

Oracle® Identity Governance

Configuring the Oracle Cerner Application



Release 12.2.1.3.0

F81231-01

June 2023

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 Cerner Application, Release 12.2.1.3.0

F81231-01

Copyright © 2023, Oracle and/or its affiliates.

Primary Authors: (Maya Chakrapani), (primary author)

Contributing Authors: (contributing author), (contributing author)

Contributors: (contributor), (contributor)

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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," "commercial computer software documentation," or "limited rights data" 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®, Java, and MySQL 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

1 Introduction to the Connector

1.1	Certified Components	1-1
1.2	Certified Languages	1-2
1.3	Usage Recommendation	1-3
1.4	Supported Connector Operations	1-3
1.5	Connector Architecture	1-3
1.6	Use Cases Supported by the Connector	1-5
1.7	Connector Features	1-6
1.7.1	User Provisioning	1-6
1.7.2	Full Reconciliation	1-6
1.7.3	Limited Reconciliation	1-7
1.7.4	Support for the Connector Server	1-7
1.7.5	Support for Cloning Applications and Creating Instance Applications	1-7
1.7.6	Transformation and Validation of Account Data	1-8

2 Creating an Application by Using the Connector

2.1	Prerequisites for Creating an Application By Using the Connector	2-1
2.1.1	Prerequisites Required from Target System to Perform Connector Operations	2-1
2.1.2	Downloading the Connector Installation Package	2-1
2.2	Process Flow for Creating an Application By Using the Connector	2-2
2.3	Creating an Application By Using the Cerner Cloud Connector	2-3

3 Configuring the Connector

3.1	Basic Configuration Parameters	3-1
3.2	Advanced Settings Parameters	3-2
3.3	Attribute Mappings	3-4
3.3.1	Attribute Mappings for the Target Application	3-4
3.4	Correlation Rules	3-9
3.4.1	Correlation Rules for the Target Application	3-10
3.5	Reconciliation Jobs	3-11

4 Performing Post configuration Tasks for the 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	4-1
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	4-2
4.3	Managing Logging for the Connector	4-3
4.3.1	Understanding Logging on the Connector Server	4-3
4.3.2	Enabling Logging for the Connector Server	4-4
4.3.3	Understanding Log Levels	4-4
4.3.4	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

5 Using the Connector

5.1	Configuring Reconciliation	5-1
5.1.1	Performing Full Reconciliation	5-1
5.1.2	Performing Limited Reconciliation	5-1
5.2	Configuring Reconciliation Jobs	5-2
5.3	Configuring Provisioning	5-3
5.3.1	Guidelines on Performing Provisioning Operations	5-3
5.3.2	Performing Provisioning Operations	5-4

6 Extending the Functionality of the Connector

6.1	Configuring Transformation and Validation of Data	6-1
6.2	Configuring Action Scripts	6-1
6.3	Configuring the Connector for Multiple Installations of the Target System	6-2

7 Known Issues

8 Files and Directories in the Connector Installation Package

Index

List of Figures

1-1	Cerner Connector Architecture	1-4
2-1	Overall Flow of the Process for Creating an Application By Using the Connector	2-3
3-1	Default Attribute Mappings for Cerner User Account	3-6
3-2	Default Attribute Mapping for Cerner Organization	3-7
3-3	Default Attribute Mapping for Personal Group	3-8
3-4	Default Organization Group entitlement mapping	3-8
3-5	Default Attribute Mapping for Cerner Personal Alias	3-9
3-6	Simple Correlation Rule for Cerner Target Application	3-10
3-7	Predefined Situations and Responses for a Cerner Target Application	3-11

List of Tables

1-1	Certified Components	1-2
1-2	Supported Connector Features Matrix	1-6
3-1	Parameters in the Basic Configuration	3-1
3-2	Advanced Settings Parameters	3-3
3-3	Default Attributes for Cerner Target Application	3-5
3-4	Default Attribute Mappings for Organization	3-7
3-5	Default Attribute Mappings for Personal Group	3-7
3-6	Default Attribute Mappings for Organization Group	3-8
3-7	Default Attribute Mappings for Personal Alias	3-9
3-8	Predefined Identity Correlation Rule for a Cerner Connector	3-10
3-9	Predefined Situations and Responses for a Cerner Target Application	3-11
3-10	Parameters of the Cerner Full User Reconciliation Job	3-12
3-11	Parameters of the Reconciliation Jobs for Entitlements	3-12
4-1	Log Levels and ODL Message Type:Level Combinations	4-5
4-2	Parameters of the IT Resource for the Cerner Connector Server	4-6
8-1	Files and Directories in the Cerner Connector Installation Package	8-1

1

Introduction to the 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 Cerner Connector lets you create and onboard Cerner 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**.

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.

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

- [Certified Components](#)
- [Certified Languages](#)
- [Usage Recommendation](#)
- [Supported Connector Operations](#)
- [Connector Architecture](#)
- [Use Cases Supported by the Connector](#)
- [Connector Features](#)

1.1 Certified Components

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

Table 1-1 Certified Components

Component	Requirement for AOB Application
Oracle Identity Governance or Oracle Identity Manager	You can use any one of the following releases: <ul style="list-style-type: none">• Oracle Identity Governance 12c PS4 (12.2.1.4.0) or later version
Oracle Identity Governance or Oracle Identity Manager JDK	JDK 1.8 and later
Target systems	Cerner Millennium, Security provisioning engine version 7.0.0
Connector Server	11.1.2.1.0 or 12.2.1.3.0
Connector Server JDK	JDK 1.8 and later

1.2 Certified Languages

These are the languages that the connector supports.

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- French (Canadian)
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak

- Spanish
- Swedish
- Thai
- Turkish

1.3 Usage Recommendation

If you are using Oracle Identity Governance 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.

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	
Create user	Yes
Update user	Yes
Enable user	Yes
Disable user	Yes
Delete user	No
Reset Password	Yes
Entitlement Grant Management	
Assign and Revoke Personal Group	Yes
Assign and Revoke Organization Group	Yes
Assign and Revoke Personal Alias	Yes
Assign and Revoke Organization	Yes

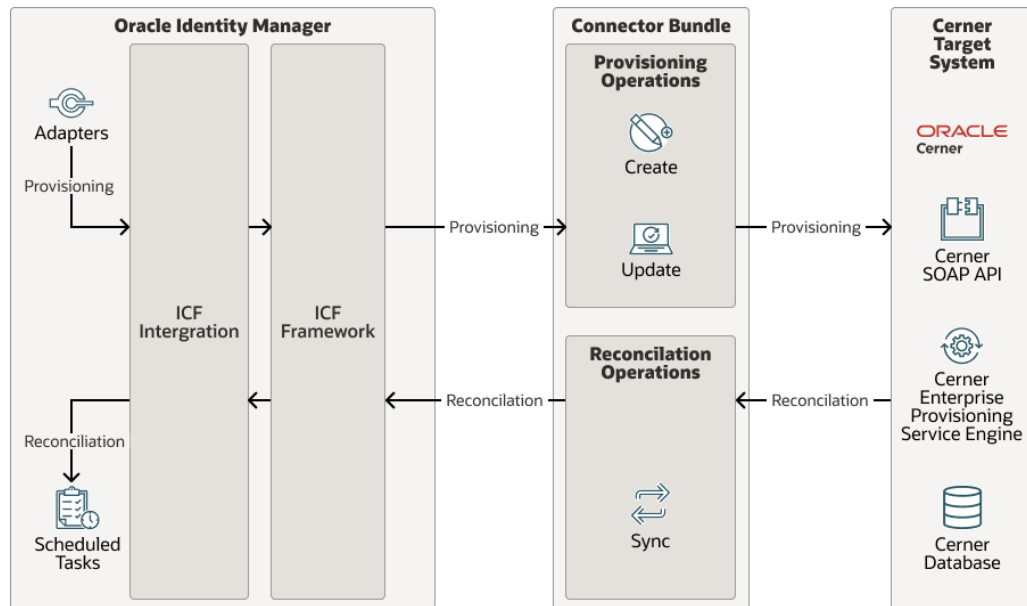
1.5 Connector Architecture

The Cerner is implemented by using the Identity Connector Framework (ICF).

The ICF is a component that is required in order to use Identity Connector. ICF 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, buffering, time outs, and filtering. ICF is distributed together with Oracle Identity Governance. Therefore, you do not need to configure or modify ICF.

[Figure 1-1](#) shows the architecture of the Cerner.

Figure 1-1 Cerner Connector Architecture



The connector is configured to run in one of the following modes:

- Account management

Account management is also known as target resource management. In this mode, the target system is used as a target resource and the connector enables the following operations:

- Provisioning

Provisioning involves creating, updating, or disabling users on the target system through Oracle Identity Governance. During provisioning, the Adapters invoke ICF operation, ICF in turn invokes create operation on the Cerner Identity Connector Bundle and then the bundle calls the target system API (Cerner API) for provisioning operations. The API on the target system accepts provisioning data from the bundle, carries out the required operation on the target system, and returns the response from the target system back to the bundle, which passes it to the adapters.

- Target resource reconciliation

During reconciliation, a scheduled task invokes an ICF operation. ICF in turn invokes a search operation on the Cerner Identity Connector Bundle and then the bundle calls Cerner API for Reconciliation operation. The API extracts user records that match the reconciliation criteria and hands them over through the bundle and ICF back to the scheduled task, which brings the records to Oracle Identity Governance.

Each record fetched from the target system is compared with Cerner resources that are already provisioned to OIM Users. If a match is found, then the update made to the Cerner record from the target system is copied to the Cerner resource in Oracle Identity Governance. If no match is found, then the Name of the record is compared with the User Login of each OIM User. If a match is found, then data in the target system record is used to provision a Cerner resource to the OIM User.

The Cerner Identity Connector Bundle communicates with the Cerner API using the HTTP protocol. The Cerner API provides programmatic access to Cerner through

Cerner SOAP API endpoint. Apps can use the SOAP API to perform create, read, and update, operations on directory data and directory objects, such as users, personnel groups, Organization, Organization Groups and Personal alias.



See Also:

[Understanding the Identity Connector Framework](#) in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance for more information about ICF.

1.6 Use Cases Supported by the Connector

The Cerner is used to integrate Oracle Identity Governance with Cerner to ensure that all Cerner accounts are created, updated, and deactivated on an integrated cycle with the rest of the identity-aware applications in your enterprise. The Cerner supports management of identities for Cloud Identity, Synchronized Identity, and Federated Identity models of Cerner. In a typical IT scenario, an organization using Oracle Identity Governance wants to manage accounts, groups, roles across Cerner Cloud Service. The following are some of the most common scenarios in which this connector can be used:

- **Cerner User Management:**

An organization using Cerner wants to integrate with Oracle Identity Governance to manage identities. The organization wants to manage its user identities by creating them in the target system using Oracle Identity Governance. The organization also wants to synchronize user identity changes performed directly in the target system with Oracle Identity Governance. In such a scenario, a quick and an easy way is to install the Cerner and configure it with your target system by providing connection information.

To create a new user in the target system, fill in and submit the OIM process form to trigger the provisioning operation. The connector executes the CreateOp operation against your target system and the user is created on successful execution of the operation. Similarly, operations like delete and update can be performed.

To search or retrieve the user identities, you must run a scheduled task from Oracle Identity Governance. The connector will run the corresponding SearchOp against the user identities in the target system and fetch all the changes to Oracle Identity Governance.

- **Cerner Group Management:**

An organization has a number of Cerner Groups allowing its users to set up new Cerner, manage memberships, and delete groups. The organization now wants to know the list of groups that have not been recently accessed or who have inactive members. In such a scenario, you can use the Cerner to highlight the usage trend for groups. By using the Cerner, you can leverage the reporting capabilities of Oracle Identity Governance to track any operations (such as create, update, delete) performed on groups.

- **Cerner Personal Alias Management**

An organization has a many numbers of users and we can set up by adding or removing personal alias. By using the Cerner connector, you can leverage the reporting capabilities of Oracle Identity Governance to track any operations (such as update, delete) performed on personal Alias and changes made in their alias memberships.

1.7 Connector Features

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

[Table 1-2](#) provides the list of features supported by the AOB application.

Table 1-2 Supported Connector Features Matrix

Feature	AOB Application
User provisioning	Yes
Full reconciliation	Yes
Limited reconciliation	Yes
Use connector server	Yes
Clone applications or create new application instances	Yes
Transformation and validation of account data	Yes
Reconcile user account status	Yes
Perform connector operations in multiple domains	Yes
Test connection	Yes
Reset password	Yes
Organization Group assignment	Yes
Personal Group Assignment	Yes
Personal Alias assignment	Yes
Organization Assignment	Yes

The following topics provide more information on the features of the AOB application:

- [User Provisioning](#)
- [Full Reconciliation](#)
- [Limited Reconciliation](#)
- [Support for the Connector Server](#)
- [Support for Cloning Applications and Creating Instance Applications](#)
- [Transformation and Validation of Account Data](#)

1.7.1 User Provisioning

User provisioning involves creating or modifying the account data on the target system through Oracle Identity Governance.

For more information about it, see [Performing Provisioning Operations](#).

1.7.2 Full Reconciliation

You can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Governance.

**Note:**

The connector cannot support incremental reconciliation because the target system does not provide a way for tracking the time at which account data is created or modified.

For more information, see [Performing Full Reconciliation](#).

1.7.3 Limited Reconciliation

You can reconcile records from the target system based on a specified filter criterion. To limit or filter the records that are fetched into Oracle Identity Governance during a reconciliation run, you can specify the subset of added or modified target system records that must be reconciled.

You can set a reconciliation filter as the value of the Filter Suffix attribute of the user reconciliation scheduled job. The Filter Suffix attribute helps you to assign filters to the API based on which you get a filtered response from the target system.

For more information, see [Performing Limited Reconciliation](#).

1.7.4 Support for the Connector Server

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

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

See Also:

[Using an Identity Connector Server](#) in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about installing and configuring connector server and running the connector server

1.7.5 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 an Instance Application](#) in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.7.6 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*.

2

Creating an Application by Using the Connector

Prerequisite: Ensure that both OIG and Cerner Millennium are on the same network domain.

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

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

2.1 Prerequisites for Creating an Application By Using the Connector

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

- [Prerequisites Required from Target System to Perform Connector Operations](#)
- [Downloading the Connector Installation Package](#)

2.1.1 Prerequisites Required from Target System to Perform Connector Operations

You require the following inputs:

- Cerner Instance URL
- Millennium Target ID



Note:

You require access to connect to **Cerner Enterprise Provisioning Service Engine**, and perform provisioning operations. Obtain the Millennium Target ID from the Cerner system, for example: `millennium_<id>`.

2.1.2 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:

Navigate to the OTN website at <http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html>.

Click OTN License Agreement and read the license agreement.

Select the Accept License Agreement option.

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

Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.

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`.

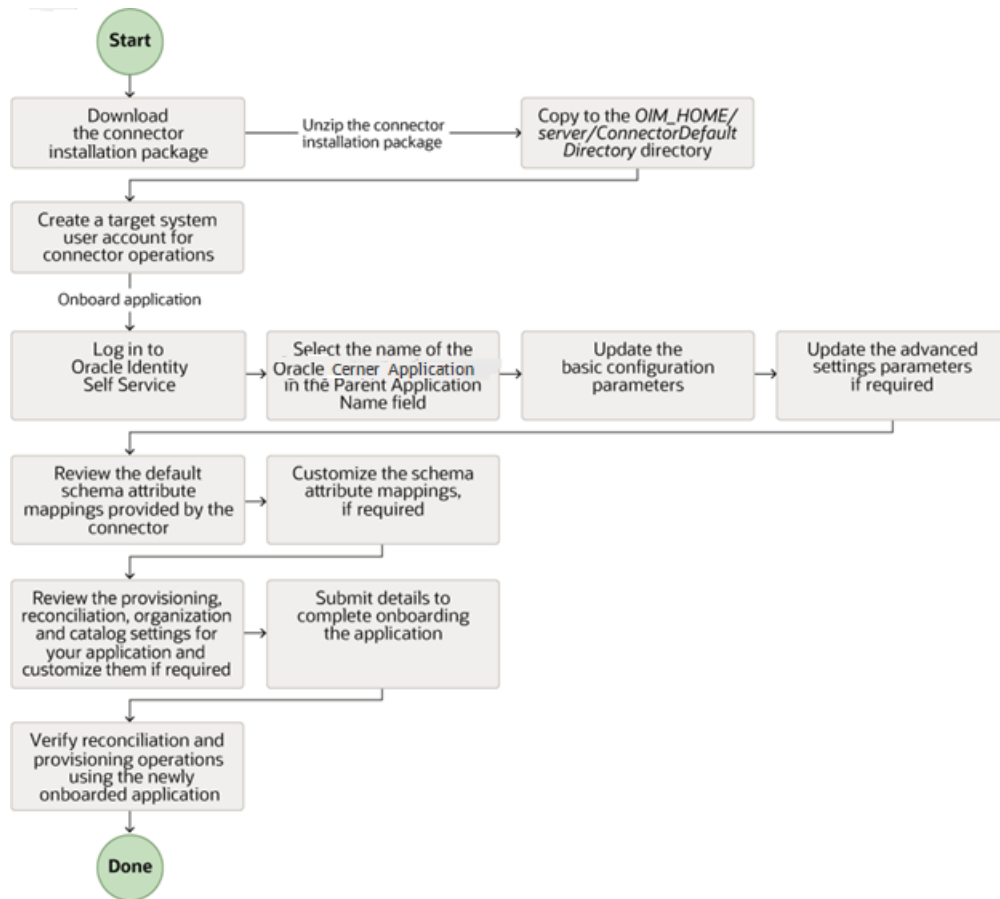
Copy the `CONNECTOR_NAME-RELEASE_NUMBER` directory to the `OIG_HOME/server/ConnectorDefaultDirectory` directory.

2.2 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



2.3 Creating an Application By Using the Cerner Cloud 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 regarding each step 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 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 Connector

While creating a target application, you must configure connection-related parameters that the connector uses to connect to 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](#)
- [Reconciliation Jobs](#)

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to a Cerner application.



Note:

Unless specified, do not modify entries in the below table.

Table 3-1 Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
targetID	Yes	Enter the targetID (unique string) issued by the Cerner team. Sample value :millenium123
host	Yes	Enter the host name of the machine hosting your Cerner target system. This is a mandatory attribute while creating an application. Sample value : api.Cerner.net
port	Yes	Enter the port number at which the target system is listening. Sample value : 8080
Connector Server Name	No	This field is blank. If you are using this connector with the Java Connector Server, then provide the name of Connector Server IT Resource here.
proxyUsername	No	Enter the name of the proxy Username used to connect to an external target.
proxyHost	No	Enter the name of the proxy host used to connect to an external target.

Table 3-1 (Cont.) Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
proxyPassword	No	Enter the password of the proxy user ID of the target system user account that Oracle Identity Governance uses to connect to the target system.
proxyPort	No	Enter the proxy port number.
sslEnabled	No	If the target system requires SSL connectivity, then set the value of this parameter to true. Otherwise set the value to false. Default value: false

3.2 Advanced Settings Parameters


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

 **Note:**


- Unless specified, do not modify entries in the below table.
- All parameters in the below table are mandatory.

Table 3-2 Advanced Settings Parameters

Parameter	Mandatory?	Description
Bundle Version	No	This entry holds the version of the connector bundle. Default value: 12.3.0
Connector Name	No	This entry holds the name of the connector. Default value: <code>org.identityconnectors.cerner.CernerConnector</code>
Bundle Name	No	This entry holds the name of the connector bundle. Default value: <code>org.identityconnectors.cerner</code>
version	Yes	This parameter holds the version of Cerner API you are using. Sample value: 1.0

 **No
te:**

Do not modify this entry.

 **No
te:**

Do not modify this entry.

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
pageCount	Yes	This parameter holds the number of records in each batch that must be fetched from the target system during a reconciliation run. While specifying a value for pageCount, ensure to specify between 1 and 999 Sample value: 100
endpointURL	Yes	This entry holds the relative URL of every object class supported by this connector and the connector operations that can be performed on these object classes. This is a mandatory attribute while creating an application. Sample value: <code>/security-provisioning/ msol.ip.devcenter.net/ ProvisioningServlet</code>

3.3 Attribute Mappings

The following topic provides the attribute mappings details.

- [Attribute Mappings for the Target Application](#)

3.3.1 Attribute Mappings for the Target Application

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.

[Table 3-3](#) lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and Cerner target application 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](#) [Creating a](#)

[Target Application](#) in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-3 Default Attributes for Cerner Target Application

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Cerner ID	__UID__	String	No	No	Yes	Yes	No
User Name	__NAME__	String	No	Yes	Yes	No	Not applicable
Password	__PASSWORD__	String	No	Yes	No	No	Not applicable
First Name	firstName	String	No	Yes	Yes	No	Not applicable
Last Name	lastName	String	No	Yes	Yes	No	Not applicable
Middle Name	middleName	String	No	Yes	Yes	No	Not applicable
Suffix	suffix	String	No	Yes	Yes	No	Not applicable
Title	title	String	No	Yes	Yes	No	Not applicable
PhysicianInd	physicianInd	String	No	Yes	Yes	No	Not applicable
Gender	gender	String	No	Yes	Yes	No	Not applicable
DirectoryIndicator	directoryIndicator	String	No	Yes	Yes	No	Not applicable
LogicalDomain	logicalDomain	String	No	Yes	Yes	No	Not applicable
Birth Date	birthdate	Date	No	Yes	Yes	No	Not applicable
Begin Effective DateTime	beginEffectiveDateTime	Date	No	Yes	Yes	No	Not applicable
End Effective DateTime	endEffectiveDateTime	Date	No	Yes	Yes	No	Not applicable
Position	position	String	No	Yes	Yes	No	Not applicable
Status	__ENABLE__	String	No	No	Yes	No	Not applicable
Server		Long	Yes	No	Yes	Yes	No

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

Figure 3-1 Default Attribute Mappings for Cerner 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		
Select a value	Cerner ID	__UID__	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	User Name	__NAME__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	Password	__PASSWORD__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	First Name	firstName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	Last Name	lastName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	Middle Name	middleName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	Suffix	suffix	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	Title	title	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	PhysicianInd	physicianInd	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	Gender	gender	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	DirectoryIndicat	directoryIndicator	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	LogicalDomain	logicalDomain	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	Birth Date	birthdate	Date	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	Begin Effective I	beginEffectiveDateTime	Date	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	End EffectiveDat	endEffectiveDateTime	Date	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	Position	position	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	Status	__ENABLE__	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮
Select a value	Server		Long	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮

Cerner Organization Entitlement

Table 3-4 lists the attribute mappings for Organization between the process form fields in Oracle Identity Governance and Cerner target application 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.

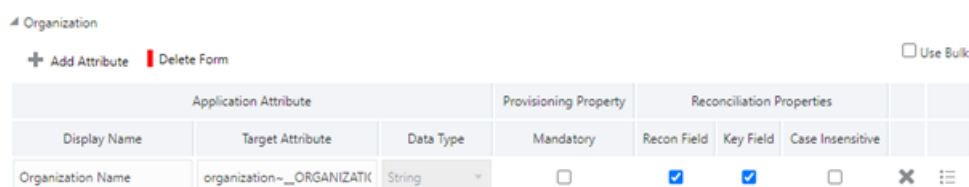
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in [Creating a Target Application](#) in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-4 Default Attribute Mappings for Organization

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Organization Name	organization~__ORGANIZATION__~or organizationName	String	No	Yes	Yes	No

Figure 3-2 shows the default Organization entitlement mapping.

Figure 3-2 Default Attribute Mapping for Cerner Organization



Cerner Personal Group Entitlement

Table 3-5 lists the attribute mappings for Personal Group between the process form fields in Oracle Identity Governance and Cerner target application 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](#) in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-5 Default Attribute Mappings for Personal Group

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Personal Group Name	personnelGroup~__PERSONALGROUP__~personnel GroupName	String	No	Yes	Yes	No

Figure 3-3 shows the default Personal Group entitlement mapping.

Figure 3-3 Default Attribute Mapping for Personal Group

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Personal Group Name	personnelGroup~_PERSONN	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	✕	☰

Cerner Organization Group Entitlement

Table 3-6 lists the attribute mappings for Organization Group between the process form fields in Oracle Identity Governance and Cerner target application 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](#) in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-6 Default Attribute Mappings for Organization Group

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive ?
Organization Group Name	organizationGroup~__ORGANIZATION__~organizationGroupUpName	String	No	Yes	Yes	No

Figure 3-4 shows the default Organization Group entitlement mapping.

Figure 3-4 Default Organization Group entitlement mapping

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Organization Name	organization~_ORGANIZATI	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	✕	☰

Cerner Personal Alias Entitlement

Table 3-7 lists the attribute mappings for Personal Alias between the process form fields in Oracle Identity Governance and Cerner target application 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](#) in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-7 Default Attribute Mappings for Personal Alias

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
AliasID	alias~__ALIAS__~toPsolD	String	No	Yes	Yes	No
Alias Pool	alias~__ALIAS__~aliasPool	String	No	Yes	No	Not applicable
Alias Type	alias~__ALIAS__~type	String	No	Yes	No	Not applicable
Alias	alias~__ALIAS__~alias	String	No	Yes	Yes	No
BeginEffectiveDateTime	alias~__ALIAS__~beginEffectiveDateTime	Date	No	Yes	No	Not applicable
EndEffectiveDateTime	alias~__ALIAS__~endEffectiveDateTime	Date	No	Yes	No	No applicable

Figure 3-5 shows the default Personal Alias entitlement mapping.

Figure 3-5 Default Attribute Mapping for Cerner Personal Alias

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
AliasID	alias~__ALIAS__~toPsolD	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Alias Pool	alias~__ALIAS__~aliasPool	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Alias Type	alias~__ALIAS__~type	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Alias	alias~__ALIAS__~alias	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
BeginEffectiveDateTime	alias~__ALIAS__~beginEffectiv	Date	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EndEffectiveDateTime	alias~__ALIAS__~endEffective	Date	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

3.4 Correlation Rules

Learn about the predefined rules, responses and situations for Target applications. The connector uses these rules and responses for performing reconciliation.

- [Correlation Rules for the Target Application](#)

3.4.1 Correlation Rules for the Target Application

When you create a target application, the connector uses correlation rules to determine the identity to which Oracle Identity Governance must assign a resource.

Predefined Identity Correlation Rules

By default, the Cerner 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.

[Table 3-8](#) lists the default simple correlation rule for a Cerner connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see [Updating Identity Correlation Rules](#) in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-8 Predefined Identity Correlation Rule for a Cerner Connector

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 3-6 Simple Correlation Rule for Cerner Target Application

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"/>	<input type="button" value="X"/>

Predefined Situations and Responses

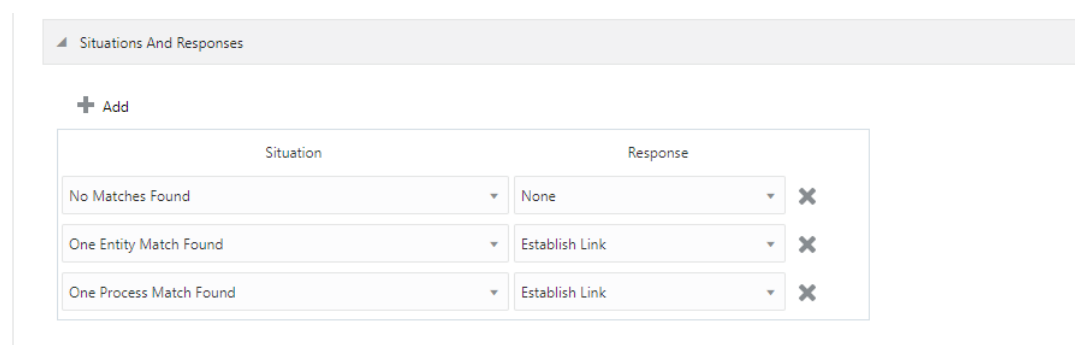
The Cerner connector provides a default set of situations and responses when you create a target application. These situations and responses specify the action that Oracle Identity Governance must take based on the result of a reconciliation event.

[Table 3-9](#) lists the default situations and responses for a Cerner Target application. 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 [Updating Situations and Responses](#) in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-9 Predefined Situations and Responses for a Cerner Target Application

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

Figure 3-7 shows the situations and responses for a Cerner that the connector provides by default.

Figure 3-7 Predefined Situations and Responses for a Cerner Target Application

3.5 Reconciliation Jobs

These are the reconciliation jobs that are automatically created in Oracle Identity Governance after you create the application.

User Reconciliation Jobs

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.

The following reconciliation jobs are available for reconciling user data:

- **Cerner Full User Reconciliation:** Use this reconciliation job to reconcile user data from a target applications.
- **Cerner Limited User Reconciliation:** Use this reconciliation job to reconcile records from the target system based on a specified filter criterion.

[Table 3-10](#) describes the parameters of the Cerner Full User Reconciliation job.

Table 3-10 Parameters of the Cerner Full User Reconciliation Job

Parameter	Description
Application name	Name of the AOB application with which the reconciliation job is associated. This value is the same as the value that you provided for the Application Name field while creating your target application. Do <i>not</i> change the default value.
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. Filter suffix for single user: 1. CernerID For more information about creating filters, see Performing Limited Reconciliation .
Object Type	This parameter holds the name of the object type for the reconciliation run. Default value: User Do <i>not</i> change the default value.
Scheduled Task Name	Name of the scheduled task used for reconciliation. Do <i>not</i> modify the value of this parameter.

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- Cerner Organization Group Lookup Reconciliation
- Cerner Personal Group Lookup Reconciliation
- Cerner Position Lookup Reconciliation
- Cerner Logical Domain Lookup Reconciliation
- Cerner Organization Lookup Reconciliation
- Cerner Personal Alias Pool Lookup Reconciliation
- Cerner Personal Alias Type Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-11 Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	Current AOB application name with which the reconciliation job is associated. Do <i>not</i> modify this value.
Code Key Attribute	Name of the connector attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: __UID__ Do <i>not</i> modify this value.
Decode Attribute	Name of the connector attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: __NAME__

Table 3-11 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Lookup Name	<p>Enter the name of the lookup definition in Oracle Identity Governance that must be populated with values fetched from the target system.</p> <p>Depending on the Reconciliation job that you are using, the default values are as follows:</p> <ul style="list-style-type: none"> For Cerner Organization Group Lookup Reconciliation : Lookup.Cerner.OrganizationGroup For Cerner Personal Group Lookup Reconciliation : Lookup.Cerner.PersonnelGroup For Cerner Position Lookup Reconciliation : Lookup.Cerner.Position For Cerner Logical Domain Lookup Reconciliation : Lookup.Cerner.LogicalDomain For Cerner Organization Lookup Reconciliation : Lookup.Cerner.Organization For Cerner Personal Alias Pool Lookup Reconciliation : Lookup.Cerner.AliasPool For Cerner Personal Alias Type Lookup Reconciliation : Lookup.Cerner.AliasType <p>If you create a copy of any of these lookup definitions, then enter the name of that new lookup definition as the value of the Lookup Name attribute.</p>
Object Type	<p>Enter the type of object you want to reconcile.</p> <p>Depending on the reconciliation job that you are using, the default values are as follows:</p> <ul style="list-style-type: none"> For Cerner Organization Group Lookup Reconciliation : __ORGANIZATIONGROUP__ For Cerner Personal Group Lookup Reconciliation : __PERSONNALGROUP__ For Cerner Position Lookup Reconciliation : __POSITION__ For Cerner Logical Domain Lookup Reconciliation : __LOGICALDOMAIN__ For Cerner Organization Lookup Reconciliation : __ORGANIZATION__ For Cerner Personal Alias Pool Lookup Reconciliation : __PERSONNELALIASPOOL__ For Cerner Personal Alias Type Lookup Reconciliation : __PERSONNELALIATYPE__

 **Note:**

Do not change the value of this parameter

4

Performing Post configuration Tasks for the Connector

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

1. [Configuring Oracle Identity Governance](#)
2. [Harvesting Entitlements and Sync Catalog](#)
3. [Managing Logging for the Connector](#)
4. [Configuring the IT Resource for the Connector Server](#)
5. [Localizing Field Labels in UI Forms](#)

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:

1. [Creating and Activating a Sandbox](#)
2. [Creating a New UI Form](#)
3. [Publishing a Sandbox](#)
4. [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 catalog:

1. Run the scheduled jobs for lookup field synchronization listed in [Reconciliation Jobs](#).
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from 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

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 Logging on the Connector Server](#)
- [Enabling Logging for the Connector Server](#)
- [Understanding Log Levels](#)
- [Enabling Logging](#)

4.3.1 Understanding Logging on the Connector Server

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

- Error

This level enables logging of information about errors that might allow connector server to continue running.

- WARNING

This level enables logging of information about potentially harmful situations.

- INFO

This level enables logging of messages that highlight the progress of the operation.

- FINE, FINER, FINEST

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

4.3.2 Enabling Logging for the Connector Server

Edit the `logging.properties` file located in the `CONNECTOR_SERVER_HOME/Conf` directory to enable logging.

To do so:

1. Navigate to the `CONNECTOR_SERVER_HOME /Conf` directory.
2. Open the `logging.properties` file in a text editor.
3. Edit the following entry by replacing `INFO` with the required level of logging:
 - `level=INFO`
4. Save and close the file.
5. Restart the connector server.

4.3.3 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
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

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

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

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

4.3.4 Enabling Logging

Perform this procedure to enable logging in Oracle WebLogic Server.

1. To enable logging in Oracle WebLogic Server: Edit the logging.xml file as follows:
 - a. Add the following blocks in the file:

```
<log_handler name='Cerner-handler'
level=' [LOG_LEVEL]'class='oracle.core.ojdl.logging.ODLHandlerFactory'>
  <property name='logreader:' value='off' /> <property name='path'
value=' [FILE_NAME]' /> <property name='format' value='ODL-Text' />
<property name='useThreadName' value='true' /> <property name='locale'
value='en' /> <property name='maxFileSize' value='5242880' /> <property
name='maxLogSize' value='52428800' /> <property name='encoding'
value='UTF-8' /></log_handler> Copy<logger name="
ORG.IDENTITYCONNECTORS.CERNER" level="[LOG_LEVEL]"
useParentHandlers="false"> <handler name="Cerner-handler" /> <handler
name="console-handler" /> </logger>
```

- b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. [Table 4-1](#) lists the supported message type and level combinations. Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages to be recorded. The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]**:

```
<log_handler name= 'Cerner -handler'
level='NOTIFICATION:1'class='oracle.core.ojdl.logging.ODLHandlerFactor
y'> <property name='logreader:' value='off' /> <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\serv
ers\oim_server1\logs\oim_server1-diagnostic-1.log' /> <property
name='format' value='ODL-Text' /> <property name='useThreadName'
value='true' /> <property name='locale' value='en' /> <property
name='maxFileSize' value='5242880' /> <property name='maxLogSize'
```

```
value='52428800' /> <property name='encoding' value='UTF-8' /></
log_handler> <logger name=" ORG.IDENTITYCONNECTORS.CERNER"
level="NOTIFICATION:1" useParentHandlers="false"> <handler
name="Cerner-handler" /> <handler name="console-handler" /></
logger>
```

2. 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.
3. Save and close the file.
4. Set the following environment variable to redirect the server logs to a file:
 - a. For Microsoft Windows: set WLS_REDIRECT_LOG= **FILENAME**
 - b. 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.
5. 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 Resources](#) of *Oracle Fusion Middleware Administering Oracle Identity Governance*. While creating the IT resource, ensure to select Connector Server from the IT Resource Type list. In addition, specify values for the parameters of IT resource for the Connector Server listed in [Table 4-2](#). For more information about searching for IT resources and updating its parameters, see [Managing IT Resources](#) in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

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

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. Sample value: HostName
Key	Enter the key for the Connector Server.
Port	Enter the number of the port at which the Connector Server is listening. Sample value: 8763
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. If the value is zero or if no value is specified, the timeout is unlimited. Sample value: 0 (recommended value)

Table 4-2 (Cont.) Parameters of the IT Resource for the Cerner Connector Server

Parameter	Description
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 [Configuring the Java Connector Server with SSL for OIG](#) in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

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 media.

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 (**oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip**) to the local computer.
5. Extract the contents of the archive, and open one of the following file in a text editor if you are using Oracle Identity Governance 12c (12.2.1.3.0) or later version:
SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf

 **Note:**

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

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:

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.userEO.UD_CERNER_USR_USER_NAME__c_description']"> <source>User
Name</source><target/> </trans-unit> <trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.CernerApp1.entity
.CernerApp1EO.UD_CERNER_USR_USER_NAME __c_LABEL"> <source>User
Name</source><target/><target/> </trans-unit>
```

- d. Open the resource file from the connector package, for example `Cerner_ja.properties`, and get the value of the attribute from the file, for example,

```
global.udf.UD_CERNER_USR_USER_NAME =
\u30E6\u30FC\u30B6\u30FC\u540D
```

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

```
</trans-unit><trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.userEO.UD_CERNER_USR_USER_NAME__c_description']"> <source>User
Name</source> <target/> </trans-unit> <trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.
CernerApp1.entity.CernerApp1EO.UD_CERNER_USR_USER_NAME
__c_LABEL"> <source>User Id</source> <target>
\u30E6\u30FC\u30B6\u30FC\u540D</target> <target/> </trans-unit>
```

- f. Repeat Steps 6.a through 6.d for all attributes of the process form.
- g. Save the file as `BizEditorBundle_LANG_CODE.xlf`. In this file name, replace `LANG_CODE` with the code of the language to which you are localizing. Sample file name: `BizEditorBundle_ja.xlf`.

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

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



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.

5

Using the Connector

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

- [Configuring Reconciliation](#)
- [Configuring Reconciliation Jobs](#)
- [Configuring Provisioning](#)

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 Reconciliation](#)
- [Performing Limited Reconciliation](#)

5.1.1 Performing Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Governance. After you create the application, you must first perform full reconciliation.

To perform a full reconciliation run, remove (delete) any value currently assigned to the Filter suffix parameters and run one of the reconciliation jobs listed in the [Reconciliation Jobs](#) section.

5.1.2 Performing Limited Reconciliation

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

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

This connector provides a Filter Suffix attribute (a scheduled task attribute) that allows you to use any of the attributes of the target system to filter target system records. You specify a value for the Filter Suffix attribute while configuring the user reconciliation scheduled job.

You can perform limited reconciliation by creating filters for the reconciliation module. The connector only supports CernerID filter. Below is the example for the filter:

Filter Suffix value: CernerID

Example: 6403170

In this example, the record whose CernerID is 6403170 is reconciled.

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**.

 **Note:**

If you are using OIG 12cPS4 with 2022OCTBP or later version, log in to Identity Console, click **Manage**, under **System Configuration**, 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:
 - a. **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.
 - b. **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

You can configure the provisioning operation for the Cerner connector.

This section provides information on the following topics:

- [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.

Provisioning attributes required to create user account

To create User provisioning operation, follow the following values as required:

- First Name: The user's first name.
- Last Name: The user's last name.
- User Name : The username of the account.
- DirectoryIndicator : The user directory of the user (required only if it is a LDAP user).
- LogicalDomain : The domain of the user (required only if target is enabled with domain).

Attributes required to be updated in the parent form

- First Name: The user's first name.
- Last Name: The user's last name.
- Middle Name: The user's middle name.
- User Name : The username of the account.
- Suffix : The suffix for the user.
- Title : The Job title of the user.
- PhysicianInd : The physician id for the physician user.
- Gender : The gender of the user.
- DirectoryIndicator : The user directory of the user.
- LogicalDomain : The domain of the user.
- Birth Date : The Birthdate of the user.
- Begin Effective DateTime : The joining date of the user.
- End EffectiveDateTime : The end date of the user account.
- Position : The user job position.
- Password: The password of the user.

5.3.2 Performing Provisioning Operations

To create a new user in the Identity Self Service by using the **Create User** page, you must provision or request for accounts on the **Accounts** tab of the **User Details** page.

To perform provisioning operations in Oracle Identity Governance, perform the following steps:

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, 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**.

6

Extending the Functionality of the Connector

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

This section discusses the following topics:

- [Configuring Transformation and Validation of Data](#)
- [Configuring Action Scripts](#)
- [Configuring the Connector for Multiple Installations of the Target System](#)

6.1 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*.

6.2 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*.

6.3 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

Known Issues

The following are the known issues associated with the Cerner connector.

We can create user with any previous begin date. Also user is not disabled from Cerner millennium target when the user's end effective date is over this is expected target behavior.

You cannot assign personal alias begin date as future dated. In case you try to add alias with future date it will not throw any error instead alias doesn't get added to user account in Cerner millennium target.

8

Files and Directories in the Connector Installation Package

These are the components of the connector installation package that comprise the Cerner connector.

Table 8-1 Files and Directories in the Cerner Connector Installation Package

File in the Installation Package	Description
/bundle/ org.identityconnectors.cerner-12.3. 0	This JAR is the ICF connector bundle.
configuration/Cerner-CI.xml	This XML file contains configuration information.
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 Oracle Identity 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/Cerner-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.
xml/Cerner-pre-config.xml	This XML file contains definitions for the connector objects associated with any non-User objects such as Groups, Organizations, and so on. Also, it contains definitions of Lookups and schedule tasks.

Glossary

Index