Oracle® Identity Governance

Configuring the Cerner Health Data Intelligence Connector

Release 12c (12.2.1.3.0)
G12814-05
September 2025

Oracle Identity Governance Configuring the Cerner Health Data Intelligence Connector, Release 12c (12.2.1.3.0)

G12814-05

Primary Author: Christina Sekar

Contributing Authors: Syam Kumar Battu, Brunda M

Contents

Index

List of Figures

List of Tables

1

Introduction to the Cerner Health Data Intelligence Connector

This chapter introduces the Oracle Health Data Intelligence Application connector (formerly known as Oracle Cerner Healtheintent Application connector).

Oracle Identity Governance is a centralized identity management solution that provides self-service, compliance, and provisioning 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 Cerner Health Data Intelligence Connector lets you create and onboard Oracle Cerner Health Data Intelligence 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:

1. Certified Components
2. Usage Recommendation
3. Certified Languages
4. Supported Connector Operations
5. Connector Architecture
6. Use Cases Supported by the Connector
7. Connector Features

Certified Components

These are the software components and their versions required for installing and using the Oracle Health data intelligence 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: • Oracle Identity Governance 12c PS4 (12.2.1.4.0) or later.
Oracle Identity Governance or Oracle Identity Manager JDK	JDK 1.8 and later
Target systems	Oracle Health data intelligence (aka) Oracle Cerner Healtheintent (Personnel Tool)
Target API version	V1
Connector Server	11.1.2.1.0 or 12.2.1.3.0
Connector Server JDK	JDK 1.8 and later

Usage Recommendation

If you are using Oracle Identity Governance 12*c* (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.

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

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
Disable user	No
Delete user	Yes
Reset Password	No
Grant Management	
Assign and Revoke Languages	Yes
Assign and Revoke Phone Numbers	Yes
Assign and Revoke Aliases	Yes
Assign and Revoke Personnel IDs	Yes
Assign and Revoke Emails	Yes
Entitlement Grant Management	
Assign and Revoke Personnel Group	Yes
Assign and Revoke Personnel Group Views(Recon only)	Yes
Assign and Revoke Organization	Yes

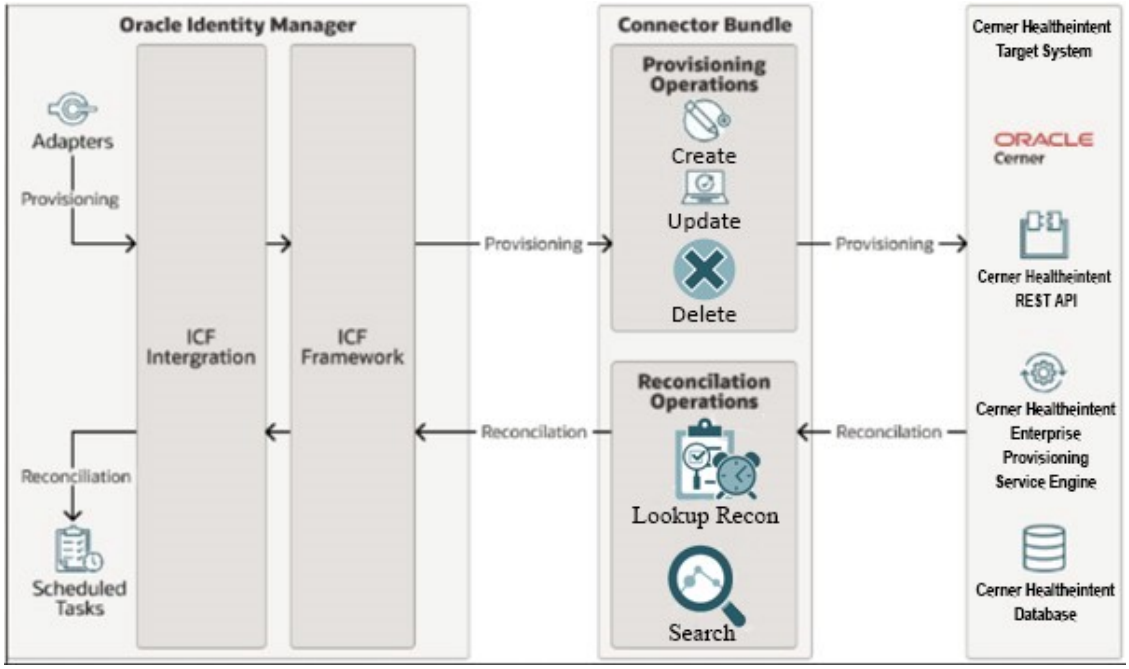
Connector Architecture

The Oracle Health data intelligence 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.

The following figure shows the architecture of the Oracle Health data intelligence.

Figure 1-1 Architecture Diagram of the Oracle Health Data Intelligence



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 deleting users on the target system through Oracle Identity Governance. During provisioning, the Adapters invoke ICF operation, ICF in turn invokes create operation on the Oracle Health data intelligence Identity Connector Bundle and then the bundle calls the target system API (Oracle Health data intelligence 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 Oracle Health data intelligence Identity Connector Bundle and then the bundle calls Oracle Health data intelligence 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 Oracle Health data intelligence resources that are already provisioned to OIM Users. If a match is found, then the update made to the Oracle Health data intelligence record from the target system is copied to the Oracle Health data intelligence 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 Oracle Health data intelligence resource to the OIM User.

The Oracle Health data intelligence Identity Connector Bundle communicates with the Oracle Health data intelligence API using the HTTP protocol. The Oracle Health data intelligence API provides programmatic access to Oracle Health data intelligence through Oracle Health data intelligence REST API endpoint. Apps can use the REST API to perform create, read, update or delete (CRUD) operations on directory data and directory objects, such as users.

See Also

Understanding the Identity Connector Framework in *Oracle Fusion Middleware Developing and Customizing Applications* for Oracle Identity Governance for more information about ICF.

Use Cases Supported by the Connector

The Oracle Health data intelligence is used to integrate Oracle Identity Governance with Oracle Health data intelligence to ensure that all Oracle Health data intelligence accounts are created, updated, deleted and deactivated on an integrated cycle with the rest of the identity-aware applications in your enterprise.

The Oracle Health data intelligence supports management of identities for Cloud Identity, Synchronized Identity, and Federated Identity models of Oracle Health data intelligence. In a typical IT scenario, an organization using Oracle Identity Governance wants to manage accounts, user association with personnel groups or Organization across Oracle Health data intelligence Cloud Service.

The following are some of the most common scenarios in which this connector can be used:

- **Oracle Health data intelligence User Management**:

An organization using Oracle Health data intelligence 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 Oracle Health data intelligence 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.

Connector Features

The features of the connector include support for connector server, user provisioning, full reconciliation, limited reconciliation and so on.

The following table provides the list of features supported by the AOB application.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application
User Provisioning	Yes
Full reconciliation	Yes
Limited (Filtered) reconciliation	Yes
Incremental reconciliation	Yes
Delete reconciliation	Yes
Use connector server	Yes
Transformation and validation of account data	Yes
Perform connector operations in multiple domains	Yes
Support for pagination	Yes
Test connection	Yes
Clone applications or create new application instances	Yes
Provide secure communication to the target system through SSL	Yes

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

1. User Provisioning
2. Full Reconciliation and Incremental Reconciliation
3. Limited (Filtered) Reconciliation
4. Support for the Connector Server
5. Transformation and Validation of Account Data
6. Support for Cloning Applications and Creating Instance Applications
7. Secure Communication to the Target System

User Provisioning

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

> **Note**
>
> For more information, see Performing Provisioning Operations.
>
> .

Full Reconciliation and Incremental Reconciliation

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

In incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Governance.

For more information, see Performing Full Reconciliation and Performing Incremental Reconciliation.

Limited (Filtered) 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.

For more information, see Performing Limited (Filtered) Reconciliation.

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

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*.

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*.

Secure Communication to the Target System

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

For more information, see Configuring SSL.

2

Creating an Application by Using the Connector

Learn about onboarding 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 Oracle Health Data Intelligence Connector

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

Prerequisites Required from Target System to Perform Connector Operations

You require the following inputs:

- Oracle Health Data Intelligence Instance URL
- Access Token with permission to perform the API operations

> **Note**
>
> You require access to connect to **CernerHealtheintent Provisioning** Service Engine, to perform provisioning operations. Obtain the Access Token from the Cerner system.

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.

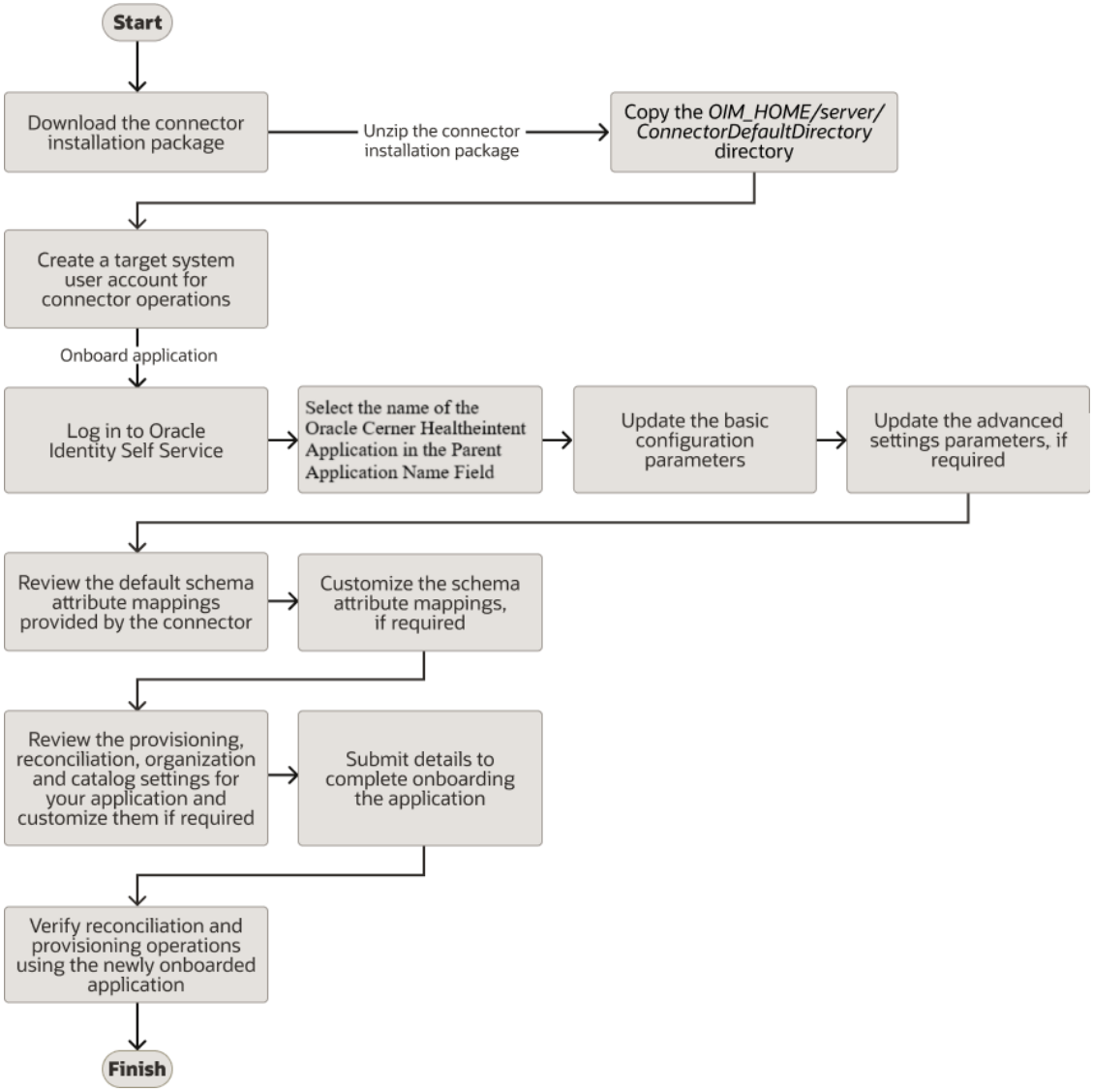
5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER.*
6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIG_HOME*/server/ConnectorDefaultDirectory directory.

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.

The following 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



Creating an Application by Using the Oracle Health Data Intelligence 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

Configure connection-related parameters while creating a target application. These parameter values will be used 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

These are the connection-related parameters that Oracle Identity Governance requires to connect to Oracle Health Data Intelligence application.

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

Table 3-1 Parameters in the Basic Configuration

Parameter	Mandatory?	Description
authenticationType	Yes	Enter the type of authentication used by your target system. This is a mandatory attribute while creating an application. Do not modify the value of the parameter. **Default value:** other
host	Yes	Enter the host name of the machine hosting your target system. This is a mandatory attribute while creating an application. **Sample value**: host.hostname.com
customAuthHeaders	Yes	"Enter the Access Token Value" **Sample value**: access_token=eyJhbGciOiJub25lIn0.eyJpc3MiOiJodHRwczpcL1wvYXV0aG9yaXphdGlvbi5zYW5kYm94Y2VybmVyLmNvbVwvIiwiaWF0IjoxNTk0Mjk5NTc5LiLCJrIXkiOiJmMWVmZmRlOS0wMjIyLTQ0OWEtOThmYi01MjczNDVkMWQyYzYifSwianRpIjoiNzQ0YTc3NjAtMzhlNS00N2ZlLWFkZDMtYzczMjlhZjNyZjNmIn0.
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.

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

Parameter	Mandatory?	Description
sslEnabled	Yes	If the target system requires SSL connectivity, then set the value of this parameter to true. Otherwise set the value to false. **Default value:** true

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.

Table 3-2 Advanced Settings Parameters

Parameter	Mandatory?	Description
Connector Name	Yes	This entry holds the name of the connector class. **Default value**: org.identityconnectors.cernerhealtheintent.CernerHealtheintentConnector
Bundle Name	Yes	This entry holds the name of the connector bundle. **Default value**: org.identityconnectors.cernerhealtheintent
Bundle Version	Yes	This entry holds the version of the connector bundle. **Default value**: 12.3.0

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
relURIs	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. **Default value**: "__ACCOUNT__.SEARCHOP=/personnel/v1/personnel?$(Filter Suffix)$&offset=$(PAGE_OFFSET)$&limit=$(PAGE_SIZE)$","__ACCOUNT__.SEARCHOP_FOR_CREATE=/personnel/v1/personnel?formattedName=$(formattedName)$&aliasType=$(__ACCOUNT__.aliases.type)$&aliasValue=$(__ACCOUNT__.aliases.value)$&aliasSystem=$(__ACCOUNT__.aliases.system)$","__ACCOUNT__.SYNCOP=/personnel/v1/personnel?syncTimeToken=$(Sync Token)$&offset=$(PAGE_OFFSET)$&limit=$(PAGE_SIZE)$","__ACCOUNT__.CREATEOP=/personnel/v1/personnel","__ACCOUNT__.UPDATEOP=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.DELETEOP=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.ADDATTRIBUTE=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.REMOVEATTRIBUTE=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.__GROUP__.SEARCHOP=/personnel/v1/personnel-groups?excludeDynamic=true","__ACCOUNT__.__GROUP__.REMOVEATTRIBUTE=/personnel/v1/personnel-groups/$(__GROUP__.id)$/members/$(__UID__)$","__ACCOUNT__.__GROUP__.ADDATTRIBUTE=/personnel/v1/personnel-groups/$(__GROUP__.id)$/members/$(__UID__)$","__ACCOUNT__.__ORGANIZATION__.SEARCHOP=/organization/v1/personnel/$(__UID__)$/organizations&offset=$(PAGE_OFFSET)$&limit=$(PAGE_SIZE)$","__ACCOUNT__.__ORGANIZATION__.ADDATTRIBUTE=/organization/v1/organizations/$(__ORGANIZATION__.id)$/members/$(__UID__)$","__ACCOUNT__.__ORGANIZATION__.REMOVEATTRIBUTE=/organization/v1/organizations/$(__ORGANIZATION__.id)$/members/$(__UID__)$","__ACCOUNT__.__DYNAMICGROUP__.SEARCHOP=/personnel/v1/dynamic-personnel-groups","__ACCOUNT__.sourceIdentifiers.ADDATTRIBUTE=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.sourceIdentifiers.REMOVEATTRIBUTE=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.aliases.ADDATTRIBUTE=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.aliases.REMOVEATTRIBUTE=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.languages.ADDATTRIBUTE=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.languages.REMOVEATTRIBUTE=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.emailAddresses.ADDATTRIBUTE=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.emailAddresses.REMOVEATTRIBUTE=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.phoneNumbers.ADDATTRIBUTE=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.phoneNumbers.REMOVEATTRIBUTE

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
		=/personnel/v1/personnel/$(__UID__)$","__ACCOUNT__.__ORGANIZATION__.SEARCHOP=/organization/v1/personnel/$(__UID__)$/organizations","__DYNAMICGROUP__.SEARCHOP=/personnel/v1/dynamic-personnel-groups?&offset=$(PAGE_OFFSET)$&limit=$(PAGE_SIZE)$","__ORGANIZATION__.SEARCHOP=/organization/v1/organizations?&offset=$(PAGE_OFFSET)$&limit=$(PAGE_SIZE)$","__GROUP__.SEARCHOP=/personnel/v1/personnel-groups?excludeDynamic=true&offset=$(PAGE_OFFSET)$&limit=$(PAGE_SIZE)$","__DATAPARTITIONID__.SEARCHOP=/data-ingestion/v1/data-partitions?&offset=$(PAGE_OFFSET)$&limit=$(PAGE_SIZE)$","__ACCOUNT__.TESTOP=/personnel/v1/personnel"
opTypes	Yes	This entry specifies the HTTP operation type for each object class supported by the connector. Values are comma separated and are in the following format: *OBJ_CLASS.OP=HTTP_OP* In this format, *OBJ_CLASS* is the connector object class, *OP* is the connector operation (for example, CreateOp, UpdateOp, SearchOp), and *HTTP_OP* is the HTTP operation (GET, PUT, or POST). **Default value**: "__ACCOUNT__.SEARCHOP=GET","__ACCOUNT__.SEARCHOP_FOR_CREATE=GET","__ACCOUNT__.SYNCOP=GET","__ACCOUNT__.CREATEOP=POST","__ACCOUNT__.UPDATEOP=PUT","__ACCOUNT__.ADDATTRIBUTE=PUT","__ACCOUNT__.REMOVEATTRIBUTE=DELETE","__ACCOUNT__.DELETEOP=DELETE","__GROUP__.SEARCHOP=GET","__ACCOUNT__.__GROUP__.SEARCHOP=GET","__ACCOUNT__.__GROUP__.ADDATTRIBUTE=PUT","__ACCOUNT__.__GROUP__.REMOVEATTRIBUTE=DELETE","__ORGANIZATION__.SEARCHOP=GET","__ACCOUNT__.__ORGANIZATION__.SEARCHOP=GET","__ACCOUNT__.__ORGANIZATION__.REMOVEATTRIBUTE=DELETE","__ACCOUNT__.__ORGANIZATION__.ADDATTRIBUTE=PUT","__DYNAMICGROUP__.SEARCHOP=GET","__ACCOUNT__.__DYNAMICGROUP__.SEARCHOP=GET","__ACCOUNT__.__DYNAMICGROUP__.ADDATTRIBUTE=PUT","__ACCOUNT__.__DYNAMICGROUP__.REMOVEATTRIBUTE=DELETE","__ACCOUNT__.emailAddresses.ADDATTRIBUTE=PUT","__ACCOUNT__.emailAddresses.REMOVEATTRIBUTE=DELETE","__ACCOUNT__.aliases.ADDATTRIBUTE=PUT","__ACCOUNT__.aliases.REMOVEATTRIBUTE=DELETE","__ACCOUNT__.sourceIdentifiers.ADDATTRIBUTE=PUT","__ACCOUNT__.sourceIdentifiers.REMOVEATTRIBUTE=DELETE","__ACCOUNT__.languages.ADDATTRIBUTE=PUT","__ACCOUNT__.languages.REMOVEATTRIBUTE=DELETE","__ACCOUNT__.phoneNumbers.ADDATTRIBUTE=PUT","__ACCOUNT__.phoneNumbers.REMOVEATTRIBUTE=DELETE","__DATAPARTITIONID__.SEARCHOP=GET"
customPayload	No	This entry lists the payloads for all operations that are not in the standard format. **Default value:** "__ACCOUNT__.__GROUP__.ADDATTRIBUTE={}","__ACCOUNT__.__GROUP__.REMOVEATTRIBUTE={}","__ACCOUNT__.__ORGANIZATION__.ADDATTRIBUTE={}","__ACCOUNT__.__ORGANIZATION__.REMOVEATTRIBUTE={}"

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
nameAttributes	Yes	This entry holds the name attribute for all the objects that are handled by this connector. For example, __NAME__ for the __ACCOUNT__each object class that it used for User accounts, the name attribute is user_name." **Default value**: "__ACCOUNT__.fullName","__GROUP__.name","__ORGANIZATION__.name","__DYNAMICGROUP__.name","__DATAPARTITIONID__.name"
uidAttributes	Yes	This entry holds the UID attribute for all the objects that are handled by this connector. For example, __UID__ for each object class. **Default value**: "__ACCOUNT__.id","__GROUP__.id","__ORGANIZATION__.id","__DYNAMICGROUP__.id","__DATAPARTITIONID__.id","sourceIdentifiers.id","emailAddresses.value","phoneNumbers.value","aliases.value","languages.languages"
httpHeaderContentType	No	This entry holds the content type expected by the target system in the header. **Default value**: application/json
httpHeaderAccept	No	This entry holds the accept type expected from the target system in the header. **Default value**: application/json
jsonResourcesTag	No	This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload. **Default value**: "__ACCOUNT__=items","__GROUP__=items","__ORGANIZATION__=items","__DYNAMICGROUP__=items","__DATAPARTITIONID__=items"
specialAttributeTargetFormat	No	This entry lists the format in which an attribute is present in the target system endpoint. For example, the alias attribute will be present as aliases.alias in the target system endpoint. Values are comma separated and are presented in the following format: *OBJ_CLASS.ATTR_NAME=TARGET_FORMAT.* **Default value**: "__ACCOUNT__=items","__GROUP__=items","__ORGANIZATION__=items","__DYNAMICGROUP__=items"

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
specialAttributeHandling	No	This entry lists the format in which an attribute is present in the target system endpoint. Values are comma separated and are presented in the following format: OBJ_CLASS.ATTR_NAME=TARGET_FORMAT. **Default value**: "__ACCOUNT__.__GROUP__.ADDATTRIBUTE=SINGLE","__ACCOUNT__.__GROUP__.REMOVEATTRIBUTE=SINGLE","__ACCOUNT__.__ORGANIZATION__.ADDATTRIBUTE=SINGLE","__ACCOUNT__.__ORGANIZATION__.REMOVEATTRIBUTE=SINGLE","__ACCOUNT__.sourceIdentifiers.ADDATTRIBUTE=SINGLE","__ACCOUNT__.sourceIdentifiers.REMOVEATTRIBUTE=SINGLE","__ACCOUNT__.aliases.ADDATTRIBUTE=SINGLE","__ACCOUNT__.aliases.REMOVEATTRIBUTE=SINGLE","__ACCOUNT__.emailAddresses.ADDATTRIBUTE=SINGLE","__ACCOUNT__.emailAddresses.REMOVEATTRIBUTE=SINGLE","__ACCOUNT__.phoneNumbers.ADDATTRIBUTE=SINGLE","__ACCOUNT__.phoneNumbers.REMOVEATTRIBUTE=SINGLE","__ACCOUNT__.languages.ADDATTRIBUTE=SINGLE","__ACCOUNT__.languages.REMOVEATTRIBUTE=SINGLE"
pageSize	No	The number of users that appears on a page for a search operation. **Default value**:100
doUpdateIfUserAlreadyExists	Yes	If true, creating an existing user updates them. If false, it throws an 'already exists' error. **Default value**: True
incrementalSyncTokenAttributes	Yes	The SyncToken is updated with the latest token by checking which configured attribute holds the most recent timestamp. **Default value**: "updatedAt","personnelGroupAssociationUpdatedAt","organizationMembershipUpdatedAt","organizationAdministrationUpdatedAt"

Attribute Mappings

The following topic provides the attribute mappings details.

- Attribute Mappings for the Target Application

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 Health Data Intelligence 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.

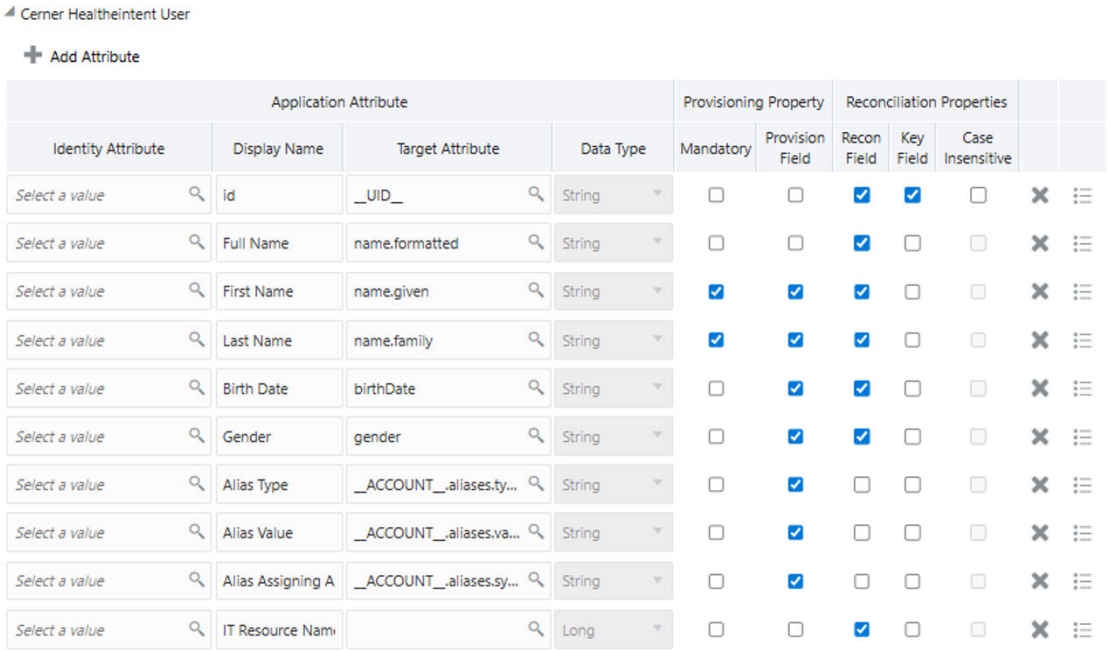
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-3 Default Attributes for Cerner Health Data Intelligence Target Application

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
id	__UID__	String	No	No	Yes	Yes	No
Full Name	name.formatted	String	No	No	Yes	No	Not applicable
First Name	name.given	String	Yes	Yes	Yes	No	Not applicable
Last Name	name.family	String	Yes	Yes	Yes	No	Not applicable
Birth Date	birthDate	String	No	Yes	Yes	No	Not applicable
Gender	gender	String	No	Yes	Yes	No	Not applicable
Alias Type	__ACCOUNT__.aliases.type	String	No	Yes	No	No	Not applicable
Alias Value	__ACCOUNT__.aliases.value	String	No	Yes	No	No	Not applicable
Alias Assigning Authority	__ACCOUNT__.aliases.system	String	No	Yes	No	No	Not applicable
IT Resource Name	-	Long	No	No	Yes	No	Not applicable

The following figure shows the default User account attribute mappings.

Figure 3-1 Default Attribute Mappings for Cerner Health Data Intelligence User Account



Cerner Health Data Intelligence Languages

The following table lists the Languages forms attribute mappings between the process form fields in Oracle Identity Governance and Cerner Health Data Intelligence 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.

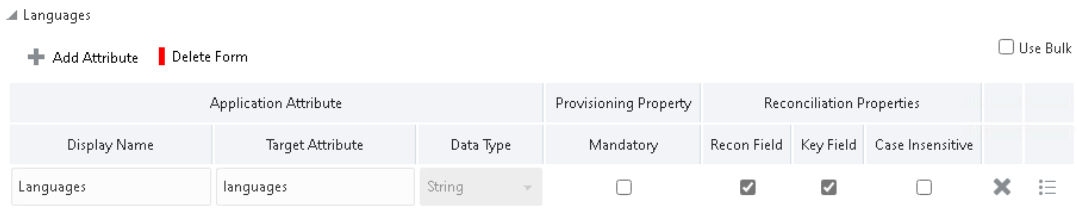
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-4 Default Attribute Mappings for Languages

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Languages	languages	String	No	Yes	Yes	No

The following figure shows the default Languages mapping.

Figure 3-2 Default Attribute Mappings for Cerner Health Data Intelligence



Cerner Health Data Intelligence Emails

The following table lists the Emails forms attribute mappings between the process form fields in Oracle Identity Governance and Cerner Health Data Intelligence 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.

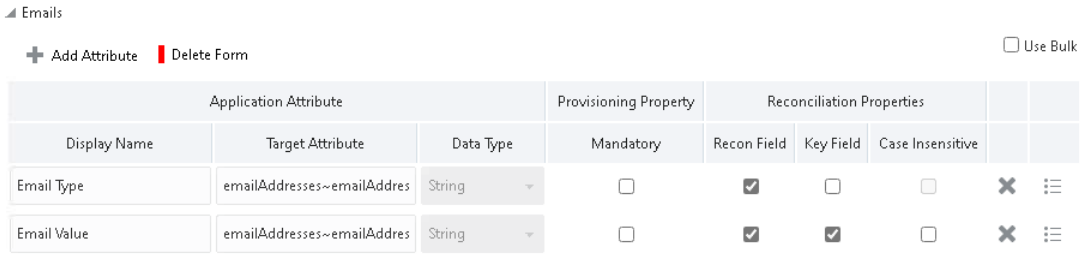
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-5 Default Attribute Mappings for Emails

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Email Type	emailAddresses~emailAddresses~type	String	No	Yes	No	Not Applicable
Email Value	emailAddresses~emailAddresses~value	String	No	Yes	Yes	No

The following figure shows the default Emails mapping.

Figure 3-3 Default Attribute Mappings for Cerner Health Data Intelligence Emails



Cerner Health Data Intelligence Phone Number

The following table lists the Phone Number forms attribute mappings between the process form fields in Oracle Identity Governance and Cerner Health Data Intelligence 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.

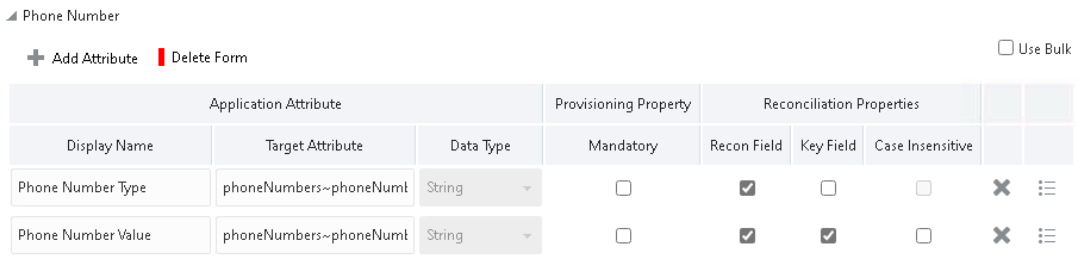
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-6 Default Attribute Mappings for Phone Number

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Phone Number Type	phoneNumbers~phoneNumbers~type	String	No	Yes	No	Not Applicable
Phone Number Value	phoneNumbers~phoneNumbers~value	String	No	Yes	Yes	No

The following figure shows the default Phone Number mapping.

Figure 3-4 Default Attribute Mappings for Cerner Health Data Intelligence Phone Number



Cerner Health Data Intelligence Aliases

The following table lists the Aliases forms attribute mappings between the process form fields in Oracle Identity Governance and Cerner Health Data Intelligence 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.

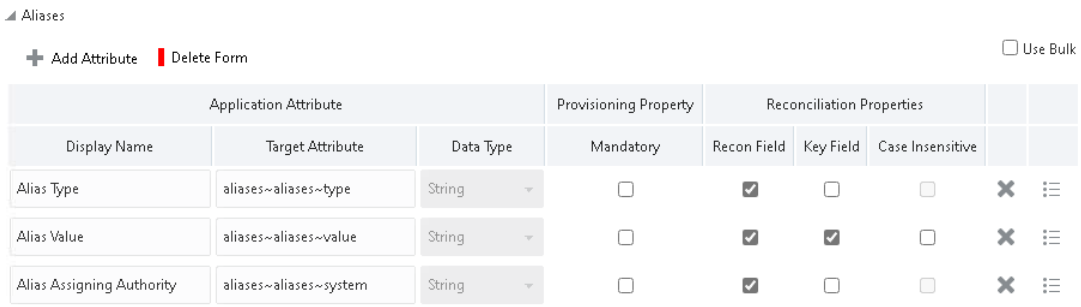
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-7 Default Attribute Mappings for Aliases

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Alias Type	aliases~aliases~type	String	No	Yes	No	Not Applicable
Alias Value	aliases~aliases~value	String	No	Yes	Yes	No
Alias Assigning Authority	aliases~aliases~system	String	No	Yes	No	Not Applicable

The following figure shows the default Aliases mapping.

Figure 3-5 Default Attribute Mappings for Cerner Health Data Intelligence Aliases



Cerner Health Data Intelligence Personnel IDs

Below table lists the Personnel IDs forms attribute mappings between the process form fields in Oracle Identity Governance and Cerner Health Data Intelligence 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.

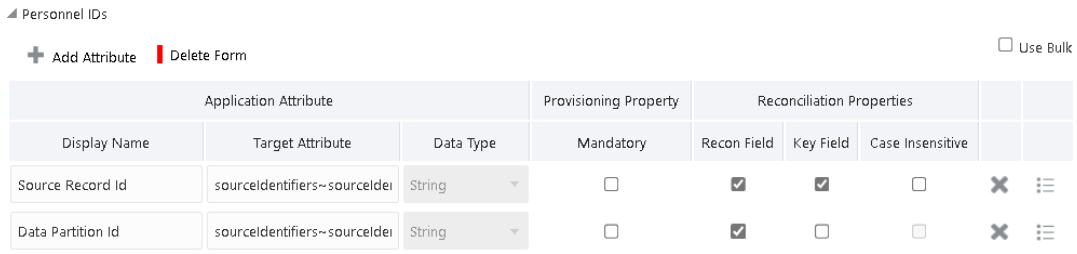
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-8 Default Attribute Mappings for Personnel IDs

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Source Record ID	sourceIdentifiers~sourceIdentifiers~id	String	No	Yes	Yes	No
Data Partition ID	sourceIdentifiers~sourceIdentifiers~dataPartitionId	String	No	Yes	No	Not Applicable

The following figure shows the default Personnel IDs mapping.

Figure 3-6 Default Attribute Mappings for Cerner Health Data Intelligence Personnel IDs



Cerner Health Data Intelligence Personnel Groups Entitlement

Below table lists the Personnel Groups forms attribute mappings between the process form fields in Oracle Identity Governance and Cerner Health Data Intelligence 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 3-9 Default Attribute Mappings for Personnel Groups

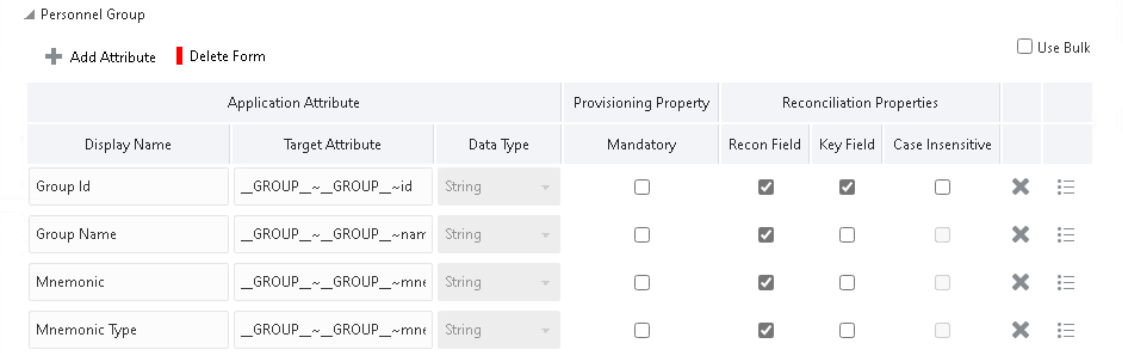
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Group Id	__GROUP__~__GROUP__~id	String	No	Yes	Yes	No
Group Name	__GROUP__~__GROUP__~name	String	No	Yes	No	Not Applicable

Table 3-9 (Cont.) Default Attribute Mappings for Personnel Groups

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Mnemonic	__GROUP__~__GROUP__~mnemonic	String	No	Yes	No	Not Applicable
Mnemonic Type	__GROUP__~__GROUP__~mnemonicType	String	No	Yes	No	Not Applicable

The following screenshot shows the default Personnel IDs mapping.

Figure 3-7 Default Attribute Mappings for Cerner Health Data Intelligence Personnel Groups



Cerner Health Data Intelligence Organization Entitlement

Below table lists the Organization forms attribute mappings between the process form fields in Oracle Identity Governance and Cerner Health Data Intelligence 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 3-10 Default Attribute Mappings for Organization

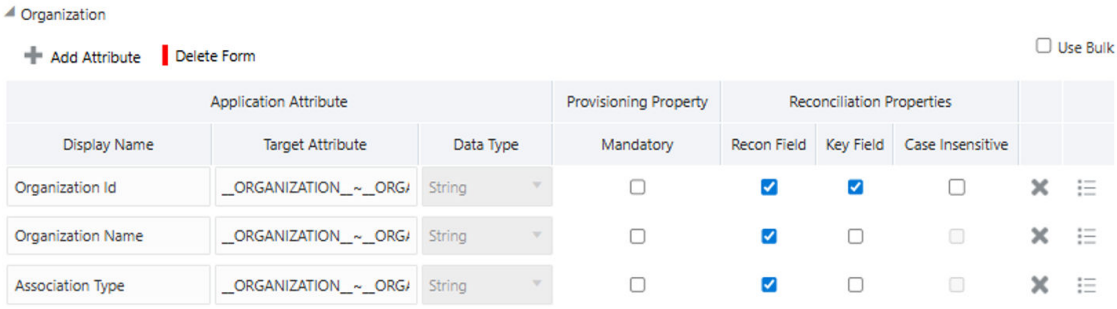
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Organization Id	__ORGANIZATION__~__ORGANIZATION__~id	String	No	Yes	Yes	No
Organization Name	__ORGANIZATION__~__ORGANIZATION__~name	String	No	Yes	No	Not applicable

Table 3-10 (Cont.) Default Attribute Mappings for Organization

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Association Type	__ORGANIZATION__~__ORGANIZATION__~associationType	String	No	Yes	No	Not applicable

The following figure shows the default Organization Entitlement mapping.

Figure 3-8 Default Attribute Mappings for Cerner Health Data Intelligence Organization



Cerner Health Data Intelligence Personnel Group Views

The below table lists the Personnel Group View forms attribute mappings between the process form fields in Oracle Identity Governance and Cerner Health Data Intelligence 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 3-11 Default Attribute Mappings for Personnel Group Views

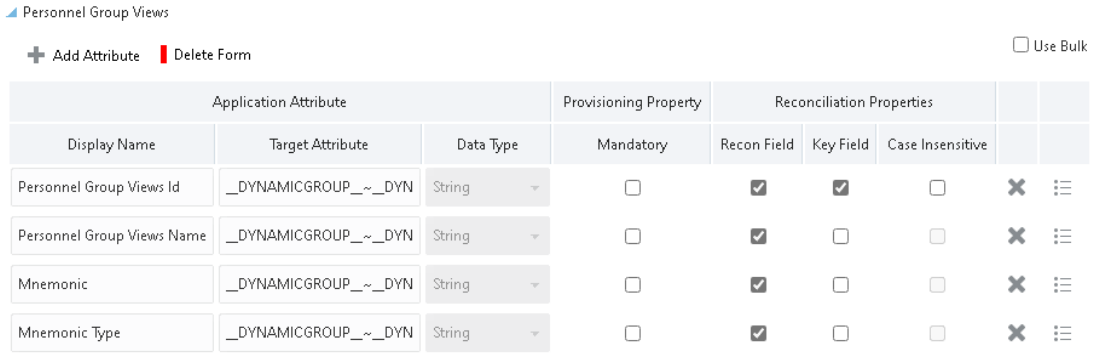
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Personnel Group Views Id	__DYNAMICGROUP__~__DYNAMICGROUP__~id	String	No	Yes	Yes	No
Personnel Group Views Name	__DYNAMICGROUP__~__DYNAMICGROUP__~name	String	No	Yes	No	Not Applicable
Mnemonic	__DYNAMICGROUP__~__DYNAMICGROUP__~mnemonic	String	No	Yes	No	Not Applicable

Table 3-11 (Cont.) Default Attribute Mappings for Personnel Group Views

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive ?
Mnemonic Type	__DYNAMICGROUP__~__DYNAMICGROUP__~mnemonicType	String	No	Yes	No	Not Applicable

The following figure shows the default Personnel Group Views mapping.

Figure 3-9 Default Attribute Mappings for Cerner Health Data Intelligence Personnel Group Views



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

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 Health Data Intelligence 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.

Below table lists the default simple correlation rule for a Cerner Health Data Intelligence 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 3-12 Predefined Identity Correlation Rule for a Cerner Health Data Intelligence Connector

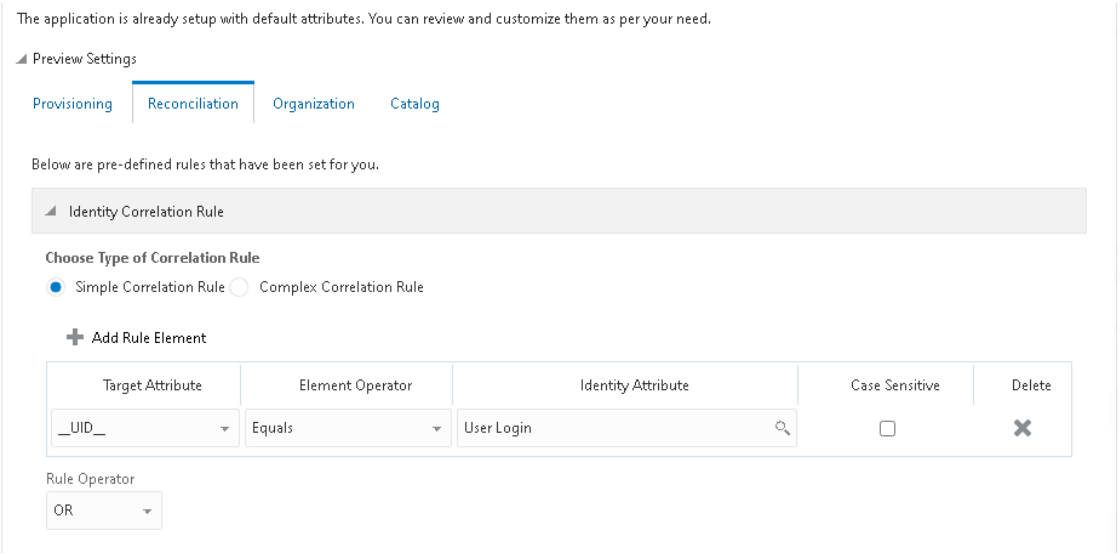
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__UID__	Equals	User Login	No

In this identity rule:

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

The following figure shows the Simple Correlation Rule for Cerner Health Data Intelligence Target Application

Figure 3-10 Simple Correlation Rule for Cerner Health Data Intelligence Target Application



Predefined Situations and Responses

The Cerner Health Data Intelligence 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.

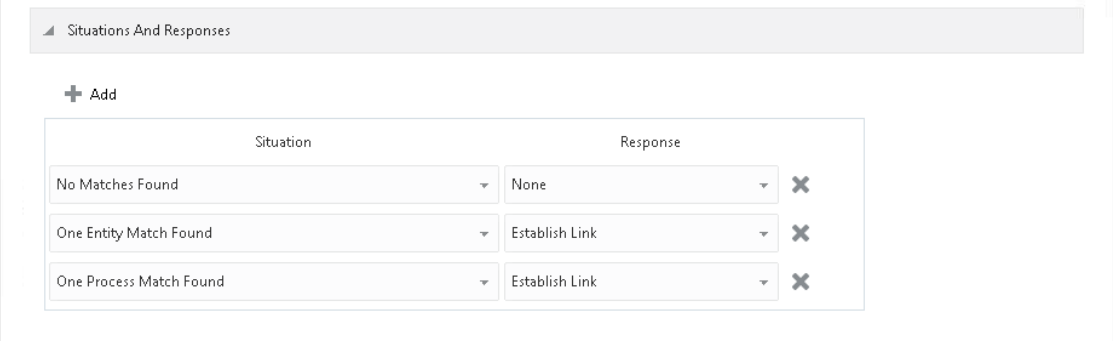
Below table lists the default situations and responses for a Cerner Health Data Intelligence Target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses Updating Situations and Responses in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance

Table 3-13 Predefined Situations and Responses for a Cerner Health Data Intelligence Target Application

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

The following figure shows the situations and responses for a Cerner Health Data Intelligence that the connector provides by default.

Figure 3-11 Predefined Situations and Responses for a Cerner Health Data Intelligence Target Application



Reconciliation Jobs

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

User Reconciliation Job

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*.

Cerner Healtheintent Full User Reconciliation: Job is used reconcile user data from a target application.

Cerner Healtheintent Incremental User Reconciliation: Job is used to fetch the records that are added or modified after the last reconciliation run.

Below table describes the parameters of the Cerner Healtheintent Full User Reconciliation job.

Table 3-14 Parameters of the Cerner Healtheintent 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 *not* change the default value.
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. See Performing Limited (Filtered) Reconciliation for more information about this attribute.
Object Type	This parameter holds the name of the object type for the reconciliation run. **Default value**: User Do *not* change the default value.
Scheduled Task Name	Name of the scheduled task used for reconciliation. Do *not* modify the value of this parameter.

Below table describes the parameters of the Cerner Healtheintent Incremental User Reconciliation job.

Table 3-15 Parameters of the Cerner Healtheintent Incremental 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 *not* change the default value.
Object Type	This parameter holds the name of the object type for the reconciliation run. **Default value**: User Do *not* change the default value.
Scheduled Task Name	Name of the scheduled task used for reconciliation. Do *not* modify the value of this parameter.
Sync Token	This parameter holds the value of the target system attribute that is specified as the value of the Incremental Recon Attribute parameter. The Latest Token parameter is used for internal purposes. By default, this value is empty. Enter the expression for filtering records that the scheduled job must reconcile. **Sample value**: <String>2025-08-01T08:43:42Z</String>

Delete User Reconciliation Job

The **Cerner Healtheintent User Delete Reconciliation** job is used to reconcile deleted user data from a target application.

Table 3-16 Parameters of the Cerner Healtheintent User Delete 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 *not* change the default value.

Table 3-16 (Cont.) Parameters of the Cerner Healtheintent User Delete Reconciliation Job

Parameter	Description
Object Type	This parameter holds the name of the object type for the reconciliation run. **Default value**: User Do *not* change the default value.
Scheduled Task Name	Name of the scheduled task used for reconciliation. Do *not* modify the value of this parameter.

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- Cerner Healtheintent Personnel Group Lookup Reconciliation
- Cerner Healtheintent Personnel Group Views Lookup Reconciliation
- Cerner Healtheintent Organization Lookup Reconciliation
- Cerner Healtheintent Data Partitions ID Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-17 Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	Current AOB application name with which the reconciliation job is associated. Do *not* 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 *not* 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__
Lookup Name	Enter the name of the lookup definition in Oracle Identity Governance that must be populated with values fetched from the target system. Depending on the Reconciliation job that you are using, the default values are as follows: • For Cerner Healtheintent Personnel Group Lookup Reconciliation: Lookup.CernerHealtheintent.Groups • For Cerner Healtheintent Personnel Group Views Lookup Reconciliation: Lookup.CernerHealtheintent.DynamicGroups • For Cerner Healtheintent Organization Lookup Reconciliation: Lookup.CernerHealtheintent.Organizations • For Cerner Healtheintent Data Partitions ID Lookup Reconciliation: Lookup.CernerHealtheintent.DataPartitionIDs 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.

Table 3-17 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Object Type	Enter the type of object you want to reconcile. Depending on the reconciliation job that you are using, the default values are as follows: • For Cerner Healtheintent Personnel Group Lookup Reconciliation: __GROUP__ • For Cerner Healtheintent Personnel Group Views Lookup Reconciliation: __DYNAMICGROUP__ • For Cerner Healtheintent Organization Lookup Reconciliation: __ORGANIZATION__ • For Cerner Healtheintent Data Partitions ID Lookup Reconciliation: __DATAPARTITIONID__ **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.

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

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

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*.

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.

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*.

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*

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.

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

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

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.

Enabling Logging for the Connector Server

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

1. Open the logging.properties file in a text editor.

2. Navigate to the *CONNECTOR_SERVER_HOME*/Conf directory.
3. Edit the following entry by replacing INFO with the required level of Logging:`.level=INFO`

   `example: .level=FINEST ORG.IDENTITYCONNECTORS.CERNERHEALTHEINTENT.level=FINEST`
4. Save and close the file.
5. Restart the connector server.

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 the following table.

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

Table 4-1 (Cont.) Log Levels and ODL Message Type:Level Combinations

Java Level	ODL Message Type:Level
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.

Enabling Logging

Perform this procedure to enable logging in Oracle WebLogic Server.

To enable logging in Oracle WebLogic Server:

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

```
<log_handler name='HealtheIntent-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>


<logger name=" ORG.IDENTITYCONNECTORS.CERNERHEALTHEINTENT"
level="[LOG_LEVEL]" useParentHandlers="false"> <handler
name="HealtheIntent-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= ‘HealtheIntent-handler’
level='NOTIFICATION:1'class='oracle.core.ojdl.logging.ODLHandlerFactory'
> <property name='logreader:' value='off'/> <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\server
s\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.CERNERHEALTHEINTENT"
level="NOTIFICATION:1" useParentHandlers="false"> <handler name="
HealtheIntent-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.

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 below table.

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 Oracle Health data intelligence 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 Oracle Health data intelligence 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*.

Localizing Field Labels in UI Forms

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

To localize field labels 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 (oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip) to the local computer**.**
5. Extract the contents of the archive, and open the following file in a text editor:

   ```
   SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.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 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 Oracle Health data intelligence Application instance. The original code is:

```
<trans-unit
   id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBund
le']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO
.UD_HEALHEINTENT_USR_FIRST_NAME__c_description']}"><source>User Id</
source><target/></trans-unit><trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.
HEALHEINTENT.entity.HEALHEINTENT.UD_ HEALHEINTENT _ FIRST_NAME
__c_LABEL"><source> FIRST NAME</source><target/> </trans-unit>
```

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

```
global.udf.UD_ HEALHEINTENT_USR_FIRST_NAME =
\u30E6\u30FC\u30B6\u30FC\u540D
```

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.user
EO.UD_ HEALHEINTENT_FIRST_NAME _c_description']}"><source> First Name</
source> <target>\u30E6\u30FC\u30B6\u30FCID </target></trans-unit>
<trans-unitid="sessiondef.oracle.iam.ui.runtime.form.model.
HEALHEINTENT.entity.HEALHEINTENT_USR_FIRST_NAME __c_LABEL "><source>
First Name</source> <target> \u30E6\u30FC\u30B6\u30FC\u540D </target></
trans-unit>
```

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

f. 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.

> **Note**
>
> 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 and log in to Oracle Identity Governance.

Configuring SSL

Configure SSL to secure data communication between Oracle Identity Governance and the Oracle Cerner Health Data Intelligence target system.

If you are using this connector along with a Connector Server, then there is no need to configure SSL. You can skip this section.

To configure SSL:

1. Obtain the SSL public key certificate of Oracle Cerner Health Data Intelligence.
2. Copy the public key certificate of Oracle Cerner Health Data Intelligence to the computer hosting Oracle Identity Governance.
3. Run the following `keytool` command to import the public key certificate into the identity key store in Oracle Identity Governance:
   `keytool -import -alias ALIAS -trustcacerts -file CERT_FILE_NAME -keystore KEYSTORE_NAME -storepass PASSWORD`

In this command:

- *ALIAS* is the public key certificate alias.
- *CERT_FILE_NAME* is the full path and name of the certificate store (the default is cacerts).
- *KEYSTORE_NAME* is the name of the keystore.
- *PASSWORD* is the password of the keystore.

The following are sample values for this command:

- `keytool -import -keystore <JAVA_HOME>/jre/lib/security/cacerts -file <Cert_Location>/HealtheIntent.crt -storepass changeit -alias HealtheIntent01`
- `keytool -import -keystore <WL_HOME>/server/lib/DemoTrust.jks -file <Cert_Location>/HealtheIntent.crt -storepass DemoTrustKeyStorePassPhrase -alias HealtheIntent02`

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
  - – In the Oracle Identity Governance cluster, perform this procedure on each node of the cluster and then restart each node.
  - – Ensure that the system date for Oracle Identity Governance is in sync with the validity date of the SSL certificate to avoid any errors during SSL communication.

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

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 Incremental Reconciliation
- Performing Limited (Filtered) Reconciliation

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, ensure that no value is specified for the Filter parameter of the job for reconciling users.

Performing Incremental Reconciliation

In incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Governance

During an incremental reconciliation run, the scheduled job fetches only target system records that are added or modified after the timestamp stored in the Sync Token attribute of the scheduled job. At the end of the reconciliation run, the connector automatically updates the Sync Token parameter of the job for user record reconciliation to the time stamp at which the run ended. This is incremental reconciliation.

Sample value for Sync Token: `<String>2025-08-01T08:43:42Z</String>`

Performing Limited (Filtered) Reconciliation

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

By default, all target system records added or modified after the last reconciliation run are reconciled during the current one. 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. Cerner Health Data Intelligence API only supports /i**d** filter. Below is an example of the filter.

Filter Suffix value: /id

Example: /3bae409-071e-4f7e-83c1-bd34090697d7

In this example, the record whose User Id value is 3bae409-071e-4f7e-83c1-bd34090697d7 is reconciled.

Configuring Reconciliation Jobs

Configure reconciliation jobs to perform reconciliation runs that check for latest 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.

Configuring Provisioning

You can configure the provisioning operation for the Cerner Health Data Intelligence Connector.

This section provides information on the following topics:

- Guidelines on Performing Provisioning Operations
- Performing Provisioning Operations

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, following values as required:

- First Name: First name of the user
- Last Name: Last name of the user
- Alias Type: Alias Type of the user
- Alias Value: Alias value of the user
- Alias Assigning Authority: Alias assigning authority of user

Attributes to Update in the parent form of User account

- First Name: First name of the user
- Last Name: Last name of the user
- Birth Date: The User’s birth date

> **Note**
>
> Birth date format: YYYY-MM-DD
>
> Sample value: 1947-08-15

- Gender: The User’s gender

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

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*.

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 operation. 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*.

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, Limitations and FAQ for Oracle Cerner Health Data Intelligence Application

The following are the known issues, limitations and FAQ for this connector.

- After assigning Personnel Group and Organization to the personnel user account, you need to run the User Reconciliation job to fetch the group IDs and organization IDs to do further actions on those groups and organization.
- User filter reconciliation requires about 4 minutes.
- When reconciling a user who does not exist in OIM, the alias information will not appear in the parent form even after the user is successfully linked to OIM user.

Limitation:

DEA, NPI – These aliases cannot be assigned from OIG due to Cerner Health Data Intelligence API limitation.

8

Files and Directories in the Connector Installation Package

These are the components of the connector installation package that comprise the Oracle Health Data Intelligence connector.

Table 8-1 Files and Directories in the Oracle Health data intelligence Connector Installation Package

File in the Installation Package	Description
/bundle/ org.identityconnectors.cernerhealtheintent-12.3.0.jar	This JAR is the ICF connector bundle.
configuration/CernerHealtheintent-CI.xml	This XML file contains configuration information.
Files in the resource's 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.

Table 8-1 (Cont.) Files and Directories in the Oracle Health data intelligence Connector Installation Package

File in the Installation Package	Description
xml/CernerHealtheintent-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 and the configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/CernerHealtheintent-pre-config.xml	This XML file contains definitions for lookup and schedule task.

Glossary

Index