



# Connector Administration

*Oracle® Identity Governance Connector for  
Keycloak Realm*

*Administrator Guide*

*Release 1.0.0*

*June 2023*

# Connector Administration

*Oracle® Identity Governance Connector for  
Keycloak Realm*

*Administrator Guide*

*Release 1.0.0*

*June 2023*

First Edition

Publication date 2023-06-08

by Sophie Strecke, Dieter Steding, Sylvert Bernet, Adrien Farkaš, Tomas Sebo, Jovan Lakic, and Ádám Vincze

Copyright © 2022, 2023 Red.Security, All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

Except as contained in this notice, the names of individuals credited with contribution to this software shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from the individuals in question.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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

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

# Table of Contents

Preface .....	1
Audience .....	1
Related Documents .....	1
Typographical Conventions .....	1
Symbol Conventions .....	1
About the Keycloak Realm Connector .....	3
Certified Components .....	3
Required Versions .....	4
Required Patches .....	4
Usage Recommendation .....	4
Certified Languages .....	5
Connector Architecture .....	5
Provisioning .....	6
Reconciliation .....	6
Supported Operations .....	6
Account Management .....	6
Entitlement Management .....	7
Connector Features .....	7
Full and Incremental Reconciliation .....	7
Limited Reconciliation .....	8
Reconciliation of Deleted User Records .....	8
Lookup Fields Synchronized with the Target System .....	8
Support for the Connector Server .....	8
Support for Running Pre and Post Action Scripts .....	8
Transformation of Account Data .....	9
Secure Communication to the Target System .....	9
Connection Pooling .....	9
Support for High-Availability Configuration of the Target System .....	9
Creating a Keycloak Realm Application .....	10
Process Flow for Creating an Application .....	10
Prerequisites for Creating an Application .....	11
Configuring the Target System .....	12
Downloading the Connector Installation Package .....	15
Creating an Application .....	15
Configuring the Keycloak Realm Connector .....	16
Basic Configuration Parameters .....	16
Advanced Setting Parameters .....	17
Attribute Mappings .....	18
User Account Attributes .....	18
Group Entitlement Attributes .....	19
Client Role Entitlement Attributes .....	19
Realm Role Entitlement Attributes .....	20
Correlation Rules .....	20
Predefined Identity Correlation Rules .....	20
Predefined Situations and Responses .....	21

## Connector Administration

Reconciliation Jobs .....	21
Account Reconciliation Jobs .....	21
Reconciliation Jobs for Lookup Field Synchronization .....	24
Performing Tasks for the Keycloak Realm Connector .....	30
Configuring Oracle® Identity Governance .....	30
Creating and Activating a Sandbox .....	30
Creating a New UI Form .....	30
Updating with a New UI Form .....	31
Publishing a Sandbox .....	31
Harvesting Entitlements and Sync Catalog .....	32
Managing Logging .....	32
Understanding Log Levels .....	32
Enabling Logging .....	34
Localizing Field Labels in UI Forms .....	35
Configuring the Connector Seerver IT Resource .....	35
Configuring SSL .....	36
Using the RKC Provisioning Connector .....	38
Configuring Reconciliation .....	38
Performing Full and Incremental Reconciliation .....	38
Performing Limited Reconciliation .....	39
Configuring Reconciliation Jobs .....	39
Guidelines on Performing Provisioning Operations .....	40
Performing Provisioning Operations .....	40
Uninstalling the Connector .....	41
Extending the Functionality of the RKC Connector .....	42
Configuring Transformation and Validation of Data .....	42
Configuring Action Scripts .....	43
Configuring the Connector for Multiple Installations of the Target System .....	43
Connector Model .....	44
Overview .....	44
Account .....	45
Attributes .....	45
Prepopulation .....	46
Groups .....	46
Attributes .....	47
Prepopulation .....	47
Client Roles .....	47
Attributes .....	47
Prepopulation .....	47
Realm Roles .....	47
Attributes .....	47
Prepopulation .....	47

# List of Figures

1. Connector Architecture .....	5
2. Overall Flow of the Process for Creating an Application By Using the Connector .....	11
3. Connector Model .....	44

# List of Tables

1. Required versions of software components .....	4
2. Required patches of software components .....	4
3. Supported features per connector deployment .....	5
4. Supported operations on accounts .....	6
5. Supported operations on entitlements .....	7
6. Basic Configuration Parameters for RKC .....	16
7. Advanced Settings Parameters for a Target Application for RKC .....	18
8. Default Attribute Mappings for Keycloak Realm Account .....	18
9. Default Attribute Mappings for Keycloak Realm Account .....	19
10. Default Attribute Mappings for Keycloak Realm Account .....	20
11. Default Attribute Mappings for Keycloak Realm Account .....	20
12. Predefined Identity Correlation Rule for RKC .....	20
13. Predefined Situations and Responses for an RKC Target Application .....	21
14. Job parameters for RKC Target Application .....	22
15. Job parameters for RKC Delete Reconciliation .....	23
16. Job parameters for Group Entitlement Synchronization .....	24
17. Job parameters for Client Role Entitlement Synchronization .....	26
18. Job parameters for Realm Role Entitlement Synchronization .....	27
19. Diagnostic Logging Log Levels .....	33
20. Log Levels and ODL Message Type:Level Combinations .....	33
21. Log Levels .....	34
22. IT Resource parameters .....	36
23. Attributes stored in the form UD_RKC_USR .....	45
24. Prepopulation rules applied on the form UD_RKC_USR .....	46
25. Attributes stored in the form UD_RKC_UGR .....	47
26. Attributes stored in the form UD_RKC_UCR .....	47
27. Attributes stored in the form UD_RKC_URR .....	47

# Preface

This guide describes the connector that is used to onboard Red Hat Keycloak Realm as an applications into Oracle® Identity Governance.

## Audience

This document is intended for people who deal with the administration of resources as well as teams who deal with the integration of target systems.

## Related Documents

For information about installing and using Oracle® Identity Governance 12c, visit the following Oracle® Help Center page:

- <https://docs.oracle.com/en/middleware/idm/suite/12.2.1.3/index.html>
- <https://docs.oracle.com/en/middleware/idm/suite/12.2.1.4/index.html>

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

- <https://docs.oracle.com/en/middleware/idm/identity-governance-connectors/12.2.1.3/index.html>

## Typographical Conventions

The following table describes the typographic conventions that are used in this document.

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

## Symbol Conventions

The following table explains symbols that might be used in this document.

## Preface

Convention	Meaning
[ ]	Contains optional arguments and command options.
{   }	Contains a set of choices for a required command option.
\${ }	Indicates a variable reference.
-	Joins simultaneous multiple keystrokes.
+	Joins consecutive multiple keystrokes.
>	Indicates menu item selection in a graphical user interface.



# About the Keycloak Realm Connector

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

The Keycloak Realm connector lets you create and onboard Red Hat Keycloak Realm applications in Oracle® Identity Governance.



## Note

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

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

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

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

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

## Certified Components

The platform-specific hardware and software requirements listed in this document are valid as of the date this document was created. Since new platforms and operating systems may be certified after this document is published, it is recommended to consult the certification matrix on Oracle® Technology Network. The current statements about certified platforms and operating systems can be found there.

## About the Keycloak Realm Connector

The respective certification matrix for Oracle® Identity and Access Management Suite products are available at the following URLs:

- [Oracle® Fusion Middleware 12c \(12.2.1.4.0\)](#)
- [Oracle® Fusion Middleware 12c \(12.2.1.3.0\)](#)

### Required Versions

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

Component	Version
Oracle® Java Development Kit	JDK 1.8.0_131 or higher
Oracle® Infrastruktur	Oracle® WebLogic 12c (12.2.1.3.0)
Oracle® Database	Oracle® RDBMS 12c (12.2.0.1.0) or higher
Oracle® Identity Governance	Oracle® Identity Governance 12c Release 12.2.1.3.0
Connector Server	Identity Connector Server Release 12.2.1.3.0
Target System	Red Hat Keycloak Realm Connector Release 1.0.0.0

Table 1. Required versions of software components

### Required Patches

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

Component	Version
Oracle® Identity Governance	Patch 30735905 Oracle® Identity Governance Bundle Patch ID:200108.2108)

Table 2. Required patches of software components

### Usage Recommendation

These are the recommendations for the Identity Governance Provisioning Connector versions that you can deploy and use depending Oracle® Identity Governance version that you are using.



#### Note

Oracle® Identity Governance release 11.1.x, is not supported by this connector.

If you are using Identity Governance 12c (12.2.1.4.0) and want to integrate it the target system, then use the latest 12.2.1.x version of this connector and deploy it using either the **Applications** option on the **Manage** tab of Identity Self Service or the **Manage Connector** option in Oracle® Identity System Administration.

If you are using Identity Governance 12c (12.2.1.3.0) and want to integrate it the target system, then use the latest 12.2.1.x version of this connector and deploy it using either the **Applications** option on the **Manage** tab of Identity Self Service or the **Manage Connector** option in Oracle® Identity System Administration.

## About the Keycloak Realm Connector

Below provides the list of features supported by the *AOB* application and *CI*-based connector.

Feature	AOB	CI
Account Full Reconciliation	Yes	Yes
Account Incremental Reconciliation	Yes	Yes
Account Limited Reconciliation	Yes	Yes
Account Delete Reconciliation	Yes	Yes
Realm Role Reconciliation	Yes	Yes
Client Role Reconciliation	Yes	Yes
Group Reconciliation	Yes	Yes
Secure Communication	Yes	Yes
Test connection	Yes	No
Connector Server	Yes	Yes

Table 3. Supported features per connector deployment

## Certified Languages

The connector supports the following languages:

- English
- French
- German

## Connector Architecture

With the connector you can manage user accounts on the target system. Account management is also known as target resource management.

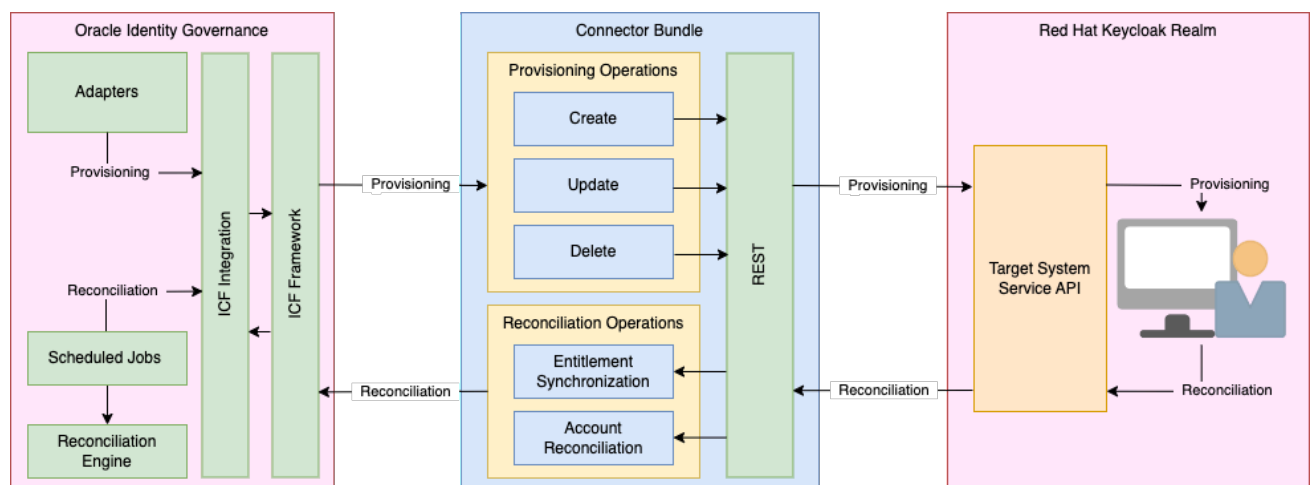


Figure 1. Connector Architecture

## About the Keycloak Realm Connector

As shown in this figure, the backend of Red Hat Keycloak Realm is configured as a target resource by Oracle® Identity Governance. Provisioning, performed in Oracle® Identity Governance, creates and updates accounts for identities on the target system. Through the reconciliation, account data that is created and updated directly on the target system is fetched in Oracle® Identity Governance and saved against the corresponding identities.

The Identity Governance Provisioning Connector is implemented by using the Identity Connector Framework (ICF). ICF is a component that is required to use Identity Connectors and provides basic reconciliation and provisioning operations that are common to all Identity Governance connectors. In addition, ICF offers general functions that developers would otherwise have to implement themselves, e.g. connection pooling, buffering, timeouts and filtering. The ICF is shipped along with Identity Governance. Therefore, you need not configure or modify the ICF.

The Identity Governance Provisioning Connector uses REST to access the target system.

This connector supports Account Management only. This mode of the connector enables the following operations:

### Provisioning

Provisioning involves creating, updating, or deleting users on the target system through Oracle® Identity Governance. When you allocate (or provision) a target system resource to an identity, the operation results in the creation of an account on the target system for that identity. In the Oracle® Identity Governance context, the term "provisioning" is also used to mean updates (for example enabling or disabling) made to the target system account through Oracle® Identity Governance.

Before you can provision users to the required groups or tenants on the target system, you must fetch into Oracle® Identity Governance the list of all groups and tenants used on the target system. This is achieved by using the IGS Role Lookup Reconciliation and IGS Tenant Lookup Reconciliation scheduled jobs for lookup synchronization.

### Reconciliation

During the target resource reconciliation, data on newly created and changed user accounts in the target system are compared and linked to existing identities and provisioned resources. To perform target resource reconciliation, scheduled jobs are used. The connector applies filters to locate users to be reconciled from the target system and then fetches the attribute values of these users.

## Supported Operations

These are the operations that the connector supports for your target system:

- [Account Management](#)
- [Entitlement Management](#)

### Account Management

Operation	Supported?
Create Account	Yes
Modify Account	Yes

## About the Keycloak Realm Connector

Operation	Supported?
Delete Account	Yes
Enable Account	Yes
Disable Account	Yes
Reset Password	No

Table 4. Supported operations on accounts

## Entitlement Management

Operation	Supported?				
	Create	Modify	Delete	Assign	Revoke
Group	No	No	No	Yes	yes
Client Role	No	No	No	Yes	yes
Realm Role	No	No	No	Yes	yes

Table 5. Supported operations on entitlements

## Connector Features

The features of the connector include support for connector server, support for high-availability configuration of the target system, connection pooling, reconciliation of deleted user records, support for groovy scripts, and so on.

- [Full and Incremental Reconciliation](#)
- [Limited Reconciliation](#)
- [Reconciliation of Deleted User Records](#)
- [Lookup Fields Synchronized with the Target System](#)
- [Support for the Connector Server](#)
- [Support for Running Pre and Post Action Scripts](#)
- [Transformation of Account Data](#)
- [Secure Communication to the Target System](#)
- [Connection Pooling](#)
- [Support for High-Availability Configuration of the Target System](#)

## Full and Incremental Reconciliation

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

## About the Keycloak Realm Connector

After you create the application, you can perform full reconciliation to bring all existing user data from the target system to Oracle® Identity Governance. After the first full reconciliation run, incremental reconciliation is automatically enabled. In incremental reconciliation, user accounts that have been added or modified since the last reconciliation run are fetched into Oracle® Identity Governance.

After you create the application, you can first perform full reconciliation. After the first full reconciliation run, incremental reconciliation is automatically enabled.

### Limited Reconciliation

You can set a reconciliation filter as the value of the Filter attribute of a reconciliation scheduled job. This filter specifies the subset of added and modified target system records that must be reconciled.

### Reconciliation of Deleted User Records

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

For more information about the reconciliation job used for reconciling these deleted records, see one of the following sections: [User Reconciliation Job](#)

### Lookup Fields Synchronized with the Target System

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Country lookup field to select a country from the list of countries in the lookup field.

When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are created in Oracle® Identity Governance. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle® Identity Governance.

For more information about the reconciliation job used for reconciling lookup definitions, see one of the following sections: [Reconciliation Jobs for Lookup Field Synchronization](#)

### Support for the Connector Server

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

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

For information about installing, configuring, and running the Connector Server, and then installing the connector in a Connector Server, see [Using an Identity Connector Server](#) in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

### Support for Running Pre and Post Action Scripts

You can run pre and post action scripts on a computer where the connector is deployed. These scripts can be of type SQL/StoredProc/Groovy. You can configure the scripts to run before or after the create, update, or delete an account provisioning operations.

## About the Keycloak Realm Connector

For more information, see [Updating the Provisioning Configuration](#) in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

### Transformation of Account Data

You can configure transformation 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*.

### Secure Communication to the Target System

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

If you do not configure TLS/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](#).

### Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle® Identity Governance connectors can use these connections to communicate with target systems.

At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

One connection pool is created for each set of basic configuration parameters that you provide while creating an application. For example, if you have three applications for three installations of the target system, then three connection pools will be created, one for each target system installation.

For more information about the parameters that you can configure for connection pooling, see: [insert link](#)

### Support for High-Availability Configuration of the Target System

You can configure the connector for compatibility with high-availability target system environments.

The connector can read information about backup target system hosts from the failover parameter of the Basic Configuration section and apply this information when it is unable to connect to the primary host

For more information about the Failover parameter, see [insert link](#).

# Creating a Keycloak Realm Application

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

- [Process Flow for Creating an Application](#)
- [Prerequisites for Creating an Application](#)
- [Creating an Application](#)

## Process Flow for Creating an Application

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



## Creating a Keycloak Realm Application

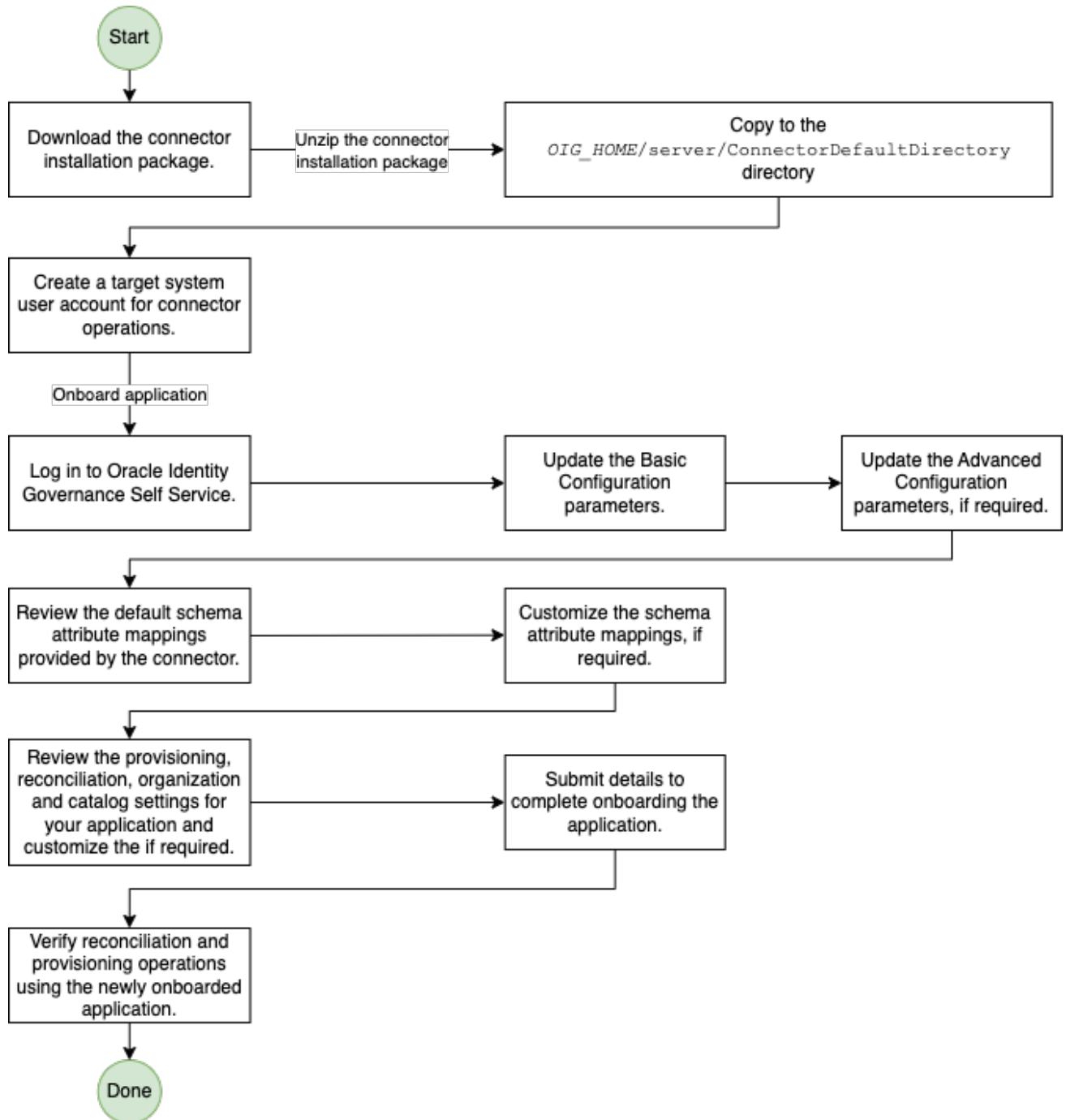


Figure 2. Overall Flow of the Process for Creating an Application By Using the Connector

## Prerequisites for Creating an Application

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

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

## Configuring the Target System

Configuring the target system involves registering a client so that the connector can access Red Hat Keycloak REST APIs. It also involves creating a user account, and assigning specific roles to the user. It is also necessary to adjust some settings at the realm level. This includes:

- [Registering a client](#)
- [Configure the realm](#)



### Important

Everything must be done as superadmin in the target realm.

Log in to admin console as superadmin.

Be sure to be in the **<target>** realm as the target.

### Registering a client

- [Creating an OpenID Connect client](#)
- [Capability Configuration](#)
- [Login Settings](#)
- ???

### Creating an OpenID Connect client

To protect an application that uses the OpenID connect protocol, you create a client.

1. In the navigation panel select **Clients**.
2. Click on **Create client** to create a new client.
3. Create a new client with the properties below:

Property	Value
Client type	OpenID Connect
Client ID	igaadmin
Name	Identity Governance Administration
Description	Identity Governance Administration
Always display in UI	Off

Click on **Next**.

This action bring you to the [Capability Configuration](#) tab, where you can perform capability configuration.

### Capability Configuration

Property	Value	Description
Client authentication	On	This defines the type of the OIDC client. When it's ON, the OIDC type is set to confidential access type. When it's OFF, it is set to public access type.
Authorization	On	Enable/Disable fine-grained authorization support for a client.
Standard flow	<unchecked>	
Implicite flow	<unchecked>	This enables support for OpenID Connect redirect based authentication without authorization code. In terms of OpenID Connect or OAuth2 specifications, this enables support of <i>Implicit Flow</i> for this client.
Device Authorization Grant	<unchecked>	This enables support for OAuth 2.0 Device Authorization Grant, which means that client is an application on device that has limited input capabilities or lack a suitable browser.
OIDC CIBA Grant	<unchecked>	This enables support for OIDC CIBA Grant, which means that the user is authenticated via some external authentication device instead of the user's browser.
Direct access grants	<unchecked>	This enables support for Direct Access Grants, which means that client has access to username/password of user and exchange it directly with Keycloak Realm for access token. In terms of OAuth2 specification, this enables support of <i>Resource Owner Password Credentials Grant</i> for this client.
Service accounts roles	<checked>	Allows you to authenticate this client to Keycloak Realm and retrieve access token dedicated to this client. In terms of OAuth2 specification, this enables support of <i>Client Credentials Grant</i> for this client.

Click on **Next**.

This action bring you to the [Login Settings](#) tab, where you can perform login configuration.

### Login Settings

On this tab nothing have to be configured.

Click on **Save** to create the client.

This action bring you to the **Client details** page, where you can perform permission configuration.

### **Managing Service Account Roles**

In the **Client details** page switch to the tab **Service accounts roles**.

Each realm has a built-in client called `realm-management`. This client defines client-level roles that specify permissions that can be granted to manage the realm.

Assign following roles to the user:

Tag	Name	Description
realm-management	view-realm	
realm-management	query-realm	may be not sure
realm-management	query-groups	may be not sure
realm-management	view-clients	
realm-management	query-clients	may be not sure
realm-management	view-users	
realm-management	query-users	
realm-management	manage-users	
realm-management	view-authorization	
realm-management	manage-authorization	
realm-management	manage-identity-providers	

### **Configure the realm**

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

- [General](#)
- [Login](#)
- [User registration](#)

Navigate to **Realm settings**.

#### **General**

In the **Realm details** page switch to the tab **General**.

Ensure the option **User-managed access** is switched off.

#### **Login**

In the **Realm details** page switch to the tab **Login**.

Ensure the option **Login with email** is switched off.

### **User registration**

In the **Realm details** page switch to the tab **User registration**.

Ensure the **Default role** option **managed account** is not assigned by default.

### **Downloading the Connector Installation Package**

## **Creating an Application**

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

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



#### **Note**

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

# Configuring the Keycloak Realm Connector

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

This section contains the following topics:

- [Basic Configuration Parameters](#)
- [Advanced Setting Parameters](#)
- [Attribute Mappings](#)
- [Correlation Rules](#)
- [Reconciliation Jobs](#)

## Basic Configuration Parameters

These are the connection-related parameters that Oracle® Identity Governance requires to connect to the Keycloak Realm target application.

Parameter	Mandatory?	Description
Server Name	yes	Enter the host name or the IP address of the target system. <b>Sample value:</b> myhost or 192.0.2.10
Server Port	yes	Enter the port number to connect to the target system. <b>Sample value:</b> 443
Server Feature	yes	The advanced feature configuration of this IT resource. <b>Sample value:</b> /metadata/ocs-features-configuration/gws/rkc-feature.xml
Secure Socket	yes	This parameter specifies whether communication with the target system must be secured using SSL.  By default, this field is blank. Enter <code>true</code> if you want to configure SSL between the Connector Server or Oracle® Identity Governance and the target system. Otherwise, enter <code>true</code> . <b>Default value:</b> false
Connector Server	no	By default, this field is blank. If you use a Connector Server, then enter the name of Connector Server IT resource.
Root Context	yes	Enter the base contexts for operations on the target system. <b>Sample value:</b> /rest/api/2
Accept Type	yes	Enter the base contexts for operations on the target system.

## Configuring the Keycloak Realm Connector

Parameter	Mandatory?	Description
		<b>Default value:</b> <code>application/json</code>
Content Type	yes	Enter the base contexts for operations on the target system. <b>Default value:</b> <code>application/json</code>
Authentication Scheme	yes	<b>Sample value:</b> <code>basic-preemptive</code>
Client Identifier	yes	Enter the user name for authenticating the principal on the target system. <b>Sample value:</b> <code>admin</code>
Client Secret	yes	Enter the credential for authenticating the client on the target system. <b>Sample value:</b> <code>admin</code>
Principal Name	yes	Enter the user name for performing operations on the target system. <b>Sample value:</b> <code>admin</code>
Principal Password	yes	Enter the credential for performing operations on the target system. <b>Sample value:</b> <code>Welcome1</code>
Resource Owner	yes	Enter the user name for authenticating the client on the target system. <b>Sample value:</b> <code>admin</code>
Resource Credential	yes	Enter the credential for authenticating the client on the target system. <b>Sample value:</b> <code>admin</code>
Locale Language	yes	<b>Default value:</b> <code>en</code>
Locale Country	yes	<b>Default value:</b> <code>US</code>
Locale TimeZone	yes	<b>Default value:</b> <code>+01:00</code>
Connection Timeout	yes	<b>Default value:</b> <code>1000</code>
Response Timeout	yes	<b>Default value:</b> <code>10000</code>

Table 6. Basic Configuration Parameters for RKC

## Advanced Setting Parameters

The advanced setting parameters for the Keycloak Realm configuration vary depending on whether you are creating a target application or an authoritative application.



### Note

The connector does not support reconciliation for an Authoritative Application.

These are the configuration-related entries that the connector uses during reconciliation and provisioning operations. You can update these values for the target systems, as specified in the [Table 7](#).

Parameter	Mandatory?	Description
bundle-entry	yes	Name of the connector class. <b>Default value:</b> <code>oracle.iam.identity.icf.connector.keycloak.Main</code>
bundle-name	yes	Name of the connector bundle package. <b>Default value:</b> <code>rkc.identity.connector.bundle</code>
bundle-version	yes	Version of the connector bundle class. <b>Default value:</b> <code>12.2.1.3</code>
fetch-schema	yes	Specifies whether the schema must be read from the server. <b>Default value:</b> <code>false</code>
enforce-rfc9110	yes	

Table 7. Advanced Settings Parameters for a Target Application for RKV

## Attribute Mappings

The attribute mappings on the Schema page vary depending on whether you are creating a target application or a authoritative application.



### Note

The connector does not support reconciliation for an Authoritative Application.

## User Account Attributes

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 8](#) lists the user-specific attribute mappings between the process form fields in Oracle® Identity Governance and target system 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*.

Display Name	Target	Type	Required	Provi- sioning	Recon- cilation	Key Field
Identifier	id	String	yes	yes	yes	no



## Configuring the Keycloak Realm Connector

Display Name	Target	Type	Required	Provi- sioning	Recon- cilation	Key Field
User Name	userName	String	yes	yes	yes	no
Password	credential.password	String	yes	yes	no	no
Last Name	lastName	String	yes	yes	yes	no
First Name	firstName	String	yes	yes	yes	no
e-Mail	email	String	yes	yes	yes	no
Verified	emailVerified	String	yes	yes	yes	no
Telephone Number	attribute.phone	String	yes	yes	yes	no
Mobile Number	attribute.mobile	String	yes	yes	yes	no
Verify e-Mail	action.emailVerify	String	yes	yes	yes	no
Verify Profile	action.profileVerify	String	yes	yes	yes	no
Update Profile	action.profileUpdate	String	yes	yes	yes	no
Update Password	action.passwordUpdate	String	yes	yes	yes	no
Update Locale	action.localeUpdate	String	yes	yes	yes	no

Table 8. Default Attribute Mappings for Keycloak Realm Account

### Group Entitlement Attributes

[Table 9](#) lists the attribute mappings for Group entitlement between the process form fields in Oracle Identity Governance and target system attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

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

Display Name	Target	Type	Required	Provi- sioning	Recon- cilation	Key Field
Group Name	groups	String	no	yes	yes	yes

Table 9. Default Attribute Mappings for Keycloak Realm Account

### Client Role Entitlement Attributes

[Table 10](#) lists the attribute mappings for Client Role entitlement between the process form fields in Oracle Identity Governance and target system attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

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

## Configuring the Keycloak Realm Connector

Display Name	Target	Type	Required	Provi- sioning	Recon- cilation	Key Field
Group Name	clientRoles	String	no	yes	yes	yes

Table 10. Default Attribute Mappings for Keycloak Realm Account

### Realm Role Entitlement Attributes

[Table 11](#) lists the attribute mappings for Realm Role entitlement between the process form fields in Oracle Identity Governance and target system attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

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

Display Name	Target	Type	Required	Provi- sioning	Recon- cilation	Key Field
Role Name	realmRoles	String	no	yes	yes	yes

Table 11. Default Attribute Mappings for Keycloak Realm Account

### Correlation Rules

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



#### Note

The connector does not support reconciliation for an Authoritative Application.

### Predefined Identity Correlation Rules

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

[Table 12](#) lists the default simple correlation rule for RKC. 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 Reconciliation Rule** in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

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

Table 12. Predefined Identity Correlation Rule for RKC

In the first correlation rule element:

## Configuring the Keycloak Realm Connector

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

In the second correlation rule element:

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

### Predefined Situations and Responses

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

Table 13 lists the default situations and responses for an RKC 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 **Creating a Target Application** in *Updating Identity Reconciliation Rule in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Situation	Response
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Table 13. Predefined Situations and Responses for an RKC Target Application

### Reconciliation Jobs



#### Note

The connector does not support reconciliation for an Authoritative Application.

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

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*.

### Account Reconciliation Jobs

The following scheduled jobs are available for reconciling accounts:

- [User Account Reconciliation](#)  
Use this reconciliation job to reconcile user data from a Target application. Use this job if either of the following conditions is true:
  - You want to perform Full or Incremental Reconciliation.

## Configuring the Keycloak Realm Connector

- Your target system supports the modifyTimestamp attribute.
- [User Delete Reconciliation](#)  
Use this reconciliation job to reconcile user records that are deleted from a Target application.

### **User Account Reconciliation**

Table 14 describes the parameters of User Account Reconciliation job.

Attribute	Description
IT Resource	The IT Resource used to establish the connection to the Keycloak Realm.  Do not modify this value.
Reconciliation Object	The Name of the Resource Object you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application.  Do not modify this value.
Reconciliation Descriptor	The path to the descriptor which specifies the mapping between the incoming field names and the reconciliation fields of the object to reconcile  Do not modify this value.
Search Filter	Enter the search filter for fetching user records from the target system during a reconciliation run.  <b>Sample:</b>
Ignore Duplicates	Select the option <b>Yes</b> to prevent event creation and processing of Keycloak Realm data that already exists in Identity Governance; otherwise select option <b>No</b> .  <b>Default:</b> <b>Yes</b>
Batch Size	Specifies the size of a batch read from the Service Provider.  <b>Default:</b> <b>500</b>
Thread Pool Size	Specifies that how many threads this task should create to distribute the workload.  <b>Default:</b> <b>10</b>
Last Reconciled	The parameter holds the value of the target system column that is specified as the value of the Incremental Recon Attribute parameter. The <i>Last Reconciled</i> parameter is used for internal purposes.  <b>Default:</b> <b>0</b>

## Configuring the Keycloak Realm Connector

Attribute	Description
Gather Only	Select the option <code>Yes</code> if the data should only be gathered from the Keycloak Realm; otherwise select option <code>No</code> .  <b>Default:</b> <code>No</code>

Table 14. Job parameters for RKC Target Application

### User Reconciliation Job

Table 15 describes the parameters of Target User Delete Reconciliation job.

Attribute	Description
IT Resource	The IT Resource used to establish the connection to the Keycloak Realm.  Do not modify this value.
Reconciliation Object	The Name of the Resource Object you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application.  Do not modify this value.
Reconciliation Descriptor	The path to the descriptor which specifies the mapping between the incoming field names and the reconciliation fields of the object to reconcile  Do not modify this value.
Search Filter	Enter the search filter for fetching user records from the target system during a reconciliation run.  <b>Sample:</b>
Ignore Duplicates	Select the option <code>Yes</code> to prevent event creation and processing of Keycloak Realm data that already exists in Identity Governance; otherwise select option <code>No</code> .  <b>Default:</b> <code>Yes</code>
Batch Size	Specifies the size of a batch read from the Service Provider.  <b>Default:</b> <code>500</code>
Thread Pool Size	Specifies that how many threads this task should create to distribute the workload.  <b>Default:</b> <code>10</code>
Last Reconciled	The parameter holds the value of the target system column that is specified as the value of the Incremental Recon Attribute parameter. The <i>Last Reconciled</i> parameter is used for internal purposes.  <b>Default:</b> <code>0</code>

## Configuring the Keycloak Realm Connector

Attribute	Description
Gather Only	Select the option <code>Yes</code> if the data should only be gathered from the Keycloak Realm; otherwise select option <code>No</code> .  <b>Default:</b> <code>No</code>

Table 15. Job parameters for RKC Delete Reconciliation

### Reconciliation Jobs for Lookup Field Synchronization

The following scheduled jobs available used for reconciling entitlements:

- [Group Entitlement Synchronization](#)  
Use this job to search for and reconcile all group data in the target system into lookup fields in Oracle® Identity Governance.
- [Client Role Entitlement Synchronization](#)  
Use this job to search for and reconcile all client roles data in the target system into lookup fields in Oracle® Identity Governance.
- [Realm Role Entitlement Synchronization](#)  
Use this job to search for and reconcile all realm roles data in the target system into lookup fields in Oracle® Identity Governance.

### Group Entitlement Synchronization

Table 16 describes the parameters of the scheduled jobs.

Attribute	Description
IT Resource	The IT Resource used to establish the connection to the Keycloak Realm.  <b>Default value:</b> <code>RKC.Endpoint</code>
Lookup Group	The value written to Lookup Group in case the operation on a particular Lookup Definition has to create it.  <b>Default value:</b> <code>RKC</code>  Do not modify this value.
Reconciliation Object	The name of the lookup definition in Oracle® Identity Governance that must be populated with values fetched from the target system.  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 parameter.  <b>Default value:</b> <code>RKC.Group</code>
Reconciliation Source	The identifier of the source (aka ObjectClass) that has to be used to reconcile.

## Configuring the Keycloak Realm Connector

Attribute	Description
	<b>Default value:</b> <code>Group</code> Do not modify this value.
Reconciliation Operation	The operation to perform on the object to reconcile. Has to be either <code>Refresh</code> or <code>Update</code> Has to be either <code>Refresh</code> or <code>Update</code> . <b>Default value:</b> <code>Update</code>
Encoded Value	The name of the connector or target system attribute that the connector uses to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name parameter). <b>Default:</b> <code>__UID__</code> Do not modify this value.
Decoded Value	The name of the connector or target system attribute that the connector uses to populate the Decode column of the lookup definition (specified as the value of the Lookup Name parameter). <b>Default:</b> <code>__NAME__</code> Do not modify this value.
Last Reconciled	The parameter holds the value of the target system column that is specified as the value of the Incremental Recon Attribute parameter. The <i>Last Reconciled</i> parameter is used for internal purposes. <b>Default:</b> <code>0</code>
Gather Only	Select the option <code>Yes</code> if the data should only be gathered from the Keycloak Realm; otherwise select option <code>No</code> . <b>Default:</b> <code>No</code>
Batch Size	Specifies the size of a batch read from the Service Provider. <b>Default:</b> <code>500</code>
Entitlement Prefix Required	Select the option <code>Yes</code> if the entitlements loaded needs to be prefixed with the internal system identifier and/or the name of the IT Resource; otherwise select option <code>No</code> . <b>Default:</b> <code>Yes</code> Do not modify this value.
Dependent Job	Specifies the name of the Job that will be started by this Job on successfully completion.

Table 16. Job parameters for Group Entitlement Synchronization

## Configuring the Keycloak Realm Connector

### *Client Role Entitlement Synchronization*

Table 17 describes the parameters of the scheduled job.

Attribute	Description
IT Resource	<p>The IT Resource used to establish the connection to the Keycloak Realm.</p> <p><b>Default value:</b> <code>RKC.Endpoint</code></p>
Lookup Group	<p>The value written to Lookup Group in case the operation on a particular Lookup Definition has to create it.</p> <p><b>Default value:</b> <code>RKC</code></p> <p>Do not modify this value.</p>
Reconciliation Object	<p>The name of the lookup definition in Oracle® Identity Governance that must be populated with values fetched from the target system.</p> <p>If you create a copy of any of these lookup definitions, then enter the name of that new lookup definition as the value of the Lookup Name parameter.</p> <p><b>Default value:</b> <code>RKC.Client Role</code></p>
Reconciliation Source	<p>The identifier of the source (aka ObjectClass) that has to be used to reconcile</p> <p><b>Default value:</b> <code>ClientRole</code></p> <p>Do not modify this value.</p>
Reconciliation Operation	<p>The operation to perform on the object to reconcile. Has to be either Refresh or Update</p> <p>Has to be either <code>Refresh</code> or <code>Update</code>.</p> <p><b>Default value:</b> <code>Update</code></p>
Encoded Value	<p>The name of the connector or target system attribute that the connector uses to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name parameter).</p> <p><b>Default:</b> <code>__UID__</code></p> <p>Do not modify this value.</p>
Decoded Value	<p>The name of the connector or target system attribute that the connector uses to populate the Decode column of the lookup definition (specified as the value of the Lookup Name parameter).</p> <p><b>Default:</b> <code>__NAME__</code></p> <p>Do not modify this value.</p>



## Configuring the Keycloak Realm Connector

Attribute	Description
Last Reconciled	<p>The parameter holds the value of the target system column that is specified as the value of the Incremental Recon Attribute parameter. The <i>Last Reconciled</i> parameter is used for internal purposes.</p> <p><b>Default:</b> 0</p>
Gather Only	<p>Select the option <code>Yes</code> if the data should only be gathered from the Keycloak Realm; otherwise select option <code>No</code>.</p> <p><b>Default:</b> <code>No</code></p>
Batch Size	<p>Specifies the size of a batch read from the Service Provider.</p> <p><b>Default:</b> 500</p>
Entitlement Prefix Required	<p>Select the option <code>Yes</code> if the entitlements loaded needs to be prefixed with the internal system identifier and/or the name of the IT Resource; otherwise select option <code>No</code>.</p> <p><b>Default:</b> <code>Yes</code></p> <p>Do not modify this value.</p>
Dependent Job	<p>Specifies the name of the Job that will be started by this Job on successfully completion.</p>

Table 17. Job parameters for Client Role Entitlement Synchronization

### Realm Role Entitlement Synchronization

Table 18 describes the parameters of the scheduled job.

Attribute	Description
IT Resource	<p>The IT Resource used to establish the connection to the Keycloak Realm.</p> <p><b>Default value:</b> <code>RKC.Endpoint</code></p>
Lookup Group	<p>The value written to Lookup Group in case the operation on a particular Lookup Definition has to create it.</p> <p><b>Default value:</b> <code>RKC</code></p> <p>Do not modify this value.</p>
Reconciliation Object	<p>The name of the lookup definition in Oracle® Identity Governance that must be populated with values fetched from the target system.</p> <p>If you create a copy of any of these lookup definitions, then enter the name of that new lookup definition as the value of the Lookup Name parameter.</p> <p><b>Default value:</b> <code>RKC.Realm Role</code></p>

## Configuring the Keycloak Realm Connector

Attribute	Description
Reconciliation Source	<p>The identifier of the source (aka ObjectClass) that has to be used to reconcile</p> <p><b>Default value:</b> <code>RealmRole</code></p> <p>Do not modify this value.</p>
Reconciliation Operation	<p>The operation to perform on the object to reconcile. Has to be either Refresh or Update</p> <p>Has to be either <code>Refresh</code> or <code>Update</code>.</p> <p><b>Default value:</b> <code>Update</code></p>
Encoded Value	<p>The name of the connector or target system attribute that the connector uses to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name parameter).</p> <p><b>Default:</b> <code>__UID__</code></p> <p>Do not modify this value.</p>
Decoded Value	<p>The name of the connector or target system attribute that the connector uses to populate the Decode column of the lookup definition (specified as the value of the Lookup Name parameter).</p> <p><b>Default:</b> <code>__NAME__</code></p> <p>Do not modify this value.</p>
Last Reconciled	<p>The parameter holds the value of the target system column that is specified as the value of the Incremental Recon Attribute parameter. The <i>Last Reconciled</i> parameter is used for internal purposes.</p> <p><b>Default:</b> <code>0</code></p>
Gather Only	<p>Select the option <code>Yes</code> if the data should only be gathered from the Keycloak Realm; otherwise select option <code>No</code>.</p> <p><b>Default:</b> <code>No</code></p>
Batch Size	<p>Specifies the size of a batch read from the Service Provider.</p> <p><b>Default:</b> <code>500</code></p>
Entitlement Prefix Required	<p>Select the option <code>Yes</code> if the entitlements loaded needs to be prefixed with the internal system identifier and/or the name of the IT Resource; otherwise select option <code>No</code>.</p> <p><b>Default:</b> <code>Yes</code></p> <p>Do not modify this value.</p>

## Configuring the Keycloak Realm Connector

Attribute	Description
Dependent Job	Specifies the name of the Job that will be started by this Job on successfully completion.

Table 18. Job parameters for Realm Role Entitlement Synchronization

# Performing Tasks for the Keycloak Realm Connector

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

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

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

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

### 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.

## Updating with a New UI 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

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*.

## 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*.

## 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 for Lookup Field Synchronization](#).
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

See Also

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

## Managing Logging

The following topics provide detailed information about logging:

- [Understanding Log Levels](#)
- [Enabling Logging](#)

### Understanding Log Levels

This section describes Log Levels for the connector, by:

- [Diagnostic Logging Log Levels](#)
- [Connector Server Log Levels](#)

### *Diagnostic Logging Log Levels*

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

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. Oracle® Identity Governance uses Oracle® Diagnostic Logging (ODL) for logging.

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:

## Performing Tasks for the Keycloak Realm Connector

Level	Description
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.

Table 19. Diagnostic Logging Log Levels

These message types are mapped to ODL message type and level combinations as shown in Table 4-1.

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	TRACE1
FINER	TRACE16
FINEST	TRACE32

Table 20. Log Levels and ODL Message Type:Level Combinations

The configuration file for ODL 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 and server names specified during the installation of Oracle Identity Governance.

### Connector Server Log Levels

The `conf` directory contains the `logging.properties` file, which you can edit to meet your requirements.

The following topics provide detailed information about logging:

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.

## Performing Tasks for the Keycloak Realm Connector

Level	Description
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.

Table 21. Log Levels

### Enabling Logging

This section describes how to enable logging for the connector, by:

- [Enabling Logging on Oracle® WebLogic Server](#)
- [Enabling Logging on the Connector Server](#)

#### *Enabling Logging on Oracle® WebLogic Server*

To enable logging on Oracle® WebLogic Server:

1. Edit the `/logging.xml` file as follows:
  - a. Add the following blocks in the file:
  - b. Replace both occurrences of **[LOG-LEVEL]** with the ODL message type and level combination that you require. Table 2-1 lists the supported message type and level combinations.

Similarly, replace **[PATH-TO-LOG-ROOT]** and **[WEBLOGIC-DOMAIN]** 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      ='identity-handler'  
             level     ='[LOG-LEVEL]'  
             class     ='oracle.core.ojdl.logging.ODLHandlerFactory'  
             formatter='oracle.core.ojdl.weblogic.ConsoleFormatter'>  
  <property name='logreader' value='off' />  
  <property name='path'     value='[PATH-TO-LOG-ROOT]/[WEBLOGIC-DOMAIN]  
  <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           ="OCS.RKC.PROVISIONING"  
        level          ="[LOG-LEVEL]"  
        useParentHandlers="false">  
  <handler name="identity-handler" />  
</logger>
```



## Performing Tasks for the Keycloak Realm Connector

```
<logger name          = "OCS.RKC.RECONCILIATION"
       level          = "[LOG-LEVEL]"
       useParentHandlers="false">
  <handler name="identity-handler"/>
</logger>
```

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

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:

**For Microsoft Windows:**

```
set WLS_REDIRECT_LOG=[FILENAME]
```

**For UNIX:**

```
export WLS_REDIRECT_LOG=[FILENAME]
```

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

4. Restart the application server.

### Enabling Logging on the Connector Server

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

To do so:

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

## Localizing Field Labels in UI Forms

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

To localize field label that you add to in UI forms:

## Configuring the Connector Seerver IT Resource

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

## Performing Tasks for the Keycloak Realm Connector

After you create the application for your target system, the connector creates a default IT resource for the Connector Server. The name of this default IT resource is `RKC Connector Server`.

In Oracle® Identity System Administration, search for and edit the RkC Connector Server IT resource to 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*.


Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. <b>Sample:</b> <code>HostName</code>
Key	Enter the key for the Connector Server.
Port	Enter the number of the port at which the Connector Server is listening. <b>Sample:</b> <code>8752</code>
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. <b>Sample:</b> <code>0</code> (recommended value)
Timeout	Enter <code>true</code> to specify that you will configure SSL between Oracle® Identity Governance and the Connector Server. Otherwise, enter <code>false</code> . <b>Default:</b> <code>false</code> <div> <b>Note</b> It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see <i>Configuring SSL for Java Connector Server in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance</i>.</div>

Table 22. IT Resource parameters

## Configuring SSL

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

To configure SSL:

1. Obtain the SSL public key certificate of Keycloak.

## Performing Tasks for the Keycloak Realm Connector

2. Copy the public key certificate of Keycloak 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
```

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 is a sample value for this command:

```
keytool -import -alias serverwl -trustcacerts -file supportcert.pem -keystore cl
```

### **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.
- 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.

# Using the RKC Provisioning Connector

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

The following topics are discussed in this chapter:

- [Configuring Reconciliation](#)
- [Configuring Reconciliation Jobs](#)
- [Guidelines on Performing Provisioning Operations](#)
- [Performing Provisioning Operations](#)
- [Uninstalling the Connector](#)



## Note

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

## Configuring Reconciliation

Reconciliation involves duplicating in Oracle® Identity Governance the creation of and modifications to user accounts on the target system.

The following topics related to configuring reconciliation are discussed in this section:

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

## Performing Full and Incremental 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 whenever you want to ensure that all target system records are reconciled in Oracle® Identity Governance.

At the end of the reconciliation run, the `Last Reconciled` parameter of the reconciliation job for user record reconciliation is automatically updated. From the next reconciliation run onward, only records created after this time stamp are considered for reconciliation. This is incremental reconciliation.

You can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle® Identity Governance. To perform a full reconciliation run, remove (delete) any value currently assigned to the `Last Reconciled` and `Search Filter` parameters and run one of the reconciliation jobs listed in the [Reconciliation Jobs](#) section.

For example, consider `createdOn` and `updatedOn` as sample Incremental Recon Attributes associated with the RKC Provisioning Target Resource Account Reconciliation.

## Using the RKC Provisioning Connector

After the first full reconciliation run, the `Last Reconciled` parameter gets populated accordingly. In subsequent reconciliation runs, the connector fetches only the user records that are created or updated after the timestamp.

### Performing Limited Reconciliation

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

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

You can perform limited reconciliation 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.

Consider a filter suffix value: `loginName eq 'JohnDoe'`

In this example, the connector performs filter reconciliation and only reconciles the user information whose `Login Name` is JOHNDOE.

### 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 scheduled jobs for lookup field synchronization and reconciliation.

To configure a scheduled job:

1. Log in to Oracle® Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled 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:

<b>Retries</b>	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</b>	Depending on the frequency at which you want the job to run, select the appropriate schedule type.

## Using the RKC Provisioning Connector

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.

## Guidelines on Performing Provisioning Operations

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

- Before you perform provisioning operations, lookup definitions must be synchronized with the lookup fields of the target system. In other words, scheduled tasks for lookup field synchronization must be run before provisioning operations.

## Performing Provisioning Operations

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

To perform provisioning operations in Oracle® Identity Governance:

1. Log in to Identity Self Service.
2. Create a user as follows:
  - a. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
  - b. From the Actions menu, select **Create**. Alternatively, you can click **Create** on the toolbar. The Create User page is displayed with input fields for user profile attributes.
  - c. Enter details of the user in the Create User page.
3. On the Account tab, click **Request Accounts**.

## Using the RKC Provisioning Connector

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**.



### Note

See Also

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

## Uninstalling the Connector

Uninstalling the RKC Provisioning connector deletes all the account-related data associated with its resource objects.

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

For example: RKC Account



### Note

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

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

# Extending the Functionality of the RKC Connector

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

The following topics are discussed in this section:

- [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*.

Following is a sample transformation script for reference:

```
def attributeFromContext(attributeName) {  
    return (context.beneficiary != null) ? context.beneficiary.getAttribute(attributeName) : null;  
}
```

```
def passwordFromContext() {  
    return context.beneficiaryPassword;  
}
```

```
if (binding.variables != null) {  
    if (binding.variables.containsKey("context")) {  
        if (context.operationType != null && context.operationType.equalsIgnoreCase("create")) {  
            if (context.provisionMechanism != null) {  
                if (context.provisionMechanism.equalsIgnoreCase("POLICY")) {  
                    Login_Name = attributeFromContext("User Login");  
                    First_Name = attributeFromContext("First Name");  
                    Last_Name = attributeFromContext("Last Name");  
                    Display_Name = attributeFromContext("Display Name");  
                }  
                else if (context.provisionMechanism.equalsIgnoreCase("REQUEST")) {  

```



## Extending the Functionality of the RKC Connector

```
if (Login_Name == null || Login_Name == "") {  
    Login_Name = attributeFromContext("User Login");  
}  
if (First_Name == null || First_Name == "") {  
    First_Name = attributeFromContext("First Login");  
}  
if (Last_Name == null || Last_Name == "") {  
    Last_Name = attributeFromContext("Last Login");  
}  
if (Display_Name == null || Display_Name == "") {  
    Display_Name = attributeFromContext("Display Login");  
}  
}  
}  
}  
}
```

## Configuring Action Scripts

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

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

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

## 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.

You must create copies of configurations of your base application to configure it for multiple 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*.

# Connector Model

## Overview

The figure below shows an overview of the data model of the connector.

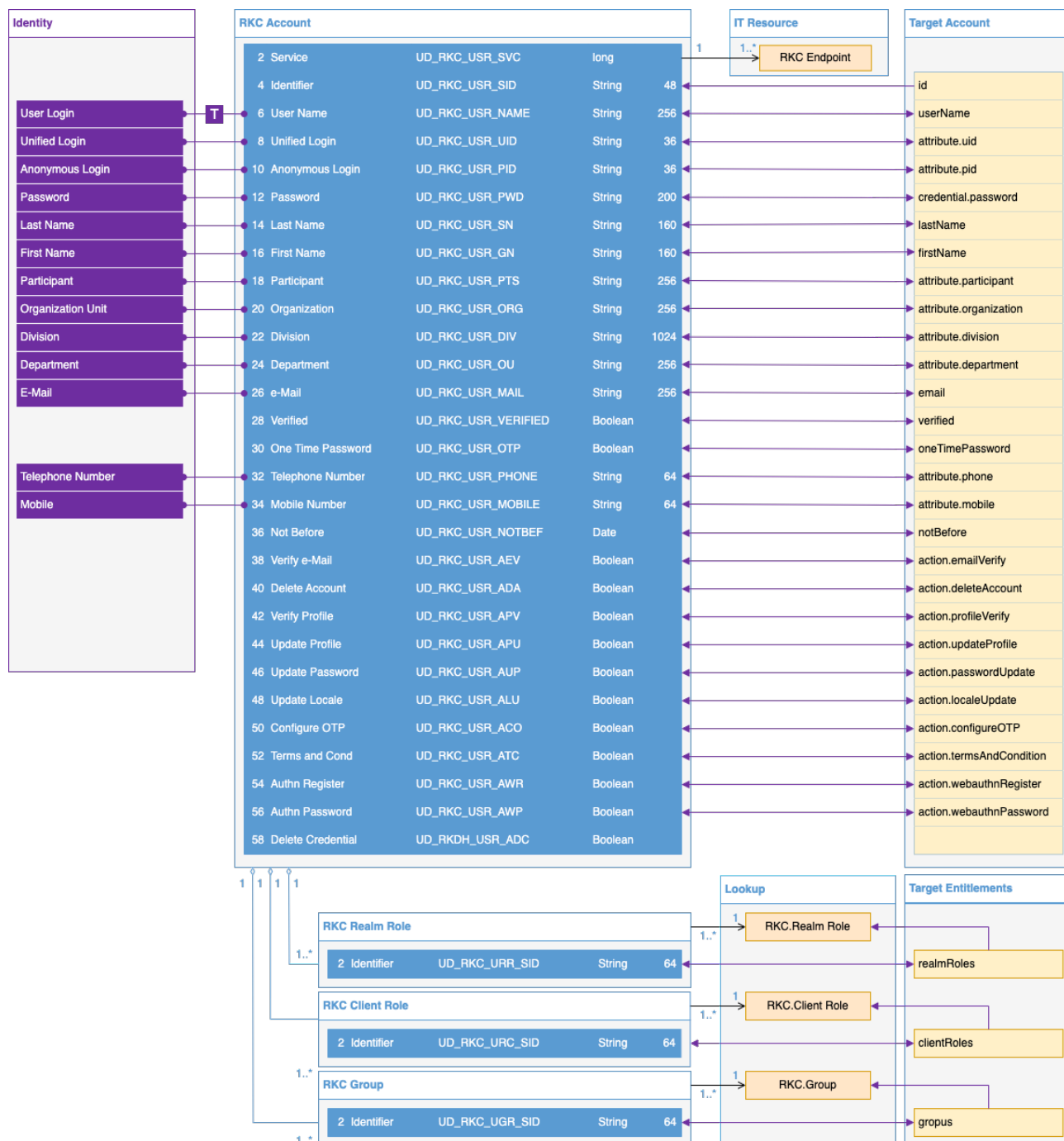


Figure 3. Connector Model

In addition to the [Account](#) data model required by Identity Governance, the data model of the connector supports the storage of roles, global admin roles and scoped adminroles.

- [Groups](#)

- [Client Roles](#)
- [Realm Roles](#)

## Account

The account data are stored in the form UD\_RKC\_USR.

### Attributes

Label	Name	Type	Length
Service	UD_RKC_USR_SVC	long	
Identifier	UD_RKC_USR_SID	String	48
Login Name	UD_RKC_USR_NAME	String	256
Unified Login	UD_RKC_USR_UID	String	36
Password	UD_RKC_USR_PWD	String	200
Last Name	UD_RKC_USR_SN	String	160
First Name	UD_RKC_USR_GN	String	160
Participant	UD_RKC_USR_PTS	String	256
Organization	UD_RKC_USR_ORG	String	256
Division	UD_RKC_USR_DIVISION	String	1024
Department	UD_RKC_USR_OU	String	256
e-Mail	UD_RKC_USR_MAIL	String	256
Verified	UD_RKC_USR_VERIFIED	Boolean	
One Time Password	UD_RKC_USR_OTP	Boolean	
Telephone Number	UD_RKC_USR_PHONE	String	64
Mobile Number	UD_RKC_USR_MOBILE	String	64
Not Before	UD_RKC_USR_NOTBEF	Date	
Verify e-Mail	UD_RKC_USR_AEV	Boolean	
Delete Account	UD_RKC_USR_ADA	Boolean	
Verify Profile	UD_RKC_USR_APV	Boolean	
Update Profile	UD_RKC_USR_APU	Boolean	
Update Password	UD_RKC_USR_AUP	Boolean	
Update Locale	UD_RKC_USR_ALU	Boolean	
Configure OTP	UD_RKC_USR_ACO	Boolean	
Terms and Cond	UD_RKC_USR_ATC	Boolean	

Label	Name	Type	Length
Authn Register	UD_RKC_USR_AWR	Boolean	
Authn Password	UD_RKC_USR_AWP	Boolean	
Delete Credential	UD_RKDH_USR_ADC	Boolean	

Table 23. Attributes stored in the form UD\_RKC\_USR

## Prepopulation

Rules are implemented for some of the attributes described above, which derive values for such an attribute from the profile of an identity the account belongs to.

Label	Adapter	Rule
User Name	OCS PrePopulate String Converted	Derives the value from <i>User Definition</i> attribute <b>User Login</b> and converts it to lower case.
Unified Login	OCS PrePopulate String	Derives the value from <i>User Definition</i> attribute <b>uniqueIdentifier</b> .
Password	OCS PrePopulate String	Derives the value from <i>User Definition</i> attribute <b>Password</b> .
Last Name	OCS PrePopulate String	Derives the value from <i>User Definition</i> attribute <b>Last Name</b> .
First Name	OCS PrePopulate String	Derives the value from <i>User Definition</i> attribute <b>First Name</b> .
Participant	OCS PrePopulate String	Derives the value from <i>User Definition</i> attribute <b>participant</b> .
Organization	OCS PrePopulate String	Derives the value from <i>User Definition</i> attribute <b>organizationalUnit</b> .
Division	OCS PrePopulate String	Derives the value from <i>User Definition</i> attribute <b>division</b> .
Department	OCS PrePopulate String	Derives the value from <i>User Definition</i> attribute <b>department</b> .
e-Mail	OCS PrePopulate String	Derives the value from <i>User Definition</i> attribute <b>Email Address</b> .
Telephone Number	OCS PrePopulate String	Derives the value from <i>User Definition</i> attribute <b>Telephone Number</b> .
Mobile Number	OCS PrePopulate String	Derives the value from <i>User Definition</i> attribute <b>Mobile</b> .

Table 24. Prepopulation rules applied on the form UD\_RKC\_USR

## Groups

The admin roles assigned to a user account are stored in the UD\_RKC\_UGR form.

## Attributes

Label	Name	Type	Length
Name	UD_RKC_UGR_SID	String	64

Table 25. Attributes stored in the form UD\_RKC\_UGR

## Prepopulation

The form is not subject to any rules for prepopulating values.

## Client Roles

The roles assigned to a user account are stored in the UD\_RKC\_UCR form.

## Attributes

Label	Name	Type	Length
Name	UD_RKC_UCR_SID	String	64

Table 26. Attributes stored in the form UD\_RKC\_UCR

## Prepopulation

The form is not subject to any rules for prepopulating values.

## Realm Roles

The roles assigned to a user account are stored in the UD\_RKC\_UCR form.

## Attributes

Label	Name	Type	Length
Name	UD_RKC_URR_SID	String	64

Table 27. Attributes stored in the form UD\_RKC\_URR

## Prepopulation

The form is not subject to any rules for prepopulating values.