Oracle® Identity Governance

Configuring the Arcon PAM Connector

12c (12.2.1.3.0)
F89840-01

ORACLE

Oracle Identity Governance Configuring the Arcon PAM Connector, 12c (12.2.1.3.0)

F89840-01

Primary Author: Maya Chakrapani

Contributors:

Contents

List of Figures

List of Tables

Preface

This guide describes the connector that is used to onboard the DocuSign application to Oracle Identity Governance.

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

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

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Introduction to the Connector

This chapter introduces the ARCON Privileged Access Management Application 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 ARCON Privileged Access Management Connector lets you create and onboard ARCON Privileged Access Management 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 Recommendations
3. Certified Languages
4. Supported Connector Operations
5. Connector Architecture
6. Use Cases Supported by the Connector
7. Connector Features

1.1 Certified Components

These are the software components and their versions required for installing and using the ARCON Privileged Access Management 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 12*c* PS3 (12.2.1.3.0) or later.
Oracle Identity Governance or Oracle Identity Manager JDK	JDK 1.8 and later
Target systems	ARCON Privileged Access Management
Connector Server	11.1.2.1.0 or 12.2.1.3.0
Connector Server JDK	JDK 1.8 and later
Target API version	v1

1.2 Usage Recommendations

If you are using Oracle Identity Governance 12c (12.2.1.3.0), 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.

1.3 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

1.4 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
Role Grant Management	
Assign and Revoke Roles	Yes
Group Grant Management	
Assign and Revoke Groups	Yes
LOB Grant Management	
Assign and Revoke LOBs	Yes
MFA Grant Management	
Assign and Revoke MFA	Yes
Service Grant Management	
Assign and Revoke PemanentServices	Yes
Assign and Revoke OneTimeServices	Yes
Assign and Revoke TimeBasedServices	Yes

1.5 Connector Architecture

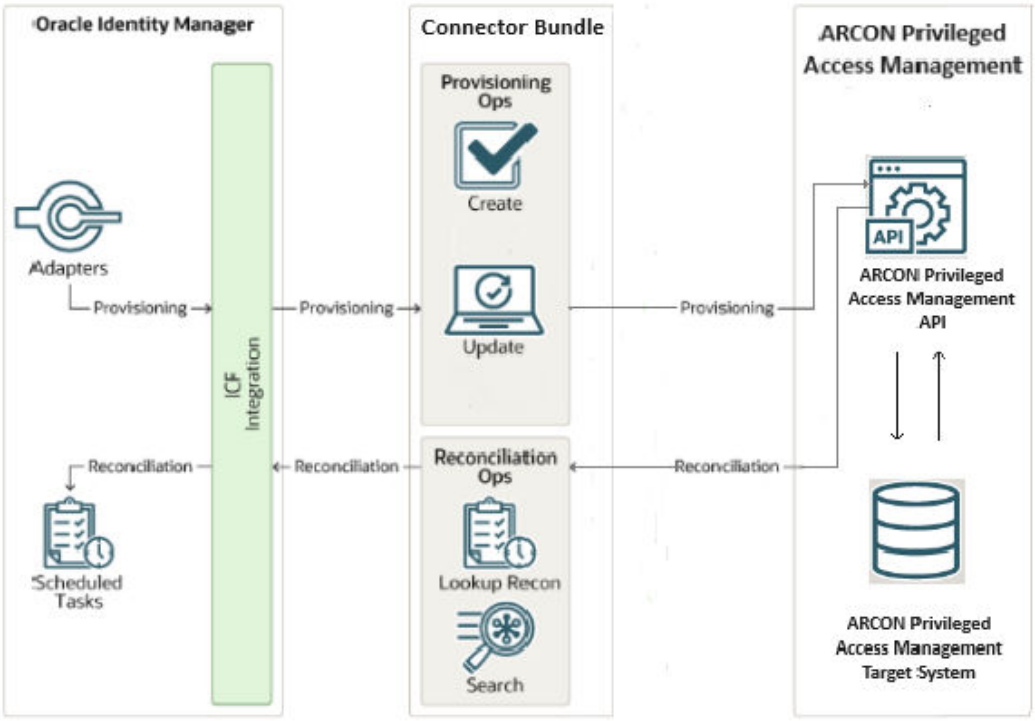
The ARCON Privileged Access Management is implemented by using the Identity Connector Framework (ICF).

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 ARCON Privileged Access Management.

Figure 1-1 ARCON Privileged Access Management 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 and updating users on the target system through Oracle Identity Governance. During provisioning, the adapters invoke the ICF operation; ICF in turn invokes the create operation on the ARCON Privileged Access Management Identity Connector Bundle, and then the bundle calls the target system API (ARCON Privileged Access Management 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 initiates an ICF operation, which involves searching the ARCON Privileged Access Management Identity Connector Bundle. This bundle interfaces with the ARCON Privileged Access Management API to retrieve user records that meet specific criteria. These records are then returned via the bundle and ICF to the scheduled task, where they are integrated into Oracle Identity Governance.

Each record from the target system is compared to existing ARCON Privileged Access Management resources provisioned in OIM. When a match is found, updates from the target system's ARCON Privileged Access Management record are copied to the corresponding ARCON Privileged Access Management resource in Oracle Identity Governance. If there's no match, the record's name is compared with OIM user logins. In the event of a match, the data from the target system's record is utilized to provision an ARCON Privileged Access Management resource for the OIM user.

The Connector Bundle uses the HTTPS protocol to communicate with the ARCON Privileged Access Management API, which provides programmatic access through SCIM API endpoints. These endpoints enable applications to perform create, read, and update operations on various directory data and objects, including users, roles, multi-factor authentication, services, and groups.

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

ARCON Privileged Access Management can be integrated with Oracle Identity Governance to ensure synchronized lifecycle management of privileged accounts within your enterprise, aligning with other identity-aware applications. ARCON Privileged Access Management offers identity management for various models, including Cloud Identity, Synchronized Identity, and Federated Identity, making it a valuable choice for organizations seeking consistent management of accounts, groups, and roles. The following is the most common scenarios in which this connector can be used:

- **ARCON Privileged Access Management User Management:**
  An organization using ARCON Privileged Access Management aims to integrate it with Oracle Identity Governance for efficient identity management. This integration enables user identity creation within the target system via Oracle Identity Governance. It also facilitates the synchronization of user identity changes made directly in the target system with Oracle Identity Governance.

  To achieve this, you need to configure the ARCON Privileged Access Management connector application with your target system, providing the necessary connection details. When you wish to create a new user in the target system, you can complete and submit the OIM process form to initiate the provisioning operation. The connector will execute the CreateOp operation in the target system, resulting in the user's creation upon successful execution. Updates can be performed in a similar manner.

  For searching and retrieving user identities, a scheduled task from Oracle Identity Governance must be run. The connector will execute the corresponding SearchOp operation within the target system, capturing all changes and syncing them with Oracle Identity Governance.

1.7 Connector Features

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

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
Delete reconciliation	No
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
Reset password	Yes

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

1. User Provisioning
2. Full 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

1.7.1 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

1.7.2 Full Reconciliation

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

For more information, see Performing Full Reconciliation

1.7.3 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.

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 (Filtered) 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 Transformation and Validation of Account Data

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

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

1.7.6 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*.

1.7.7 Secure Communication to the Target System

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

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

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.

2.1 Prerequisites for Creating an Application By Using the Connector

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

2.1.1 Prerequisites Required from Target System to Perform Connector Operations

You require the following inputs:

- ARCON Privileged Access Management Instance URL.
- ARCON Privileged Access Management Instance UserName and Password.
- HostName of the target.

> **Note:**
>
> UserName and Password encrypted through ARCON Privileged Access Management is required in basic configuration details while creating connector application.
>
> Reach out to ARCON Privileged Access Management support team for above details.

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:

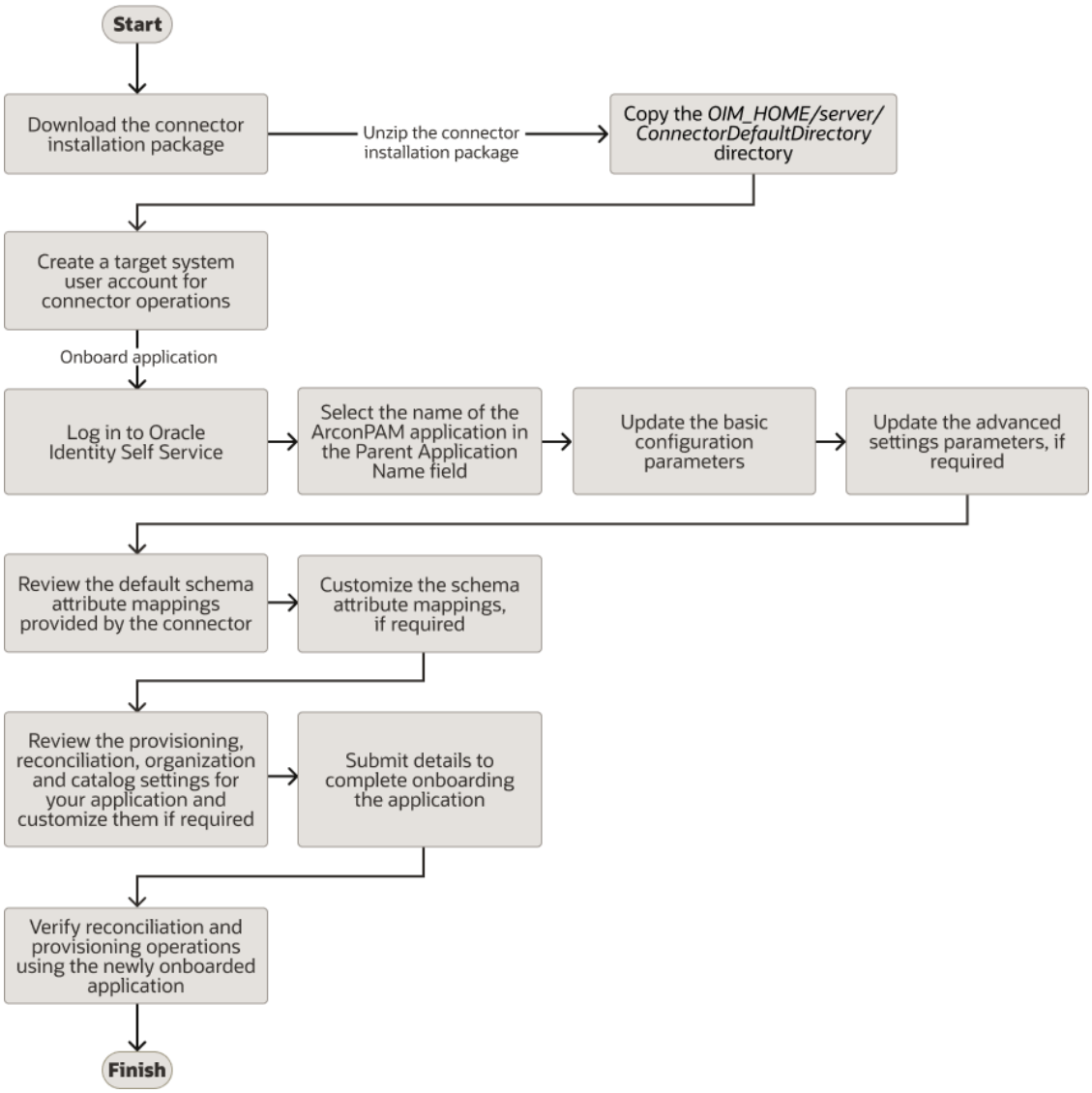
1. Navigate to the OTN website at http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html .
2. Click **OTN License Agreement** and read the license agreement.
3. Select the **Accept License Agreement** option.
   You must accept the license agreement before you can download the installation package.
4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.
5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER.*
6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIG_HOME*/server/ConnectorDefaultDirectory directory.

2.2 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.

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



2.3 Creating an Application by Using the ARCON Privileged Access Management 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.

Note:

- Configuring the Connector of 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.

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to ARCON Privileged Access Management 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. For this connector, the target system uses custom authentication which is similar to client credentials but with UserName and Password. This is a mandatory attribute while creating an application. Do not modify the value of the parameter. **Default value:** custom
customAuthClassName	No	Enter the name of the class implementing the custom authentication logic. **Default value**: `oracle.iam.connectors.arconpam.auth.ArconPAMAuth`

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

Parameter	Mandatory?	Description
authenticationServerUrl	No	Enter the URL of the authentication server that validates the UserName and Password for your target system. **Default value**: https://apigateway-poc.arconnet.com/authentication/api/Token/getToken
username	Yes	Enter the username of the target system that you create for performing connector operations. **Sample value**: lUmsHktlhZKaAPjhCrVRz9hbSrBhEDO57MQpC9U=
password	Yes	Enter the password of the target system user account that you create for connector operations. **Sample value**: o7axkq8DIxo9EbN8PcEOSC/JyvyyrehidmDt80m9Q=
acceptType	No	Parameter which allows you to specify your preferred data format. **Default value:** application/json
host	Yes	Enter the host name of the machine hosting your target system. This is a mandatory attribute while creating an application. **Sample value**: myhost.example.com
uriPlaceHolder	No	Enter the key-value pair for replacing place holders in the relURIs. The URI place holder consists of values which are repeated in every relative URL. Values must be comma separated. For example, tenant ID and API version values are a part of every request URL. Therefore, we replace it with a key-value pair. **Default value**: api_version;v1
ConnectorServerName	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.
port		Enter the port number at which the target system is listening. **Sample value**: 443
proxyHost	No	Enter the name of the proxy host used to connect to an external target. **Sample value**: www.example.com
proxyPassword	No	Enter the password for the proxy user
proxyPort	No	Enter the proxy port number. **Sample value**: 1105
proxyUser	No	Enter the proxy username if you are using a proxy server to access the internet.

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

Parameter	Mandatory?	Description
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:** True

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 table below are mandatory.

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.genericrest.GenericRESTConnector
Bundle Name	Yes	This entry holds the name of the connector bundle. **Default value**: org.identityconnectors.genericrest
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
nameAttributes	Yes	This entry holds the namehelpText="Target 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**: "GroupID.groupName","__ACCOUNT__.userName","RoleId.RoleName","LobId.lobName","__DOMAIN__.SadDomainName","__USERTYPE__.UserTypeName","UserDualAuthFactType.DualFactorType","__USERSERVICE__.ServiceTypeName","__ONETIMEUSERSERVICE__.ServiceTypeName","__TIMEBASEDUSERSERVICE__.ServiceTypeName","__ACCESSTYPE__.AccessTypeName"
uidAttributes	Yes	This entry holds the uidhelpText="Target attribute for all the objects that are handled by this connector. For example, __UID__ for each object class. **Default value**: "GroupID.id","__DOMAIN__.SadDomainName","LobId.id","RoleId.RoleId","__ACCOUNT__.id","UserDualAuthFactType.id","__USERTYPE__.UserTypeId","__USERSERVICE__.ServiceId","__ONETIMEUSERSERVICE__.ServiceId","__TIMEBASEDUSERSERVICE__.ServiceId","__ACCESSTYPE__.AccessTypeId"

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**: "LobId.SEARCHOP=/$(api_version)$/Lobs","__ACCOUNT__.LobId.ADDATTRIBUTE=/$(api_version)$/Lobs","__ACCOUNT__.LobId.REMOVEATTRIBUTE=/$(api_version)$/Lobs","__ACCOUNT__.SEARCHOP=/$(api_version)$/Users$(Filter Suffix)$?LobId=All Lobs&PageNumber=$(PAGE_INCREMENT)$&PageSize=$(PAGE_SIZE)$","__ACCOUNT__.TESTOP=/$(api_version)$/UserType","__ACCOUNT__.CREATEOP=/$(api_version)$/Users","__ACCOUNT__.UPDATEOP=/$(api_version)$/Users/$(__UID__)$","__ACCOUNT__.DELETEOP=/$(api_version)$/Users/$(__UID__)$","GroupID.SEARCHOP=/$(api_version)$/Groups?LobId=All Lobs&IsFullRecords=1","__ACCOUNT__.GroupID.ADDATTRIBUTE=/$(api_version)$/Groups","__ACCOUNT__.GroupID.REMOVEATTRIBUTE=/$(api_version)$/Groups","__USERSERVICE__.SEARCHOP=/$(api_version)$/Services?LobId=All Lobs&IsFullRecords=1","__ACCOUNT__.__USERSERVICE__.ADDATTRIBUTE=/$(api_version)$/Services","__ACCOUNT__.__USERSERVICE__.REMOVEATTRIBUTE=/$(api_version)$/Services","__ACCOUNT__.__ONETIMEUSERSERVICE__.ADDATTRIBUTE=/$(api_version)$/Services","__ACCOUNT__.__TIMEBASEDUSERSERVICE__.ADDATTRIBUTE=/$(api_version)$/Services","RoleId.SEARCHOP=/$(api_version)$/Role?LobId=All Lobs","__ACCOUNT__.RoleId.A

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
		DDATTRIBUTE=/$(api_version)$/Role","__ACCOUNT__.RoleId.REMOVEATTRIBUTE=/$(api_version)$/Role","__DOMAIN__.SEARCHOP=/$(api_version)$/Domain","__USERTYPE__.SEARCHOP=/$(api_version)$/UserType","UserDualAuthFactType.SEARCHOP=/$(api_version)$/DualAuth","__ACCOUNT__.ENABLEOP=/$(api_version)$/Users/$(__UID__)$","__ACCOUNT__.DISABLEOP=/$(api_version)$/Users/$(__UID__)$","__ACCOUNT__.__PASSWORD__.UPDATEOP=/$(api_version)$/Users/$(__UID__)$","__ACCOUNT__.UserDualAuthFactType.ADDATTRIBUTE=/$(api_version)$/DualAuth","__ACCOUNT__.UserDualAuthFactType.REMOVEATTRIBUTE=/$(api_version)$/DualAuth","__ACCESSTYPE__.SEARCHOP=/$(api_version)$/Services/GetAccessTypes"

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
opTypes	No	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**: "LobId.SEARCHOP=GET","__ACCOUNT__.LobId.ADDATTRIBUTE=PATCH","__ACCOUNT__.LobId.REMOVEATTRIBUTE=PATCH","__ACCOUNT__.SEARCHOP=GET","__ACCOUNT__.CREATEOP=POST","__ACCOUNT__.UPDATEOP=PUT","__ACCOUNT__.DELETEOP=DELETE","GroupID.SEARCHOP=GET","__ACCOUNT__.GroupID.ADDATTRIBUTE=PATCH","__ACCOUNT__.GroupID.REMOVEATTRIBUTE=PATCH","__ACCOUNT__.__USERSERVICE__.SEARCHOP=GET","__ACCOUNT__.__USERSERVICE__.ADDATTRIBUTE=PATCH","__ACCOUNT__.__USERSERVICE__.REMOVEATTRIBUTE=PATCH","__ACCOUNT__.__ONETIMEUSERSERVICE__.ADDATTRIBUTE=PATCH","__ACCOUNT__.__TIMEBASEDUSERSERVICE__.ADDATTRIBUTE=PATCH","RoleId.SEARCHOP=GET","__ACCOUNT__.RoleId.ADDATTRIBUTE=PATCH","__ACCOUNT__.RoleId.REMOVEATTRIBUTE=PATCH","__DOMAIN__.SEARCHOP=GET","__USERTYPE__.SEARCHOP=GET","UserDualAuthFactType.SEARCHOP=GET","__ACCOUNT__.TESTOP=GET","__ACCOUNT__.ENABLEOP=PUT","__ACCOUNT__.DISABLEOP=PUT","__ACCOUNT__.__PASSWORD__.UPDATEOP=PUT","__ACCOUNT__.UserDualAuthFactType.ADDATTRIBUTE=PATCH","__ACCOUNT__.UserDualAuthFactType.REMOVEATTRIBUTE=PATCH"

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
pageSize	No	The number of users that appears on a page for a search operation. **Default value**:100
statusEnableValue	No	This value is used to activate the user during reconciliation. **Default value**:1
statusDisableValue	No	This value is used to deactivate the user during reconciliation. **Default value**:0
jsonResourcesTag	No	This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload. **Default value**: "GroupID=Result","__DOMAIN__=Result","LobId=Result","__ACCOUNT__=Result","RoleId=Result","UserDualAuthFactType=Result","__USERTYPE__=Result","__ACCESSTYPE__=Result","__USERSERVICE__=Result","__ONETIMEUSERSERVICE__=Result","__TIMEBASEDUSERSERVICE__=Result"
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

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__.GroupID.ADDATTRIBUTE=SINGLE","__ACCOUNT__.GroupID.REMOVEATTRIBUTE=SINGLE","__ACCOUNT__.RoleId.ADDATTRIBUTE=SINGLE","__ACCOUNT__.RoleId.REMOVEATTRIBUTE=SINGLE","__ACCOUNT__.LobId.ADDATTRIBUTE=SINGLE","__ACCOUNT__.LobId.REMOVEATTRIBUTE=SINGLE","__ACCOUNT__.__USERSERVICE__.ADDATTRIBUTE=SINGLE","__ACCOUNT__.__USERSERVICE__.REMOVEATTRIBUTE=SINGLE","__ACCOUNT__.UserDualAuthFactType.ADDATTRIBUTE=SINGLE","__ACCOUNT__.UserDualAuthFactType.REMOVEATTRIBUTE=SINGLE","__ACCOUNT__.__ONETIMEUSERSERVICE__.ADDATTRIBUTE=SINGLE","__ACCOUNT__.__TIMEBASEDUSERSERVICE__.ADDATTRIBUTE=SINGLE"

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
customPayload	No	This entry lists the payloads for all operations that are not in the standard format. **Default value**: "__ACCOUNT__.ENABLEOP={\"ValidTillDate\":\"12/31/2058 12:00:00 AM\",\"IsActive\":1}","__ACCOUNT__.DISABLEOP={\"ValidTillDate\":\"12/31/2022 12:00:00 AM\",\"IsActive\":1}","__ACCOUNT__.__PASSWORD__.UPDATEOP={\"password\":\"$(__PASSWORD__)$\"}","__ACCOUNT__.GroupID.ADDATTRIBUTE={\"op\":\"add\",\"GroupID\":(id),\"LobId\":\"All Lobs\",\"value\":[{\"UserId\":$(__UID__)$}]}","__ACCOUNT__.GroupID.REMOVEATTRIBUTE={\"op\":\"remove\",\"GroupID\":(id),\"LobId\":\"All Lobs\",\"value\":[{\"UserId\":$(__UID__)$}]}","__ACCOUNT__.RoleId.ADDATTRIBUTE={\"op\":\"add\",\"UserId\":$(__UID__)$,\"RoleId\":[$(RoleId)$]}","__ACCOUNT__.RoleId.REMOVEATTRIBUTE={\"op\":\"remove\",\"UserId\":$(__UID__)$,\"RoleId\":[$(RoleId)$]}","__ACCOUNT__.CREATEOP={\"userName\":\"$(__NAME__)$\",\"displayName\":\"$(displayName)$\",\"ValidTillDate\":\"$(ValidTillDate)$\",\"IsActive\":1,\"emails\":{\"value\":\"$(emails.value)$\"},\"phoneNumbers\":{\"value\":\"$(phoneNumbers.value)$\"},\"GroupID\":[],\"domainName\":\"$(domainName)$\",\"LobId\":\"$(LobPrimary)$\",\"userTypeId\":$(userTypeId)$,\"password\":\"$(__PASSWORD__)$\",\"RoleId\":[4]}","__ACCOUNT__.LobId.ADDATTRIBUTE={\"op\":\"add\",\"UserID\":$(__UID__)$,\"LobId\":[$(LobId)$]}","__ACCOUNT__.LobId.REMOVEATTRIBUTE={\"op\":\"remove\",\"UserID\":$(__UID__)$,\"LobId\":[$(LobId)$]}","__ACCOUNT__.User

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
		DualAuthFactType.ADDATTRIBUTE={\"op\": \"add\",\"UserId\": $(__UID__)$,\"DualFactorTypeId\": [(id)]}","__ACCOUNT__.UserDualAuthFactType.REMOVEATTRIBUTE={\"op\": \"remove\",\"UserId\": $(__UID__)$,\"DualFactorTypeId\": [(id)]}","__ACCOUNT__.__USERSERVICE__.ADDATTRIBUTE={\"op\":\"add\",\"UserID\":$(__UID__)$,\"LobId\":\"AllLobs\",\"value\":[{\"ServiceId\": $(ServiceId)$}]}","__ACCOUNT__.__USERSERVICE__.REMOVEATTRIBUTE={\"op\":\"remove\",\"UserID\":$(__UID__)$,\"LobId\":\"AllLobs\",\"value\":[{\"ServiceId\": $(ServiceId)$}]}","__ACCOUNT__.__ONETIMEUSERSERVICE__.ADDATTRIBUTE={\"op\":\"add\",\"UserID\":$(__UID__)$,\"LobId\":\"All Lobs\",\"AccessType\":\"$(AccessTypeId)$\",\"StartDateTime\":\"$(StartDateTime)$\",\"EndDateTime\":\"$(EndDateTime)$\",\"value\":[{\"ServiceId\":$(ServiceId)$}]}","__ACCOUNT__.__TIMEBASEDUSERSERVICE__.ADDATTRIBUTE={\"op\":\"add\",\"UserID\":$(__UID__)$,\"LobId\":\"AllLobs\",\"AccessType\":\"$(AccessTypeId)$\",\"StartDate\":\"$(StartDate)$\",\"EndDate\":\"$(EndDate)$\",\"StartTime\":\"$(StartTime)$\",\"EndTime\":\"$(EndTime)$\",\"hours\":\"$(hours)$\",\"minutes\":\"$(minutes)$\",\"value\":[{\"ServiceId\":$(ServiceId)$}]}" **Note**: ValidTillDate can be provided as per the customer requirement for ENABLEOP and DISABLEOP URLs in the custom payload

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description

statusAttributes	No	This entry lists the name of the target system attribute that holds the status of an account. For example, for the
		
		`__ACCOUNT__`
		
		object class that it used for User accounts, the status attribute is
		
		`accountEnabled`
		
		.
		Default value: __ACCOUNT__.IsActive

passwordAttribute	No	This entry holds the name of the target system attribute that is mapped to the __PASSWORD__ attribute of the connector in OIM. **Default value**: password
targetObjectIdentifier	No	This entry specifies the key-value pair for replacing place holders in the relURIs. Values are comma separated and in the *KEY*;*VALUE* format. **Default value:** "__ACCOUNT__.__USERSERVICE__=AccessTypeId;1","__ACCOUNT__.__ONETIMEUSERSERVICE__=AccessTypeId;2","__ACCOUNT__.__TIMEBASEDUSERSERVICE__=AccessTypeId;3"
attrNameIdentifier	No	This entry specifies the variable to identify the services information in the json response **Default value:** "__USERSERVICE__=UserServicesId","__ONETIMEUSERSERVICE__=UserServicesId","__TIMEBASEDUSERSERVICE__=UserServicesId"

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.

The following table lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and ARCON Privileged Access Management 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.

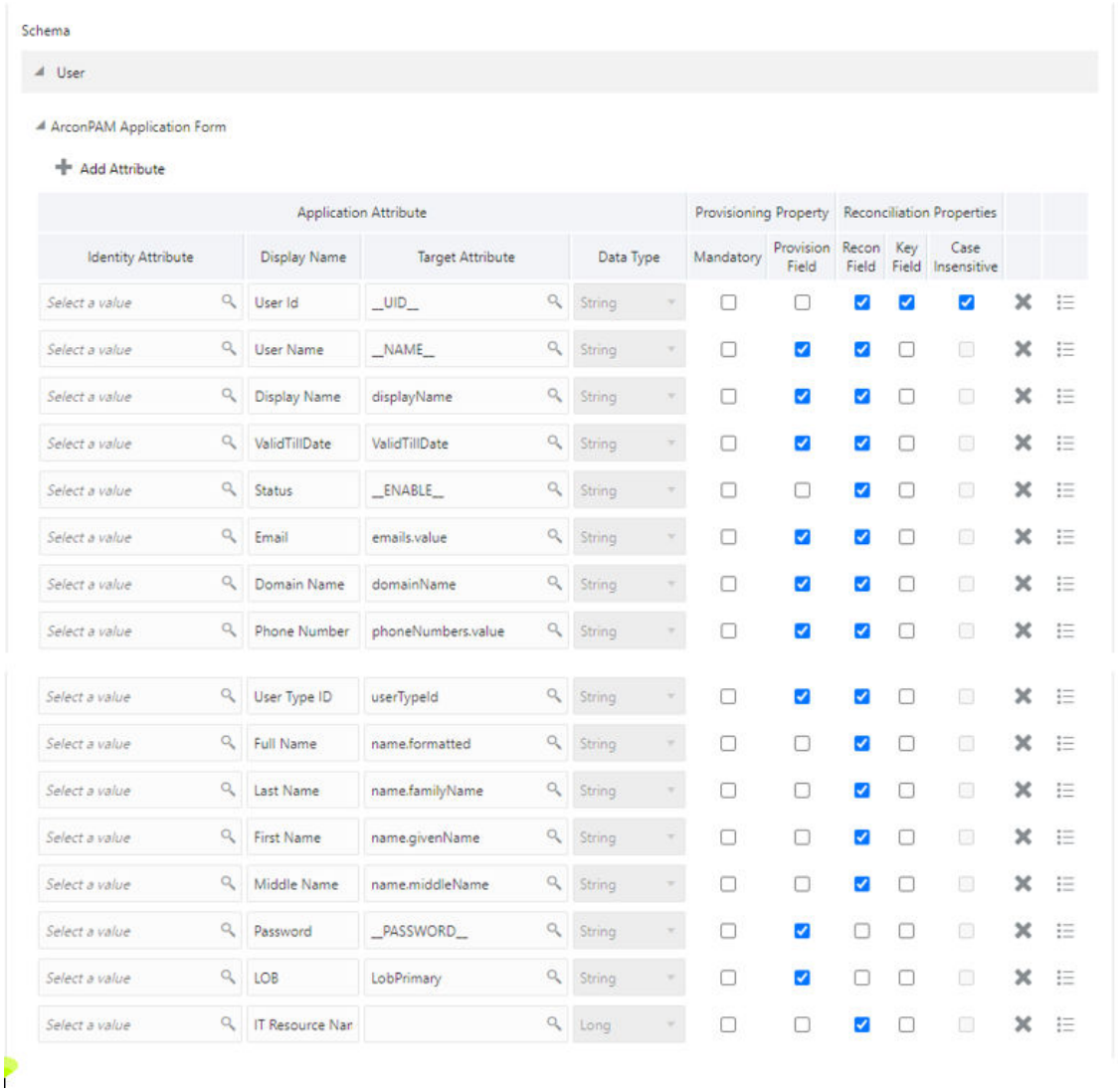
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-3 Default Attribute for ARCON Privileged Access Management Target Application

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
User ID	__UID__	String	No	No	Yes	Yes	Yes
User Name	__NAME__	String	No	Yes	Yes	No	Not applicable
Display Name	displayName	String	No	Yes	Yes	No	Not applicable
ValidTillDate	ValidTillDate	String	No	Yes	Yes	No	Not applicable
Status	__ENABLE__	String	No	No	Yes	No	Not applicable
Email	emails.value	String	No	Yes	Yes	No	Not applicable
Domain Name	domainName	String	No	Yes	Yes	No	Not applicable
Phone Number	phoneNumbers.value	String	No	Yes	Yes	No	Not applicable
User Type ID	userTypeId	String	No	Yes	Yes	No	Not applicable
Full Name	name.formatted	String	No	No	Yes	No	Not applicable
Last Name	name.familyName	String	No	No	Yes	No	Not applicable
First Name	name.givenName	String	No	No	Yes	No	Not applicable
Middle Name	name.middleName	String	No	No	Yes	No	Not applicable
Password	__PASSWORD__	String	No	Yes	No	No	Not applicable
LOB	LobPrimary	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 ARCON Privileged Access Management User Account



ARCON Privileged Access Management Roles Entitlement

The following table lists the roles forms attribute mappings between the process form fields in Oracle Identity Governance and ARCON Privileged Access Management 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.

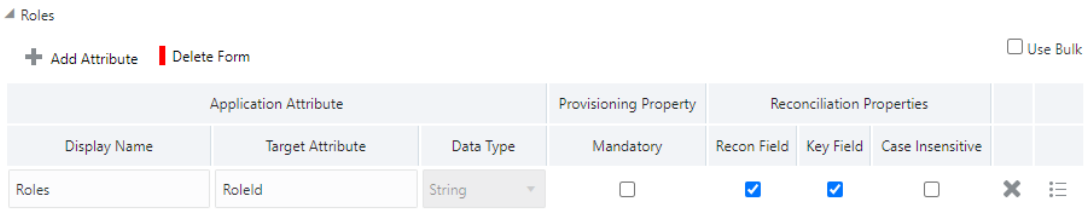
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks* with Oracle Identity Governance.

Table 3-4 Default Attribute Mappings for Roles

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

The following figure shows the default Roles Entitlement mapping.

Figure 3-2 Default Attribute Mappings for ARCON Privileged Access Management



ARCON Privileged Access Management Groups Entitlement

The following table lists the group forms attribute mappings between the process form fields in Oracle Identity Governance and ARCON Privileged Access Management 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.

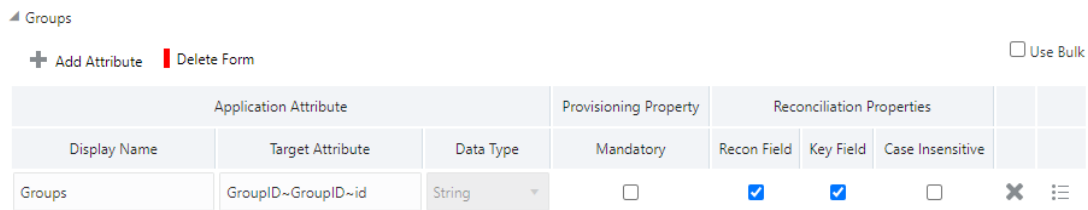
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-5 Default Attribute Mappings for Groups

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Groups	GroupID~GroupID~id	String	No	Yes	Yes	No

The following figure shows the default Groups Entitlement mapping.

Figure 3-3 Default Attribute Mappings for ARCON Privileged Access Management Groups



ARCON Privileged Access Management LOBs

The following table lists the LOB forms attribute mappings between the process form fields in Oracle Identity Governance and ARCON Privileged Access Management 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.

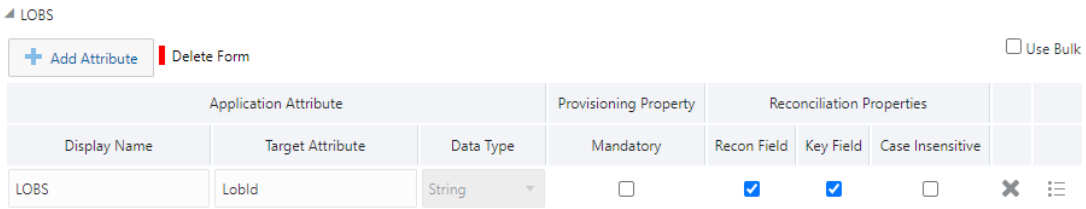
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-6 Default Attribute Mappings for LOBs

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

The following figure shows the default LOBs mapping.

Figure 3-4 Default Attribute Mappings for LOBs



ARCON Privileged Access Management Multi-factor Authentication

The following table lists the Multi-factor Authentication forms attribute mappings between the process form fields in Oracle Identity Governance and ARCON Privileged Access Management 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.

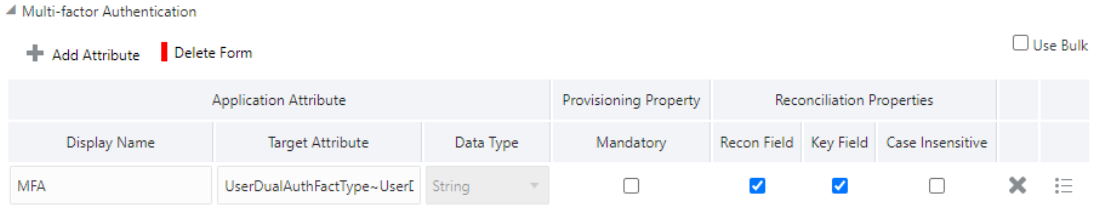
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-7 Default Attribute Mappings for Multi-factor Authentication

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
MFA	UserDualAuthFactType~UserDualAuthFactType~id	String	No	Yes	Yes	No

The following figure shows the default Multi-factor Authentication mapping.

Figure 3-5 Default Attribute Mappings for ARCON Privileged Access Management Multi-factor Authentication



ARCON Privileged Access Management PermanentServices Entitlement

The following table lists the PermanentService forms attribute mappings between the process form fields in Oracle Identity Governance and ARCON Privileged Access Management 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.

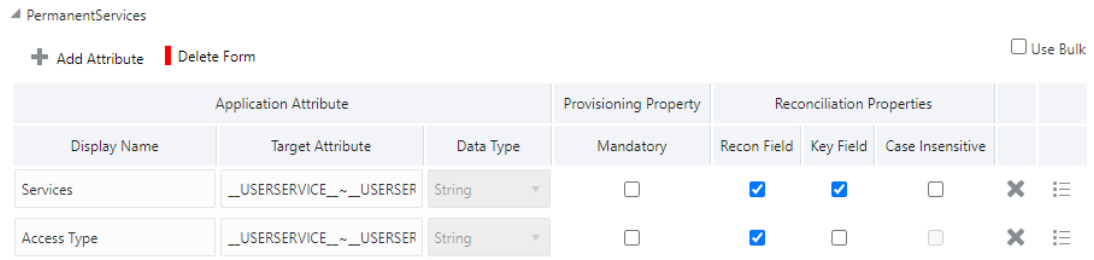
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-8 Default Attribute Mappings for PermanentServices

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Services	__USERSERVICE__~__USERSERVICE__~ServiceId	String	No	Yes	Yes	No
Access Type	__USERSERVICE__~__USERSERVICE__~AccessTypeId	String	No	Yes	No	Not Applicable

The following figure shows the default PermanentService mapping.

Figure 3-6 Default Attribute Mappings for ARCON Privileged Access Management PermanentServices



ARCON Privileged Access Management OneTimeServices Entitlement

The following table lists the OneTimeService forms attribute mappings between the process form fields in Oracle Identity Governance and ARCON Privileged Access Management 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.

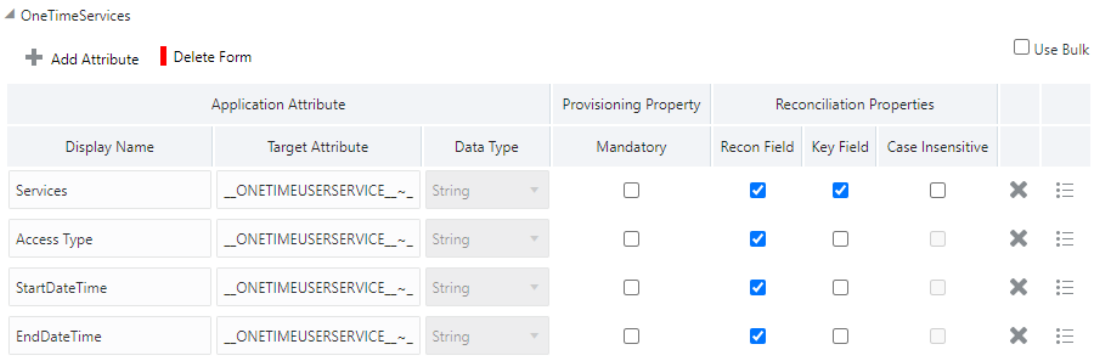
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

Table 3-9 Default Attribute Mappings for OneTimeServices

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Services	__ONETIMEUSERSERVICE__~__ONETIMEUSERSERVICE__~ServiceId	String	No	Yes	Yes	No
Access Type	__ONETIMEUSERSERVICE__~__ONETIMEUSERSERVICE__~AccessTypeId	String	No	Yes	No	Not Applicable
StartDateTime	__ONETIMEUSERSERVICE__~__ONETIMEUSERSERVICE__~StartDateTime	String	No	Yes	No	Not Applicable
EndDateTime	__ONETIMEUSERSERVICE__~__ONETIMEUSERSERVICE__~EndDateTime	String	No	Yes	No	Not Applicable

The following figure shows the default OneTimeService Entitlement mapping.

Figure 3-7 Default Attribute Mappings for ARCON Privileged Access Management OneTimeServices



ARCON Privileged Access Management TimeBasedServices Entitlement

The following table lists the TimeBasedService forms attribute mappings between the process form fields in Oracle Identity Governance and ARCON Privileged Access Management 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 TimeBasedService

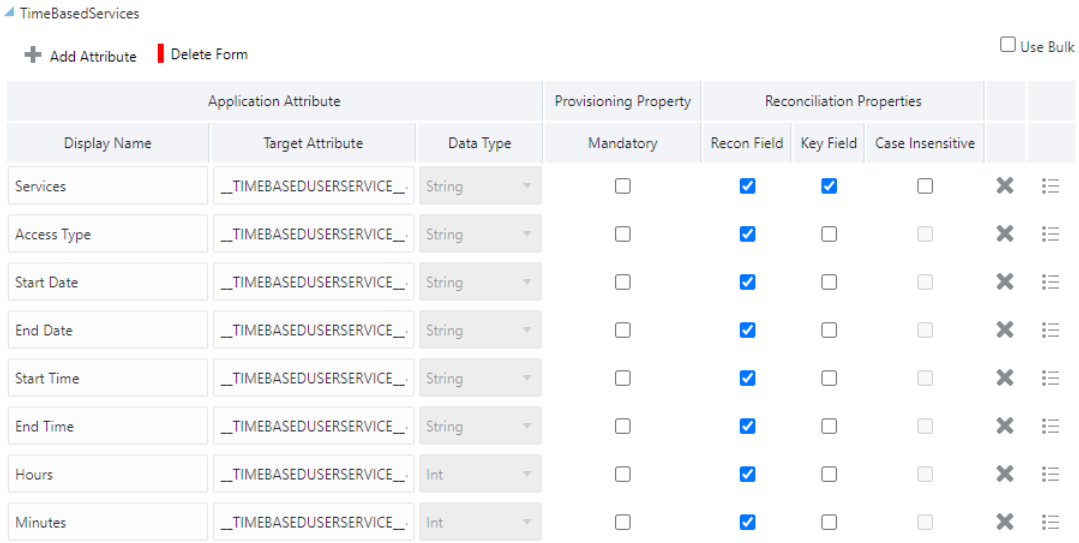
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Services	__TIMEBASEDUSERSERVICE__~__TIMEBASEDUSERSERVICE__~ServiceId	String	No	Yes	Yes	No
Access Type	__TIMEBASEDUSERSERVICE__~__TIMEBASEDUSERSERVICE__~AccessTypeId	String	No	Yes	No	Not Applicable
Start Date	__TIMEBASEDUSERSERVICE__~__TIMEBASEDUSERSERVICE__~StartDate	String	No	Yes	No	Not Applicable

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

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
End Date	__TIMEBASEDUSERSERVICE__~__TIMEBASEDUSERSERVICE__~EndDate	String	No	Yes	No	Not Applicable
Start Time	__TIMEBASEDUSERSERVICE__~__TIMEBASEDUSERSERVICE__~StartTime	String	No	Yes	No	Not Applicable
End Time	__TIMEBASEDUSERSERVICE__~__TIMEBASEDUSERSERVICE__~EndTime	String	No	Yes	No	Not Applicable
Hours	__TIMEBASEDUSERSERVICE__~__TIMEBASEDUSERSERVICE__~hours	String	No	Yes	No	Not Applicable
Minutes	__TIMEBASEDUSERSERVICE__~__TIMEBASEDUSERSERVICE__~minutes	String	No	Yes	No	Not Applicable

The following figure shows the default TimeBasedService Entitlement mapping.

Figure 3-8 Default Attribute Mappings for ARCON Privileged Access Management TimeBasedService



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 ARCON Privileged Access Management 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.

The following table lists the default simple correlation rule for a ARCON Privileged Access Management 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 3-11 Predefined Identity Correlation Rule for an ARCON Privileged Access Management Connector

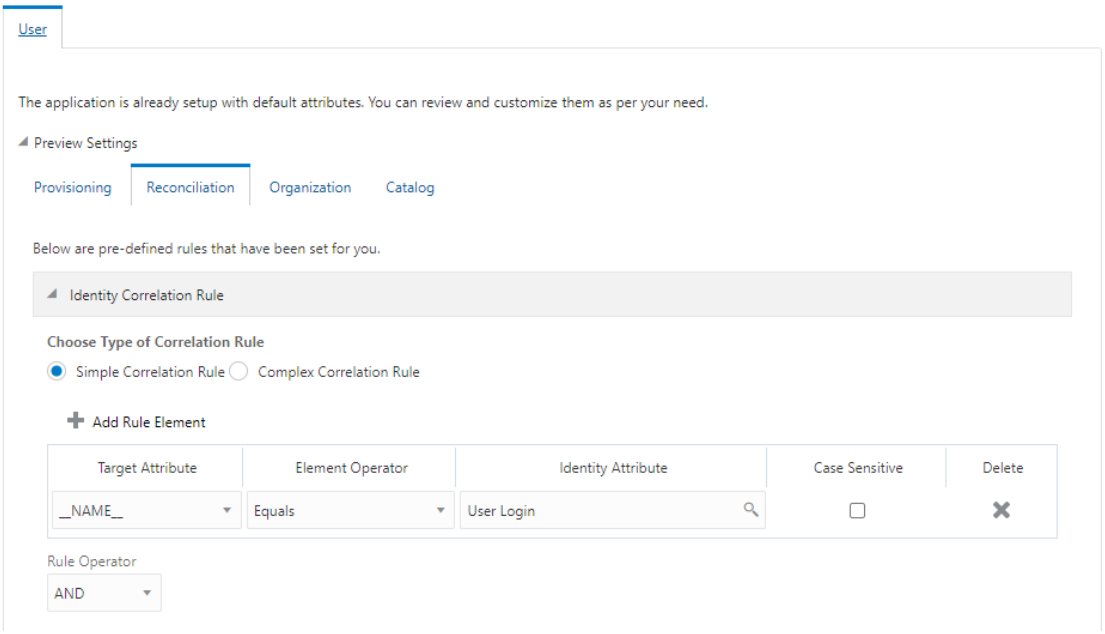
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

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.

The following figure shows the Simple Correlation Rule for ARCON Privileged Access Management Target Application

Figure 3-9 Simple Correlation Rule for ARCON Privileged Access Management Target Application



Predefined Situations and Responses

The ARCON Privileged Access Management 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.

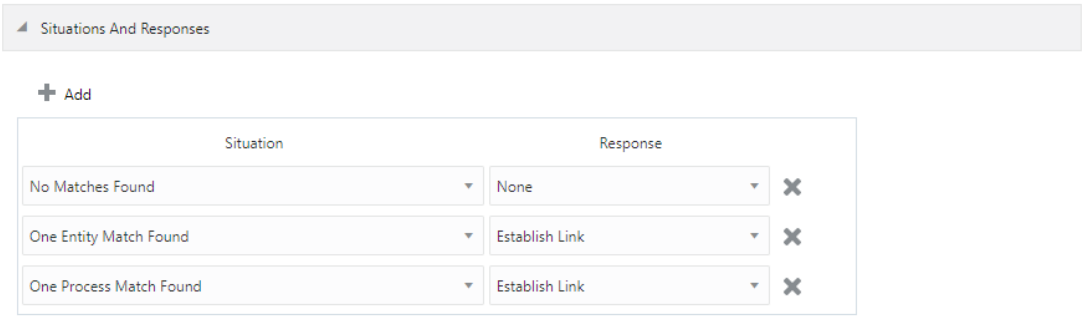
The following table lists the default situations and responses for a ARCON Privileged Access Management Target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses Updating Situations and Responses in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-12 Predefined Situations and Responses for a ARCON Privileged Access Management 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 ARCON Privileged Access Management that the connector provides by default.

Figure 3-10 Predefined Situations and Responses for a ARCON Privileged Access Management 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:

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

The following table describes the parameters of the ARCON Privileged Access Management Full User Reconciliation job.

Table 3-13 Parameters of the ARCON Privileged Access Management 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. **Filter suffix**: /User Id **Sample value:** /123 In this example, the record whose User Id value is 123 is reconciled. Note : Arcon PAM API supports only /User Id in the User Recon Filter suffix For more information about creating filters, see Performing Limited (Filtered) Reconciliation.

Table 3-13 (Cont.) Parameters of the ARCON Privileged Access Management Full User 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:

- ArconPAM Group Lookup Reconciliation
- ArconPAM LOB Lookup Reconciliation
- ArconPAM Role Lookup Reconciliation
- ArconPAM Service Lookup Reconciliation
- ArconPAM Domain Lookup Reconciliation
- ArconPAM UserType Lookup Reconciliation
- ArconPAM MFA Lookup Reconciliation
- ArconPAM AccessType Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-14 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__

Table 3-14 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
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 ArconPAM Group Lookup Reconciliation: Lookup.ArconPAM.Groups • For ArconPAM LOB Lookup Reconciliation: Lookup.ArconPAM.LOB • For ArconPAM Role Lookup Reconciliation: Lookup.ArconPAM.Roles • For ArconPAM Service Lookup Reconciliation: Lookup.ArconPAM.Services • For ArconPAM Domain Lookup Reconciliation: Lookup.ArconPAM.Domain • For ArconPAM UserType Lookup Reconciliation: Lookup.ArconPAM.UserType • For ArconPAM MFA Lookup Reconciliation: Lookup.ArconPAM.MFA • For ArconPAM AccessType Lookup Reconciliation: Lookup.ArconPAM.AccessType 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.
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 ArconPAM Group Lookup Reconciliation: GroupID • For ArconPAM LOB Lookup Reconciliation: LobId • For ArconPAM Role Lookup Reconciliation: RoleId • For ArconPAM Service Lookup Reconciliation: UserServicesId • For ArconPAM Domain Lookup Reconciliation: __DOMAIN__ • For ArconPAM UserType Lookup Reconciliation: __USERTYPE__ • For ArconPAM MFA Lookup Reconciliation: UserDualAuthFactType • For ArconPAM AccessType Lookup Reconciliation: __ACCESSTYPE__ **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

4.1 Configuring Oracle Identity Governance

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

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

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

- Creating and Activating a Sandbox
- Creating a New UI Form
- Publishing a Sandbox
- Updating an Existing Application Instance with a New Form

4.1.1 Creating and Activating a Sandbox

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

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

4.1.2 Creating a New UI Form

You can use Form Designer in Oracle Identity System Administration to create and manage application instance forms.

> **Note:**
>
> 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.

> **Note:**
>
> - 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.

> **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.

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.

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.GENERICREST.level=FINEST
   ```
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 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

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

Java Level	ODL Message Type:Level
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.

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='ArconPAM-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.GENERICREST" level="[LOG_LEVEL]"
          useParentHandlers="false">   <handler
          name="'ArconPAM-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= 'ArconPAM-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.GENERICREST" level="NOTIFICATION:1"
          useParentHandlers="false">   <handler name=" ArconPAM-
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 ARCON Privileged Access Management 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)
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. 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 ARCON Privileged Access Management 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_ARCONPAM_USER_ID __c_description']}"><source>User Id</
   source><target/></trans-unit><trans-unit
   id="sessiondef.oracle.iam.ui.runtime.form.model.ARCONPAM.entity.
   ARCONPAMEO.UD_ARCONPAM_USER_ID__c_LABEL"><source> User Id</
   source><target/> </trans-unit>
   ```

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

   ```
   global.udf.UD_ARCONPAM_USR_USER_ID=\u30E6\u30FC\u30B6\u30FCID
   ```

e. 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_ARCONPAM_USER_ID__c_description']}"><source> User Id </source>
<target>\u30E6\u30FC\u30B6\u30FCID </target></trans-unit> <trans-
unitid="sessiondef.oracle.iam.ui.runtime.form.model.
ARCONPAM.entity.ARCONPAMEO.UD_ARCONPAM_USER_ID__c_LABEL "><source> User
Id </source> <target> \u30E6\u30FC\u30B6\u30FCID </target></trans-unit>
```

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

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

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

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

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

4.6 Configuring SSL

Configure SSL to secure data communication between Oracle Identity Governance and the ARCON Privileged Access Management target system.

> **Note:**
>
> 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 ARCON Privileged Access Management.
2. Copy the public key certificate of ARCON Privileged Access Management 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.
- `keytool -import -alias serverwl -trustcacerts -file supportcert.pem -keystore client_store.jks -storepass weblogic1`
- `keytool -import -keystore <JAVA_HOME>/jre/lib/security/cacerts -file <Cert_Location>/ArconPAM.crt -storepass changeit -alias ArconPAM_1`
- `keytool -import -keystore <WL_HOME>/server/lib/DemoTrust.jks -file <Cert_Location>/ArconPAM.crt -storepass DemoTrustKeyStorePassPhrase -alias ArconPAM_2`

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

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 (Filtered) 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 job for reconciling users listed in Reconciliation Jobs.

5.1.2 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 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. ARCON PAM API only supports **User Id** filter. Below is the example for the filter.

Filter Suffix value: /User Id

Example: /524

In this example, the record whose User Id value is 524 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 ARCON Privileged Access Management 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:

- User name: The user's Username.
- Display name: The user's Display name.
- ValidTillDate: Date till the user is valid/effective.

Note: Valid date format : MM/DD/YYYY HH:MM:SS AM

Sample value: 12/31/2058 12:00:00 AM

- Email: The user's email ID.
- Domain: Domain to which user belongs to.
- User Type ID: The user's User Type ID.
- LOB: Line of Business to which the user belongs to.
- Password: The password of the user.

Attributes required to be updated in the parent form.

- User name: The user's Username
- Display name: The user's Display name.
- ValidTillDate: Date till the user is valid/effective.
- Email: The user's email ID.
- Domain: Domain to which user belongs to.
- Phone Number: The user's phone number.
- 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 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*.

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

Frequently Asked Questions of the ARCON Privileged Access Management Connector

The following is a frequently asked question (FAQ) associated with this connector.

1. How to assign services to a user from OIG?
   Answer: You can assign User services along with associated groups from the Child table, and these assignments are considered entitlements.
2. Why is the LOB attribute available in both parent form and child form?
   Answer: During creation of User in ArconPAM , at least one LOB attribute is mandatory. This attribute is sourced from the parent form, as it cannot be derived from the child form. After reconciliation, the parent LOB is incorporated into the child. At this point, removing all LOB attributes is not feasible because each user must retain at least one associated LOB attribute.
3. Is User Type Id allowed to be updated in OIG?
   Answer: The only use of User Type is during the create operation. OIG also accepts the fact that ArconPAM does not permit updating the User type ID.

8

Files and Directories in the Connector Installation Package

These are the components of the connector installation package that comprise the ARCON Privileged Access Management connector.

Table 8-1 Files and Directories in the ARCON Privileged Access Management Connector Installation Package

File in the Installation Package	Description
/bundle/ org.identityconnectors.genericrest-12.3.0.jar	This JAR is the ICF connector bundle.
configuration/ArconPAM-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/ArconPAM-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.