation rules, see *Updating Identity Correlation Rule in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-5 Predefined Identity Correlation Rule for an Identity Cloud Service Target Application

Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

In this identity rule:

- __NAME__ is a single-valued attribute on the target system that identifies the user account.
- User Login is the field on the OIG User form.

Figure 3-3 shows the simple correlation rule for the Identity Cloud Service connector.

Figure 3-3 Simple Correlation Rule for an Identity Cloud Service Target Application

Identity Correlation Rule

Choose Type of Correlation Rule

Simple Correlation Rule Complex Correlation Rule

+ Add Rule Element

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
NAME	Equals	User Login	<input type="checkbox"/>	X

Rule Operator

AND

Predefined Situations and Responses

The Identity Cloud Service connector provides a default set of situations and responses when you create a Target application. These situations and responses specify the action that Oracle Identity Governance must take based on the result of a reconciliation event.

Table 3-6 lists the default situations and responses for the Identity Cloud Service connector. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see *Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-6 Predefined Situations and Responses for an Identity Cloud Service Target Application

Situation	Response
No Matches Found	None
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Figure 3-4 shows the default situations and responses for the Identity Cloud Service connector.

Figure 3-4 Default Situations and Responses for an Identity Cloud Service Target Application

Situations And Responses

+ Add

Situation	Response	
No Matches Found	None	X
One Entity Match Found	Establish Link	X
One Process Match Found	Establish Link	X

3.5 Reconciliation Jobs

Learn about the reconciliation jobs that are automatically created in Oracle Identity Governance after you create the application for your target system.

You can either use these predefined jobs or edit them to meet your requirements. Alternatively, you can create custom reconciliation jobs. For information about editing these predefined jobs or creating new ones, see *Updating Reconciliation Jobs in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

IDCS Target Resource User Reconciliation Job

You use the IDCS Target Resource User Reconciliation job to perform full or incremental reconciliation, which involves reconciling all user records from a target application into Oracle Identity Governance.

Table 3-7 Parameters of the IDCS Target Resource User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Note: Do <i>not</i> modify this value.
Batch Size	Enter the number of records that must be included in each batch fetched from the target system during reconciliation. By default, the value of this attribute is empty, indicating that all records are included for reconciliation.
Filter	Enter the search filter for fetching records from the target system during a reconciliation run. See Performing Limited Reconciliation for more information about filtered reconciliation.
Incremental Recon Attribute	This attribute holds the value of the target system attribute that is specified as the value of the Incremental Recon Attribute attribute. Default value: <code>meta.lastModified</code> Note: Do <i>not</i> modify this value.
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: <code>User</code> Note: <code>User</code> is the only object that is supported. Therefore, do <i>not</i> change the value of this attribute.

Table 3-7 (Cont.) Parameters of the IDCS Target Resource User Reconciliation Job

Parameter	Description
Latest Token	Attribute that holds the date on which the token record is modified. The Latest Token attribute is used for internal purposes. By default, this value is empty. Note: Do <i>not</i> 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>
Scheduled Task Name	Name of the scheduled job. Note: For the scheduled job included with this connector, you must <i>not</i> change the value of this attribute. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this attribute.

IDCS Target Resource User Delete Reconciliation Job

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

Table 3-8 Parameters of the IDCS Target Resource User Delete Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Note: Do <i>not</i> modify this value.
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 <i>not</i> change the value of this attribute.
Batch Size	Enter the number of records that must be included in each batch fetched from the target system during reconciliation. By default, the value of this attribute is empty, indicating that all records are included for reconciliation.

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- IDCS Group Lookup Reconciliation: Use this job to reconcile all group data in the target system into lookup fields in Oracle Identity Governance.
- IDCS Manager Lookup Reconciliation: Use this job to reconcile all manager data in the target system into lookup fields in Oracle Identity Governance.

The parameters for all the reconciliation jobs are the same.

Table 3-9 Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	<p>Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application.</p> <p>Note: Do <i>not</i> modify this value.</p>
Lookup Name	<p>This parameter holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched.</p> <p>Depending on the reconciliation job you are using, the default values are as follows:</p> <ul style="list-style-type: none"> • For IDCS Group Lookup Reconciliation: Lookup.IDCS.Groups • For IDCS Manager Lookup Reconciliation: Lookup.IDCS.Managers
Object Type	<p>Enter the type of object whose values must be synchronized.</p> <p>Depending on the scheduled job you are using, the default values are as follows:</p> <ul style="list-style-type: none"> • For IDCS Group Lookup Reconciliation: Group • For IDCS Manager Lookup Reconciliation: __ACCOUNT__ <p>Note: Do <i>not</i> modify this value.</p>
Code Key Attribute	<p>Enter the 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).</p> <p>Default value: __UID__</p> <p>Note: Do <i>not</i> modify this value.</p>
Decode Attribute	<p>Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute).</p> <p>Default value: __NAME__</p>

4

Performing the Postconfiguration Tasks for the Identity Cloud Service Connector

These are the tasks that you must perform after creating an application in Oracle Identity Governance.

- [Configuring Oracle Identity Governance](#)
- [Harvesting Entitlements and Sync Catalog](#)
- [Managing Logging for the Connector Server](#)
- [Configuring the IT Resource for the Connector Server](#)
- [Localizing Field Labels in UI Forms](#)
- [Configuring SSL for the Connector](#)

4.1 Configuring Oracle Identity Governance

During application creation, if you did not choose to create a default form, then you must create a UI form for the application that you created by using the connector.

 **Note:**

Perform the procedures described in this section only if you did not choose to create the default form during creating the application.

The following topics describe the procedures to configure Oracle Identity Governance:

- [Creating and Activating a Sandbox](#)
- [Creating a New UI Form](#)
- [Publishing a Sandbox](#)
- [Updating an Existing Application Instance with a New Form](#)

4.1.1 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 a Sandbox](#) in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

4.1.2 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 Governance*.

While creating the UI form, ensure that you select the resource object corresponding to the newly created application that you want to associate the form with. In addition, select the **Generate Entitlement Forms** check box.

4.1.3 Publishing a Sandbox

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

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

4.1.4 Updating an Existing Application Instance with a New Form

For any changes that you do in the schema of your application in Identity Self Service, 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 and activate a sandbox.
2. Create a new UI form for the resource.
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 Also:**

- *Creating a Sandbox and Activating a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*
- *Creating Forms By Using the Form Designer in Oracle Fusion Middleware Administering Oracle Identity Governance*
- *Publishing a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*

4.2 Harvesting Entitlements and Sync Catalog

You can populate Entitlement schema from child process form table, and harvest roles, application instances, and entitlements into catalog. You can also load catalog metadata.

To harvest entitlements and sync the catalog:

1. Run the scheduled jobs for lookup field synchronization listed in [Reconciliation Jobs for Entitlements](#).
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:**

Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Governance* for a description of the Entitlement List and Catalog Synchronization Job scheduled jobs

4.3 Managing Logging for the Connector Server

Oracle Identity Governance 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](#)

4.3.1 Understanding Log Levels

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

ODL is the principle logging service used by Oracle Identity Governance 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 Governance to continue running.
- `WARNING`
This level enables logging of information about potentially harmful situations.
- `INFO`
This level enables logging of messages that highlight the progress of the application.
- `CONFIG`
This level enables logging of information about fine-grained events that are useful for debugging.
- `FINE, FINER, FINEST`
These levels enable logging of information about fine-grained events, where `FINEST` logs information about all events.

These message types are mapped to ODL message type and level combinations as shown in [Table 4-1](#).

Table 4-1 Log Levels and ODL Message Type:Level Combinations

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

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 Governance.

4.3.2 Enabling Logging

Perform this procedure to enable logging in Oracle WebLogic Server.

To enable logging:

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. [Understanding Log Levels](#) 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 Governance, 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.

4.4 Configuring the IT Resource for the Connector Server

If you have used the Connector Server, then you must configure values for the parameters of the Connector Server IT resource.

After you create the application for your target system, you must create an IT resource for the Connector Server as described in *Creating IT Resource of Oracle Fusion Middleware Administering Oracle Identity Governance*. While creating the IT resource, ensure to use to select **Connector Server** from the **IT Resource Type** list.

In addition, specify values for the parameters of the IT resource for the Connector Server listed in [Table 4-2](#).

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

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. Sample value: myhost.com
Key	Enter the key for the Connector Server.
Port	Enter the number of the port at which the Connector Server is listening. By default, this value is blank. You must enter the port number that is displayed on the terminal when you start the Connector Server. 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 Governance times out. Recommended 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 Governance and the Connector Server. Otherwise, enter false. Default value: false Note: It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see <i>Configuring SSL for Java Connector Server in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance</i> .

4.5 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. The resource bundles are available in the connector installation package.

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:

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

 **Note:**

You will not be able to view the BizEditorBundle.xlf unless you complete creating the application for your target system or perform any customization such as creating a UDF.

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 the 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 Governance* for more information about exporting and importing metadata files

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

4.6 Configuring SSL for the Connector

You must configure SSL to secure communication between Oracle Identity Governance and your target system. Configuring SSL involves obtaining an SSL certificate from the target system and importing it into the identity keystore of Oracle Identity Governance.

Identity Cloud Service validates the client system dates to be in sync with the SSL certificate (the certificate issued by the 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.

To configure SSL:

1. Obtain an SSL certificate from the target system:
 - a. Open a web browser and enter the target system URL.
The target system loads the SSL certificate in your browser.
 - b. View and download the certificate.
2. Use the `keytool` command to import the downloaded certificate into the identity keystore in Oracle Identity Governance.

```
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.

5

Using the Identity Cloud Service Connector

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

- [Configuring Reconciliation](#)
- [Configuring Reconciliation Jobs](#)
- [Configuring Provisioning](#)
- [Connector Objects Used For Group Management](#)
- [Uninstalling the Connector](#)

5.1 Configuring Reconciliation

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 and Incremental Reconciliation](#)
- [Performing Limited Reconciliation](#)
- [Performing Batched Reconciliation](#)

5.1.1 Performing Full and Incremental Reconciliation

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

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 Governance.

To perform a full reconciliation run, ensure that a value is **not** specified for the Filter and Latest Token attributes of scheduled jobs for reconciling user and group records.

At the end of the reconciliation run, the Latest Token attribute of the scheduled jobs for user and group 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.

See [IDCS Target Resource User Reconciliation Job](#) and [IDCS Group Reconciliation Job](#) for information about these scheduled jobs.

You specify values for these attributes by following the instructions described in [Configuring Reconciliation Jobs](#).

5.1.2 Performing Batched Reconciliation

You can perform batched reconciliation to reconcile a specific number of records from the target system into Oracle Identity Governance.

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

You can configure batched reconciliation to avoid these problems.

To configure batched reconciliation, you must specify a value for the Batch Size attribute of scheduled jobs for reconciling user and group records. The Batch Size attribute is used to specify the number of records that must be included in each batch. See [IDCS Target Resource User Reconciliation Job](#), [IDCS Target Resource User Delete Reconciliation Job](#), and [IDCS Group Reconciliation Job](#) for information about these scheduled jobs.

By default, the value of this attribute is empty, indicating that all records are included (no batched reconciliation).

You specify values for these attributes by following the instructions described in [Configuring Reconciliation Jobs](#).

5.1.3 Performing Limited Reconciliation

You can perform limited reconciliation by creating filters for the reconciliation module, and reconcile records from the target system based on a specified filter criterion.

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.

This connector provides a Filter attribute (a scheduled job attribute) that allows you to use any of the Identity Cloud Service resource attributes to filter the target system records. See [IDCS Target Resource User Reconciliation Job](#) and [IDCS Group Reconciliation Job](#).

 **Note:**

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

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

You specify values for these attributes by following the instructions described in [Configuring Reconciliation Jobs](#).

5.2 Configuring Reconciliation Jobs

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

You can apply this procedure to configure the reconciliation jobs for users and entitlements.

To configure a reconciliation job:

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

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

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

 **Note:**

Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.

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.

5.3 Configuring Provisioning

Learn about performing provisioning operations in Oracle Identity Governance and the guidelines that you must apply while performing these operations.

- [Guidelines on Performing Provisioning Operations](#)
- [Performing Provisioning Operations](#)

5.3.1 Guidelines on Performing Provisioning Operations

These are the guidelines that you must apply while performing provisioning operations.

- During the Create User provisioning operation, if you do not want to send the account creation notification to users from the target system and do not want users to reset password on first login, then you must enable hashing on the default password. To do so, set the `hashPasswordEnabled` advanced settings parameter to `true`.

As a result, accounts are provisioned on Identity Cloud Service with the password that is assigned to the corresponding Oracle Identity Governance Users. Also, the e-mail notification is not sent from Identity Cloud Service and users do not need to reset password on first login in Identity Cloud Service.

- During the Delete User provisioning operation, if you want to delete users that are associated with one or more entities (Groups or Applications) in Identity Cloud Service, then you must update the `relURLs` advanced settings parameter. To do so, add the `"__ACCOUNT__.DeleteOp=/Users/${__ACCOUNT__.__UID__}$?forceDelete=true"` value at the end of the `relURLs` entry.

The updated sample value is: `"__ACCOUNT__.password.UpdateOp=/Users/${__ACCOUNT__.__UID__}$", "__ACCOUNT__.DeleteOp=/Users/${__ACCOUNT__.__UID__}$?forceDelete=true"`.

For details on the `hashPasswordEnabled` and `relURLs` parameters, see [Advanced Settings Parameters](#).

5.3.2 Performing Provisioning Operations

You create a new user in 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 Governance:

1. Log in to Identity Self Service.
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 for the connector that you configured earlier, and then click **Checkout**.
5. Specify value for fields in the application form and then click **Ready to Submit**.
6. Click **Submit**.

 **See Also:**

Creating a User in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance* for details about the fields on the Create User page

5.4 Connector Objects Used For Group Management

Learn about the objects that are used by the connector to perform group management operations such as create, update, and delete.

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

- [Lookup Definitions for Group Management](#)
- [Reconciliation Scheduled Jobs for Group Management](#)
- [Reconciliation Rules for Group Management](#)
- [Reconciliation Action Rules for Group Management](#)

5.4.1 Lookup Definitions for Group Management

These are the lookup definitions that map group resource object fields in Oracle Identity Governance and the target system attributes. The Lookup.IDCS.GM.ReconAttrMap lookup definition is used for performing target resource group reconciliation runs. The Lookup.IDCS.GM.ProvAttrMap lookup definition is used for performing group provisioning operations.

[Table 5-1](#) lists the entries in the Lookup.IDCS.GM.ReconAttrMap and Lookup.IDCS.GM.ProvAttrMap lookup definitions.

Table 5-1 Entries in the Lookup Definitions for Group Management

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

5.4.2 Reconciliation Scheduled Jobs for Group Management

After you create an application, reconciliation scheduled jobs are automatically created for group management operations in Oracle Identity Governance. You must configure these scheduled jobs to suit your requirements by specifying values for its attributes.

This topic provides information about the following scheduled jobs

- [IDCS Group Reconciliation Job](#)
- [IDCS Group Delete Reconciliation Job](#)

5.4.2.1 IDCS Group Reconciliation Job

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

Table 5-2 Attributes of the IDCS Group Reconciliation Scheduled Job

Attribute	Description
Filter	Enter the search filter for fetching records from the target system during a reconciliation run. See Performing Limited Reconciliation for more information about filtered reconciliation.
Incremental Recon Attribute	This attribute holds the value of the attribute that is specified as the value of the Incremental Recon Attribute. Default value: <code>meta.lastModified</code> Note: Do <i>not</i> 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 group records. Default value: Identity Cloud Services
Latest Token	Attribute that holds the date on which the token record was modified. The Latest Token attribute is used for internal purposes. By default, this value is empty. Note: Do <i>not</i> 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: Group Note: Group is the only object that is supported. Therefore, do <i>not</i> 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

5.4.2.2 IDCS Group Delete Reconciliation Job

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

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

Attribute	Description
Batch Size	Enter the number of records that must be included in each batch fetched from the target system during reconciliation. By default, the value of this attribute is empty, indicating that all records are included for reconciliation.
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile group records. Default value: Identity Cloud Services
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 <i>not</i> 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

5.4.3 Reconciliation Rules for Group Management

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

This section discusses the following topics related to group reconciliation rule for target resource reconciliation:

- [Reconciliation Rule for Groups](#)
- [Viewing Reconciliation Rules in the Design Console](#)

5.4.3.1 Reconciliation Rule for Groups

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

Rule name: IDCS Groups Recon Rule

Rule element: Organization Name Equals OIG Org Name.

In this rule:

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

5.4.3.2 Viewing Reconciliation Rules in the Design Console

You can view reconciliation rules for groups on the Reconciliation Rule Builder form in Oracle Identity Manager Design Console.

To view the reconciliation rule for groups:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tool** and then double-click **Reconciliation Rules**.
3. Search for and open the **IDCS Groups Recon Rule**.

5.4.4 Reconciliation Action Rules for Group Management

Reconciliation action rules specify the actions that the connector must perform depending on whether or not matching the Identity Cloud Service resources or Oracle Identity Governance 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 for Groups](#)
- [Viewing Reconciliation Action Rules in Design Console](#)

5.4.4.1 Reconciliation Action Rules for Groups

Reconciliation action rules specify the actions the connector must perform based on the result of the processing of a reconciliation event. These are the reconciliation action rules for groups.

Table 5-4 Reconciliation Action Rules for Groups

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

5.4.4.2 Viewing Reconciliation Action Rules in Design Console

You can view reconciliation action rules for groups 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 the **IDCS Group** resource object.
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.

5.5 Uninstalling the Connector

Uninstalling the Identity Cloud Service connector deletes all the account-related data associated with its resource objects.

If you want to uninstall the connector for any reason, then run the Uninstall Connector utility. Before you run this utility, ensure that you set values for `ObjectType` and `ObjectValues` properties in the `ConnectorUninstall.properties` file. For example, if you want to delete resource objects, scheduled tasks, and scheduled jobs associated with the connector, then enter "ResourceObject", "ScheduleTask", "ScheduleJob" as the value of the `ObjectType` property and a semicolon-separated list of object values corresponding to your connector as the value of the `ObjectValues` property.

For example: `IDCS User; IDCS Group`

Note:

If you set values for the `ConnectorName` and `Release` properties along with the `ObjectType` and `ObjectValue` properties, then the deletion of objects listed in the `ObjectValues` property is performed by the utility and the Connector information is skipped.

For more information, see *Uninstalling Connectors in Oracle Fusion Middleware Administering Oracle Identity Governance*.

6

Extending the Functionality of the Identity Cloud Service Connector

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

- [Adding New Group Attributes for Reconciliation](#)
- [Adding New Group Attributes for Provisioning](#)
- [Configuring Transformation and Validation of Data](#)
- [Configuring Action Scripts](#)
- [Configuring the Connector for Multiple Installations of the Target System](#)

6.1 Adding New Group Attributes for Reconciliation

The connector provides a default set of attribute mappings for reconciliation between Oracle Identity Governance and the target system. The default attribute mappings are listed in [Attribute Mappings](#). If required, you can add new user and group attributes for reconciliation.

You can edit the default user attribute mappings by adding new attributes or deleting existing attributes as described in *Creating a Target Application of Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

You can add new group attributes for reconciliation by performing the tasks listed in this section.

- [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](#)

Note:

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

6.1.1 Adding New Attributes on the Process Form

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

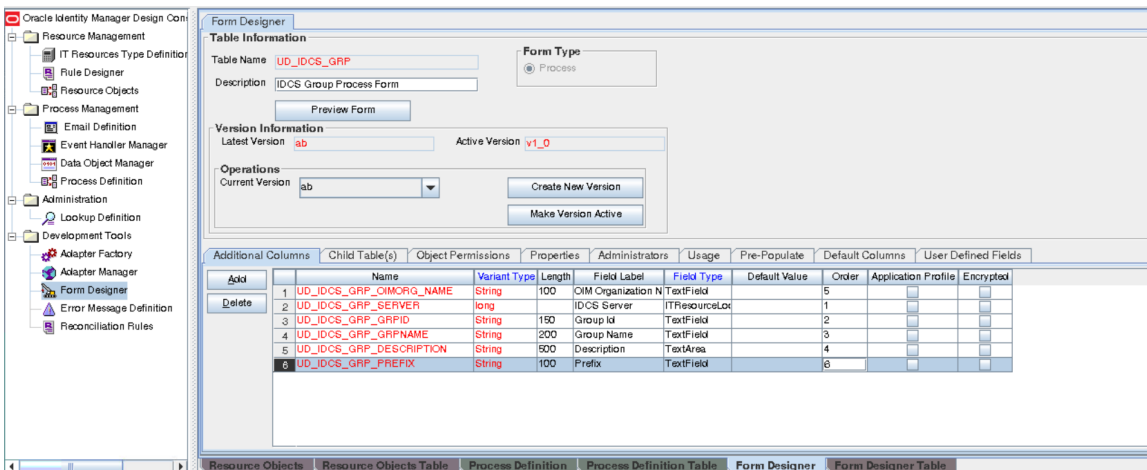
To add a new attribute on the process form:

1. Log in to the Oracle Identity Governance Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the **UD_IDCS_GRP** process form.
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_GRP_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 figure shows the new field added to the process form.

Figure 6-1 Form Designer



6.1.2 Adding Attributes to Reconciliation Fields

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

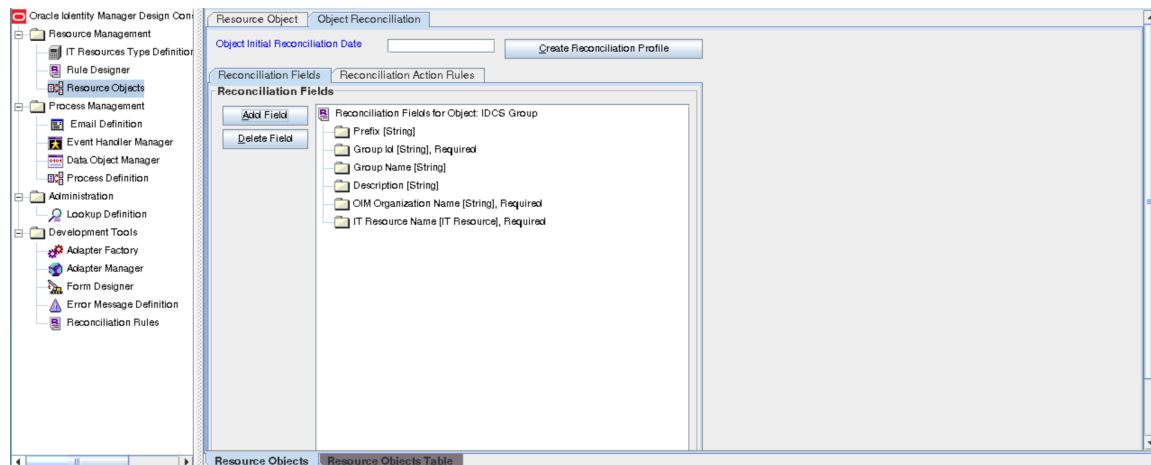
To add the new attribute to the list of reconciliation fields in the resource object:

1. Expand **Resource Management**, and double-click **Resource Objects**.
2. Search for and open the **IDCS Group** resource object.
3. On the **Object Reconciliation** tab, click **Add Field**.
4. Enter the details of the field.

For example, enter `Prefix` in the **Field Name** field and select **String** from the **Field Type** list.

- Click the **Save** icon. The following figure shows the new reconciliation field added to the resource object:

Figure 6-2 Object Reconciliation Tab



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

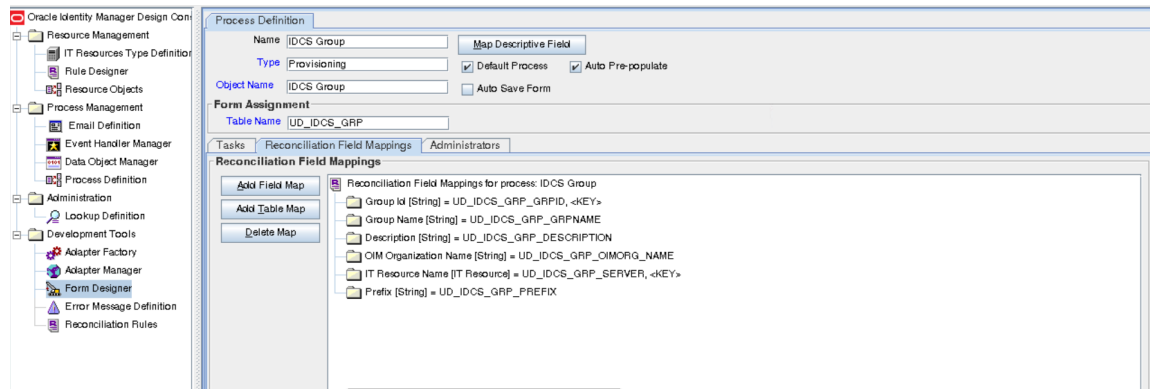
6.1.3 Creating Reconciliation Field Mapping

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

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

- Expand **Process Management**, and double-click **Process Definition**.
- Search for and open the **IDCS Group** process definition.
- On the Reconciliation Field Mappings tab of the **IDCS Group** process definition, click **Add Field Map**.
- From the Field Name list, select the field that you want to map.
- Double-click the **Process Data Field** field, and then select the column for the attribute. For example, select **UD_IDCS_GRP_PREFIX**.
- Click the **Save** icon. The following figure shows the new reconciliation field mapped to a process data field in the process definition:

Figure 6-3 Process Definition Tab



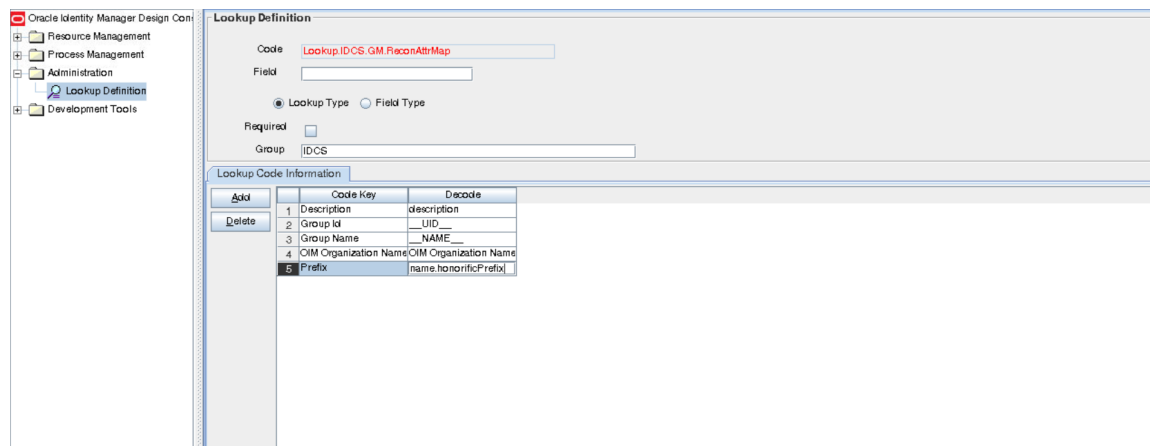
6.1.4 Creating Entries in Lookup Definitions

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 the **Lookup. IDCS.GM.Recon.AttrMap** lookup definition.
4. Click **Add** and enter the Code Key and Decode values for the field. The Code Key value must be the name of the field in the resource object.
5. Click the **Save** icon. The following figure shows the entry added to the lookup definition:

Figure 6-4 Lookup Definition Page



6.1.5 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*.

6.2 Adding New Group Attributes for Provisioning

The connector provides a default set of attribute mappings for provisioning between Oracle Identity Governance and the target system. The default attribute mappings are listed in [Attribute Mappings](#). If required, you can add new user and group attributes for provisioning.

You can edit the default user attribute mappings by adding new attributes or deleting existing attributes as described in *Creating a Target Application of Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

You can add new group attributes for provisioning by performing the tasks listed in this section.

- [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](#)

6.2.1 Adding New Attributes for Provisioning

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

 **Note:**

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

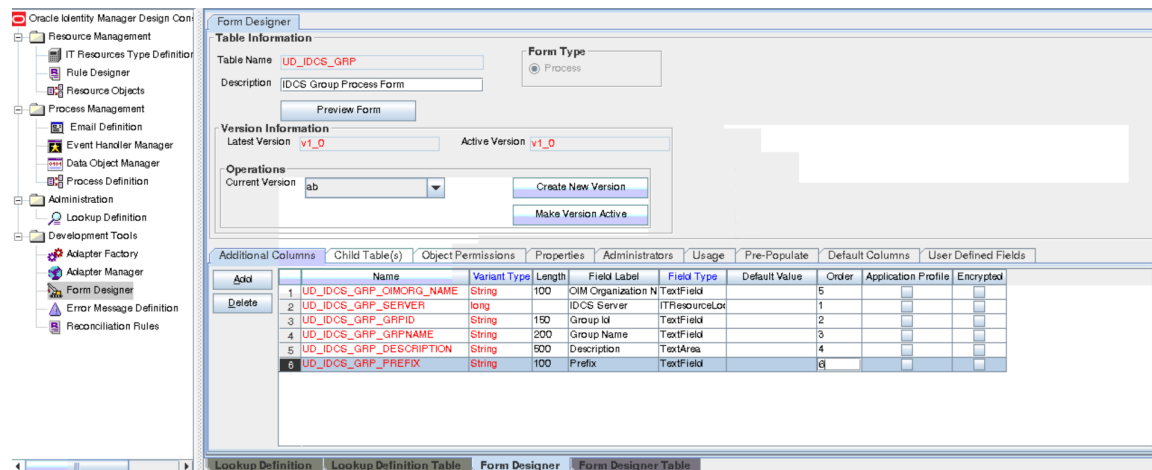
1. Log in to the Oracle Identity Governance Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the **UD_IDCS_GRP** process form.
4. Click **Create New Version**, and then click **Add**.
5. Enter the details of the attribute.

For example, if you are adding the PREFIX field, enter UD_IDCS_GRP_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 figure shows the new field added to the process form:

Figure 6-5 New Field Added to the Process Form



6.2.2 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.

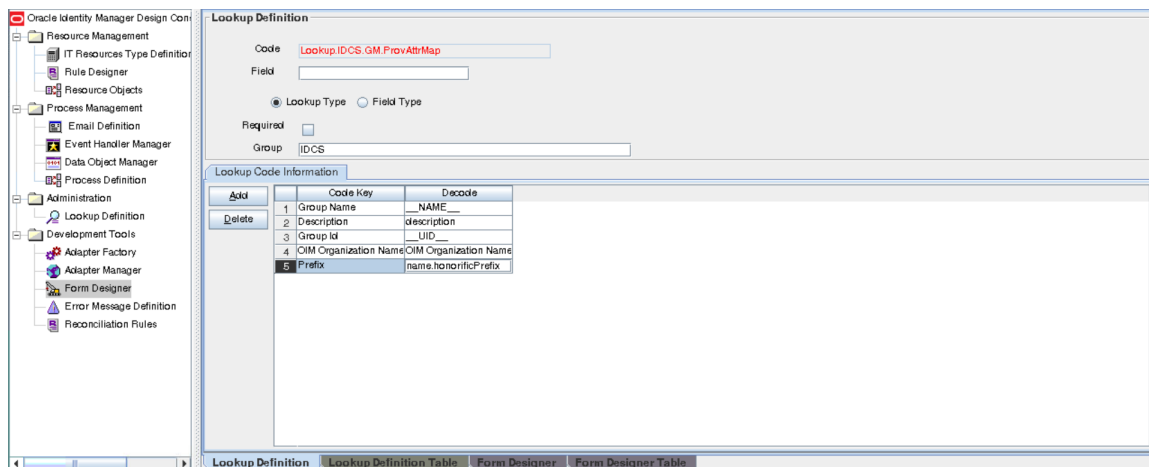
To create an entry for the newly added attribute in the lookup definition that holds attribute mappings for provisioning:

1. Expand **Administration**.

2. Double-click **Lookup Definition**.
3. Search for and open the **Lookup.IDCS.GM.ProvAttrMap** lookup definition.
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 figure shows the entry added to the lookup definition:

Figure 6-6 Entry Added to the Lookup Definition



6.2.3 Creating a Task to Enable Update Operations

Create a task to enable updates on the new 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 group attribute as follows:

See Also:

Developing Provisioning Processes in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*

1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open the **IDCS Group** process definition.
3. Click **Add**.
4. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:
 - Conditional
 - Allow Cancellation while Pending

- Allow Multiple Instances
5. Click the Save icon. The following figure shows the new task added to the process definition:

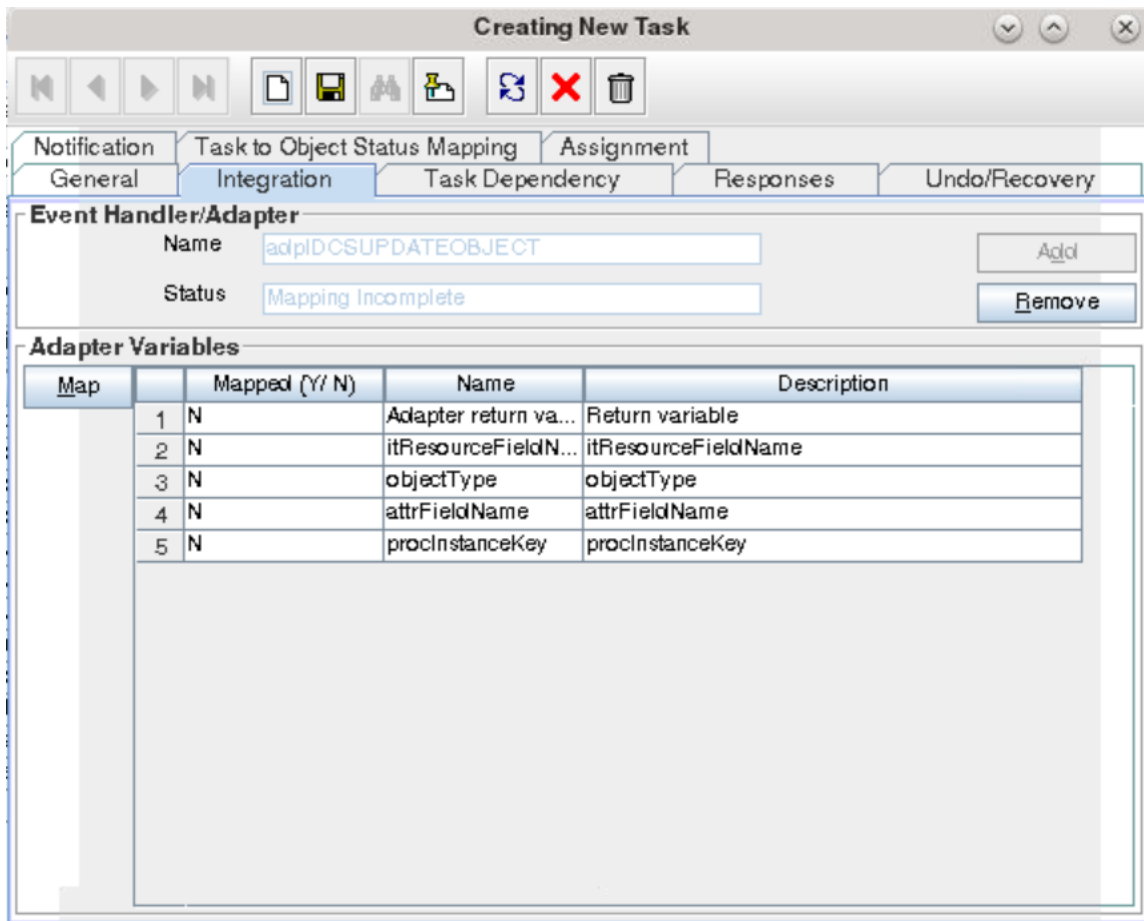
Figure 6-7 New Task Added to the Process Definition

The screenshot shows a dialog box titled "Creating New Task" with several tabs: Notification, Task to Object Status Mapping, Assignment, General, Integration, Task Dependency, Responses, and Undo/Recovery. The "General" tab is active. It contains fields for "Task Name" (Prefix Updated) and "Task Description" (Prefix Updated). To the right is a "Duration" section with input boxes for "Days", "Hours", and "Minutes". Below is a "Task Properties" section with various checkboxes: "Conditional" (unchecked), "Required for Completion" (checked), "Constant Duration" (unchecked), "Disable Manual Insert" (unchecked), "Allow Cancellation while Pending" (checked), "Allow Multiple Instances" (unchecked), "Retry Period in Minutes" (unchecked), "Retry Count" (checked), and "Off-line" (unchecked). There are also dropdown menus for "Task Effect" (set to "No Effect"), "Child Table", and "Trigger Type", along with a "Clear" button.

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 figure shows the list of adapter variables:

Figure 6-8 List of Adapter Variables



7. In the Adapter Variables region, click the **ParentFormProcessInstanceKey** variable.
8. In the dialog box that is displayed, create the following mapping:
 - **Variable Name:** ParentFormProcessInstanceKey
 - **Map To:** Process Data
 - **Qualifier:** Process Instance
9. Click **Save** and close the dialog box.
10. 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

Variable	Map To	Qualifier	Literal Value
itResourceFieldName	Literal	String	UD_IDCS_GRP_SERVER
attributeFieldName	Literal	String	<NAME_OF_THE_NEW_GROUP_ATTRIBUTE>

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

6.2.4 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*.

6.3 Configuring Transformation and Validation of Data

Configure transformation and validation of user account data by writing Groovy script logic while creating your application.

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

Similarly, you can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

To configure transformation or validation of user account data, you must write Groovy scripts while creating your application. For more information about writing Groovy script-based validation and transformation logic, see *Validation and Transformation of*

Provisioning and Reconciliation Attributes of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

6.4 Configuring Action Scripts

You can configure **Action Scripts** by writing your own Groovy scripts while creating your application.

These scripts can be configured to run before or after the create, update, or delete an account provisioning operations. For example, you can configure a script to run before every user creation operation.

For information on adding or editing action scripts, see Updating the Provisioning Configuration in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

6.5 Configuring the Connector for Multiple Installations of the Target System

You must create copies of configurations of your base application to configure it 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, including independent schema for each. The company has recently installed Oracle Identity Governance, and they want to configure it to link all the installations of the target system.

To meet the requirement posed by such a scenario, you must clone your application which copies all configurations of the base application into the cloned application. For more information about cloning applications, see Cloning Applications in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

7

Upgrading the Identity Cloud Service Connector

If you have already deployed the 11.1.1.5.0 version of the Identity Cloud Service connector, then you can upgrade the connector to version 12.2.1.3.0 by uploading the new connector JAR files to the Oracle Identity Governance database.

Note:

Before you perform the upgrade procedure:

- It is strongly recommended that you create a backup of the Oracle Identity Governance database. Refer to the database documentation for information about creating a backup.
- As a best practice, perform the upgrade procedure in a test environment initially.

The following sections discuss the procedure to upgrade the connector:

- [Preupgrade Steps](#)
- [Upgrade Steps](#)
- [Postupgrade Steps](#)

See Also:

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

7.1 Preupgrade Steps

Preupgrade steps for the connector involves performing a reconciliation run to fetch records from the target system, defining the source connector in Oracle Identity Manager, creating copies of the connector if you want to configure it for multiple installations of the target system, and disabling all the scheduled jobs.

Perform the following preupgrade steps:

1. Perform a reconciliation run to fetch all latest updates to Oracle Identity Manager.
2. Perform the preupgrade procedure documented in Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
3. Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update

the Deployment Manager XML file with all customization changes made to the connector. See Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information.

4. If required, create the connector XML file for a clone of the source connector.
5. Disable all the scheduled jobs.

7.2 Upgrade Steps

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

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

- Staging Environment

Perform the upgrade procedure by using the wizard mode.

 **Note:**

Do not upgrade IT resource type definition. In order to retain the default setting, you must map the IT resource definition to "None".

- Production Environment

Perform the upgrade procedure by using the silent mode.

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

7.3 Postupgrade Steps

Postupgrade steps involve uploading new connector JARs, configuring the upgraded IT resource of the source connector, updating the Connector Server JARs, and deleting duplicate entries for lookup definitions.

Perform the following procedure:

1. Upload new connector JARs as follows:
 - a. Run the Upload JARs utility (`$ORACLE_HOME/bin/UploadJars.sh`) for uploading connector JARs.
 - b. Upload `bundle/org.identityconnectors.genericscim-12.3.0.jar` as ICFBundle.
2. Replicate all changes made to the Form Designer of the Design Console in a new UI form as follows:
 - a. Log in to Oracle Identity System Administration.
 - b. Create and activate a sandbox.
 - c. Create a new UI form to view the upgraded fields.
 - d. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form (created in step 2.c) and then save the application instance.

- e. Publish the sandbox.
3. Configure the upgraded IT resource of the source connector.
4. If you are using the Connector Server, update the Connector Server JARs as follows:
 - a. Navigate to the bundles directory in your Connector Server directory, and replace the existing connector server bundle JAR with the new JAR.
 - b. Restart the Connector Server.
5. After upgrading the connector, a duplicate entry is created in the Lookup.IDCS.Configuration lookup definition for the `customPayload` parameter. Log in to Oracle Identity Manager Design Console and delete the following duplicate entry:

Code Key	Decode
customPayload	<pre> 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__)\\$"}]}]}] as String[] </pre>

6. After a successful upgrade operation, if any of the previous connector artifacts are retained, then log in to Oracle Identity Manager Design Console and delete duplicate entries.
7. If you want to delete users that are associated with one or more entities (Groups or Applications) in Identity Cloud Service, then update the `relURLs` advanced settings parameter. For detailed instructions, see the `relURLs` parameter description in [Table 3-2](#).
8. Perform either full reconciliation or incremental reconciliation.

This ensures that records created or modified since the last reconciliation run are fetched into Oracle Identity Governance. From the next reconciliation run onward, the reconciliation engine automatically enters a value for the Latest Token attribute.

See Also:

- [Configuring Oracle Identity Governance](#) for information about creating, activating, or publishing a sandbox and creating a new UI form
- Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about deploying the Connector Server
- [Configuring Reconciliation](#) for more information about performing full or incremental reconciliation

8

Troubleshooting the Identity Cloud Service Connector

This chapter provides solutions to the commonly encountered issues associated with the Identity Cloud Service connector.

Table 8-1 Troubleshooting the Identity Cloud Service Connector

Problem	Solution
<p>If you try to delete a user that is associated with one or more entities (Groups or Applications) in Identity Cloud Service, the following error message appears:</p> <pre>Unable to delete User <i>USER_NAME</i> since it is currently referenced by Group <i>GROUP_NAME</i>. You must either first remove these references and then delete the User or force delete the User which will automatically remove all these references and then delete the User.</pre>	<p>The target system does not allow you to delete a user that is associated with one or more entities. To delete the user, you must first update the <code>relURLs</code> advanced settings parameter.</p> <p>To do so, add the <code>"__ACCOUNT__.DeleteOp=/Users/\$(__ACCOUNT__.__UID__)\$?forceDelete=true"</code> value at the end of the <code>relURLs</code> entry.</p> <p>The updated sample value is:</p> <pre>"__ACCOUNT__.password.UpdateOp=/Users/\$(__ACCOUNT__.__UID__\$)", "__ACCOUNT___.DeleteOp=/Users/\$(__ACCOUNT__.__UID__\$)?forceDelete=true".</pre> <p>For details on the <code>relURLs</code> parameter, see Advanced Settings Parameters.</p>
<p>While creating an AOB application, if you click Test Connection to verify connection with the target system, the following error message appears:</p> <pre>Test connection failed. Internal Server Error. Error connecting to application <i>APPLICATION_NAME</i>: Error occurred while executing a POST REST call on the target.</pre>	<p>If you are using Oracle Identity Governance 12c (12.2.1.3.0), ensure to download and apply patches 26616250 and 25323654 from My Oracle Support as mentioned in Certified Components.</p> <p>If you do not apply these patches, Oracle Identity Governance fails to test the connection with the target system.</p>

9

Known Issues and Workarounds for the Identity Cloud Service Connector

This is a known issue associated with this release of the connector. It is a limitation with the target system.

Hashed Password Is Not Validated Against Password Policy in Identity Cloud Service

If you enable password hashing and try to provision an account, the target system does not validate the password against password policy. Thus, you are allowed to create a password that does not conform to the password criteria in Identity Cloud Service.

Workaround:

There is no workaround available for this issue.

A

Files and Directories in the Identity Cloud Service Connector Package

These are the files and directories on the connector installation package that comprise the Identity Cloud Service connector.

Table A-1 Files and Directories in the IDCS Connector Package

File in the Installation Media Directory	Description
bundle/ org.identityconnectors.genericscim-12.3.0.jar	This JAR is the ICF connector bundle.
configuration/IDCS-CI.xml	This file is used for installing a CI-based connector. This XML file contains configuration information that is used by the Connector Installer during connector installation.
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 Governance database. Note: A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
xml/IDCS-ConnectorConfig.xml	This XML file contains definitions for the following connector objects: <ul style="list-style-type: none">• Resource objects• IT resource types• IT resource instance• Process forms• Process tasks and adapters• Process definition• Prepopulate rules• Lookup definitions• Reconciliation rules• Scheduled jobs Note: This file is applicable only for a CI-based connector.
xml/IDCS-pre-config.xml	This XML file contains definitions for the connector objects associated with any non-User objects such as Group Names.

Table A-1 (Cont.) Files and Directories in the IDCS Connector Package

File in the Installation Media Directory	Description
xml/IDCS-target-template.xml	This file contains definitions for the connector objects required for creating a Target application. It includes certain details required to connect Oracle Identity Governance with the target system. It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.