Oracle® Identity Governance

Configuring the ServiceNow Application

12c (12.2.1.3.0)

F12378-03

October 2020

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

F12378-03

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

Primary Author: Gowri.G.R

Contributors: Bhargav Janapati

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

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

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

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

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

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

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

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

Contents

Preface

Audience viii

Documentation Accessibility viii

Related Documents viii

Conventions ix

What's New in this Guide?

Software Updates x

Documentation-Specific Updates x

1 About the ServiceNow Connector

1.1 Certified Components 1-2

1.2 Usage Recommendation 1-3

1.3 Certified Languages 1-3

1.4 Supported Connector Operations 1-4

1.5 Connector Architecture 1-5

1.6 Supported Use Cases 1-7

1.7 Supported Connector Features Matrix 1-8

1.8 Connector Features 1-9

1.8.1 Support for Both Target and Authoritative Applications 1-9

1.8.2 Support for Full and Incremental Reconciliation 1-9

1.8.3 Support for Limited (Filtered) Reconciliation 1-10

1.8.4 Support for the Connector Server 1-10

1.8.5 Transformation and Validation of Account Data 1-10

1.8.6 Support for Cloning Applications and Creating Instance Applications 1-10

1.8.7 Secure Communication to the Target System 1-11

2 Creating an Application by Using the ServiceNow Connector

2.1 Process Flow for Creating an Application By Using the Connector 2-1

2.2 Prerequisites for Creating an Application By Using the Connector 2-3

2.2.1 Configuring the Target System 2-3
2.2.2 Downloading the Connector Installation Package 2-3
2.3 Creating an Application By Using the Connector 2-4

3 Configuring the ServiceNow Connector

3.1 Basic Configuration Parameters 3-1
3.2 Advanced Settings Parameters 3-2
3.2.1 Advanced Settings Parameters for a Target Application 3-3
3.2.2 Advanced Settings Parameters for an Authoritative Application 3-7
3.3 Attribute Mappings 3-8
3.3.1 Attribute Mappings for a Target Application 3-8
3.3.2 Attribute Mappings for an Authoritative Application 3-12
3.4 Correlation Rules 3-13
3.4.1 Correlation Rules, Situations, and Responses for a Target Application 3-14
3.4.2 Correlation Rules, Situations, and Responses for an Authoritative Application 3-16
3.5 Reconciliation Jobs 3-18
3.5.1 Reconciliation Jobs for a Target Application 3-18
3.5.2 Reconciliation Jobs for an Authoritative Application 3-20

4 Performing the Postconfiguration Tasks for the ServiceNow Connector

4.1 Configuring Oracle Identity Governance 4-1
4.1.1 Creating and Activating a Sandbox 4-1
4.1.2 Creating a New UI Form 4-2
4.1.3 Publishing a Sandbox 4-2
4.1.4 Updating an Existing Application Instance with a New Form 4-2
4.2 Harvesting Entitlements and Sync Catalog 4-3
4.3 Managing Logging for the Connector 4-3
4.3.1 Understanding Log Levels 4-4
4.3.2 Enabling Logging 4-5
4.4 Configuring the IT Resource for the Connector Server 4-6
4.5 Localizing Field Labels in UI Forms 4-7
4.6 Configuring SSL for the Connector 4-9

5 Using the ServiceNow Connector

5.1 Configuring Reconciliation 5-1
5.1.1 Performing Full and Incremental Reconciliation 5-1
5.1.2 Performing Limited Reconciliation 5-1

5.2 Configuring Reconciliation Jobs 5-2
5.3 Configuring Provisioning 5-3
5.3.1 Guidelines on Performing Provisioning Operations 5-3
5.3.2 Performing Provisioning Operations 5-3
5.4 Uninstalling the Connector 5-4

6 Extending the Functionality of the ServiceNow Connector

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

7 Upgrading the ServiceNow Connector

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

8 Known Issues and Limitations of the ServiceNow Connector

A Files and Directories in the Connector Installation Package

List of Figures

1-1 Connector Architecture 1-6
2-1 Overall Flow of the Process for Creating an Application By Using the Connector 2-2
3-1 Default Attribute Mappings for ServiceNow User Account 3-10
3-2 Default Attribute Mappings for Role Entitlement 3-11
3-3 Default Attribute Mappings for Groups 3-12
3-4 Default Attribute Mappings for an Authoritative Application 3-13
3-5 Simple Correlation Rule for a ServiceNow Target Application 3-15
3-6 Predefined Situations and Responses for a ServiceNow Target Application 3-16
3-7 Simple Correlation Rule for a ServiceNow Authoritative Application 3-17
3-8 Predefined Situations and Responses for a ServiceNow Authoritative Application 3-17

List of Tables

1-1 Certified Components 1-2

1-2 Supported Connector Operations 1-4

1-3 Supported Connector Features Matrix 1-8

3-1 Basic Configuration Parameters for the ServiceNow Connector 3-1

3-2 Advanced Settings Parameters for a Target Application 3-4

3-3 Advanced Settings Parameters for an Authoritative Application 3-7

3-4 Default Attribute Mappings for ServiceNow User Account 3-9

3-5 Default Attribute Mappings for Role Entitlement 3-11

3-6 Default Attribute Mappings for Groups 3-11

3-7 ServiceNow User Account Schema Attributes 3-12

3-8 Predefined Identity Correlation Rule for a ServiceNow Target Application 3-14

3-9 Predefined Situations and Responses for a ServiceNow Target Application 3-15

3-10 Predefined Identity Correlation Rule for ServiceNow Authoritative Application 3-16

3-11 Predefined Situations and Responses for a ServiceNow Authoritative Application 3-17

3-12 Parameters of the ServiceNow Full User Reconciliation Job 3-18

3-13 Parameters of the Reconciliation Jobs for Lookup Field Synchronization 3-19

3-14 Parameters of the ServiceNow User Trusted Reconciliation Job 3-20

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

4-2 Parameters of the IT Resource for the ServiceNow Connector Server 4-6

A-1 Files and Directories in the Connector Installation Package A-1

Preface

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

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For information about installing and using Oracle Identity Governance 12.2.1.4.0, visit the following Oracle Help Center page:

`https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/index.html`

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

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

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

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

For information about Oracle Identity Manager Connectors 11.1.1 documentation, visit the following Oracle Help Center page:

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
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.

What’s New in this Guide?

These are the updates made to the software and documentation for release 12.2.1.3.0 of Configuring the ServiceNow Application.

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

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

Software Updates

These are the updates made to the connector software.

Software Updates in Release 12.2.1.3.0

The following is the software update in release 12.2.1.3.0:

Support for Onboarding Applications Using the Connector

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

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 12.2.1.3.0

The following documentation-specific update has been made in revision "3" of the guide:

Logger names present in Enabling Logging have been updated.

The following documentation-specific updates have been made in revision "2" of the guide:

- The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to include support for Oracle Identity Governance 12c (12.2.1.4.0).
- The "Connector Patch" row has been added to Table 1-1 to include information about applying patch 29874542 to the ServiceNow connector bundle to create and manage Authoritative applications. As a result, several new topics pertaining

to Authoritative applications have been added throughout the guide and a few existing topics have been updated as follows:
New Topics

- Support for Both Target and Authoritative Applications
- Advanced Settings Parameters for an Authoritative Application
- Attribute Mappings for an Authoritative Application
- Correlation Rules, Situations, and Responses for an Authoritative Application
- Reconciliation Jobs for an Authoritative Application

Updated Topics

- Connector Architecture
- Supported Connector Features Matrix
- Support for Full and Incremental Reconciliation
- Performing Full and Incremental Reconciliation
- Files and Directories in the Connector Installation Package

- The "Connector Server JDK" row of Table 1-1 has been updated to include support for the latest version of JDK.
- Known Issues and Limitations of the ServiceNow Connector has been added to include an issue about removing roles and a limitation that the connector does not support incremental reconciliation.

1 About the ServiceNow 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 ServiceNow connector lets you create and onboard ServiceNow 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 ServiceNow connector:

- Certified Components
- Usage Recommendation
- Certified Languages
- Supported Connector Operations
- Connector Architecture
- Supported Use Cases
- Supported Connector Features Matrix
- Connector Features

Note:

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

1.1 Certified Components

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

Note:

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

Table 1-1 Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Governance: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0)	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0)
Target System	ServiceNow release Eureka or later	ServiceNow release Eureka or later
Connector Server	11.1.2.1.0 or later	11.1.2.1.0 or later
Connector Server JDK	JDK 1.8 or later	JDK 1.8 or later
Connector Patch	If you want to create and manage Authoritative applications for ServiceNow, then you must download and apply patch 29874542, to the ServiceNow connector bundle, from My Oracle Support.	Not applicable

1.2 Usage Recommendation

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

- If you are using Oracle Identity Governance release 12c (12.2.1.3.0) or later, then use the latest 12.2.1.*x* version of this connector. Deploy the connector using the **Applications** option on the **Manage** tab of Identity Self Service.
- If you are using the Oracle Identity Manager release listed in the “Requirement for CI-Based Connector” column in Table 1-1, then use the 11.1.*x* version of this connector. If you want to use the 12.1.*x* version of this connector, then you can install and use it only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12c (12.2.1.3.0) or later.

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

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
Reconcile user	Yes
Update user	Yes
Delete user	Yes
Set password	Yes
Reset password	Yes
Enable user	Yes
Disable user	Yes
Role Grant Management	
Add role	Yes
Add multiple roles	Yes
Remove role	Yes
Remove multiple roles	Yes
Assign single or multiple roles	Yes
Remove single or multiple roles	Yes
Group Management	
Add group	Yes
Add multiple groups	Yes
Remove group	Yes
Remove multiple groups	Yes

Table 1-2 (Cont.) Supported Connector Operations

Operation	Supported
Assign single or multiple groups	Yes
Remove single or multiple groups	Yes

1.5 Connector Architecture

The connector uses ServiceNow APIs to synchronize user attributes between Oracle Identity Governance and ServiceNow directory services, and is implemented using the Identity Connector Framework (ICF) component.

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.

You can configure the connector to run in one of the following modes:

- **Identity reconciliation**

  Identity reconciliation is also known as authoritative or trusted source reconciliation. In this mode, the target system is used as the trusted source and users are directly created and modified on it. During reconciliation, each user record fetched from the target system is compared with existing OIM Users. If a match is found between the target system record and the OIM User, then the OIM User attributes are updated with changes made to the target system record. If no match is found, then the target system record is used to create an OIM User.

- **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**

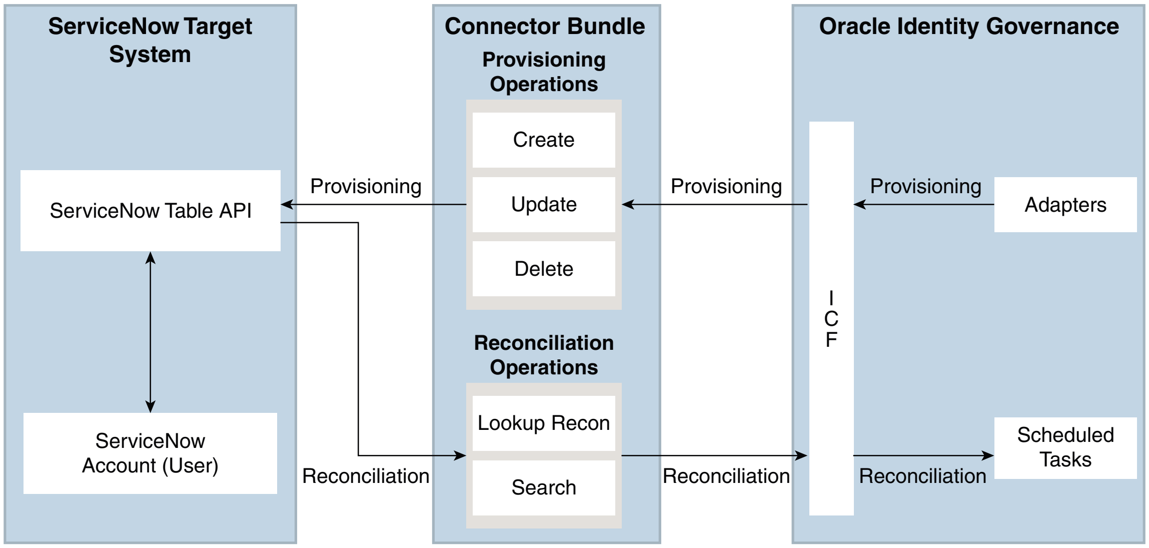
    Provisioning involves creating or updating users on the target system through Oracle Identity Governance. When you allocate (or provision) a ServiceNow resource to the OIM User, the operation results in the creation of an account on ServiceNow for that user. In the Oracle Identity Governancecontext, the term **provisioning** also covers updates made to the target system account through Oracle Identity Governance.

  - **Target resource reconciliation**

    In target resource reconciliation, data related to the newly created and modified target system accounts can be reconciled and linked with existing OIM Users and provisioned resources. You use a scheduled job for performing reconciliation.

Figure 1-1 shows the architecture of the ServiceNow connector.

Figure 1-1 Connector Architecture



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

Through the provisioning operations that are performed on Oracle Identity Governance, accounts are created and updated in the target system for Oracle Identity Governance Users. During provisioning, the Adapters invoke ICF operation, ICF inturn invokes create operation on the ServiceNow Identity Connector Bundle and then the bundle calls the target system API for provisioning operations. The ServiceNow Table 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.

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

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

The ServiceNow Identity Connector Bundle communicates with the ServiceNow Table API using the HTTPS protocol. The ServiceNow Table API provides programmatic access through REST API endpoints. Apps can use the ServiceNow API to perform create, read, update, and delete (CRUD) operations on directory data and directory objects, such as users.

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

1.6 Supported Use Cases

ServiceNow connector is used to integrate OIG with a ServiceNow instance. ServiceNow connector ensures that all ServiceNow accounts are created, updated, deleted, and deactivated on an integrated cycle with the rest of the identity-aware applications in your enterprise. ServiceNow connector standardizes service processes and implements automation to replace manual tasks. In a typical IT scenario, an organization using OIG wants to manage accounts, user association with a role or with a department across a ServiceNow Cloud instance.

As a business use case, consider a leading logistics company in Australia which was using ServiceNow for the ticketing system solution and OIG for identity management. Before using ServiceNow connector, operations such as create, edit, and delete were performed manually and lacked a centralized streamlining operation. These operations can be easily automated using the ServiceNow REST APIs. By integrating ServiceNow connector with Oracle Identity Governance, the logistics company was able to achieve complete automation.

Following are few example scenarios which ServiceNow connector facilitates:

- **ServiceNow User Management**

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

  ServiceNow connector allows new users to self-provision on a ServiceNow Cloud instance. New users can request and provision from a catalog of cloud-based resources.

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

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

- **Entitlement Grant Management**

  - **ServiceNow Groups**

    In ServiceNow context, a group is a collection of users who share a common purpose. Generally, a group will perform tasks such as approving change requests and resolving incidents.

For example, consider a network outage scenario. A Network group with several team members will receive a group notification about the incident. The outage incident task can be assigned to any Network group member for a resolution. The ServiceNow connector integration with OIG provides a request-based policy option. Before using ServiceNow connector, the approver must be an user from the Network group. With ServiceNow integration, the said outage resolution can be automatically assigned to users or groups based on predefined polices. For administrators and users, the ServiceNow connector provides an option to facilitate a request-based group membership assignment or group membership revocation options.

– **ServiceNow Roles**

  In ServiceNow context, a role is an administrator who can create groups and provide access-based permissions to various groups.

  ServiceNow connector manages role memberships. Role memberships provide selective access to ServiceNow functionalities. A user can be a member of one or more roles. Generally, new users are added to a specific role. Each role determines various tasks such as view, update, and delete operations that a ServiceNow user can perform.

  As an example, a user with specific role has the rights to view a change request, however does not have access privileges to approve or reject a change request. A ServiceNow user without a role assignment can perform minimal read and write operations. A ServiceNow user needs to have role access privilege in order to create a group. In large organizations, it may be necessary for an administrator to designate other employees to act as administrators to serve different functions. For example, you can set admin roles for your IT staff that can act as support agents to other employees, partners, customers and vendors. With the ServiceNow connector, you can assign or revoke a ServiceNow admin role to users as an entitlement, thus facilitating you to leverage the delegated administration capability of ServiceNow.

1.7 Supported Connector Features Matrix

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

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application	CI-Based Connector
Perform full reconciliation	Yes	Yes
Perform incremental reconciliation	Yes, only for Authoritative applications	No
Perform limited reconciliation	Yes	Yes
Use connector server	Yes	Yes
Configure validation and transformation of account data	Yes	Yes
Perform connector operations in multiple domains	Yes	Yes

Table 1-3 (Cont.) Supported Connector Features Matrix

Feature	AOB Application	CI-Based Connector
Support for paging	Yes	Yes
Test connection	Yes	No
Reset password	Yes	Yes
Clone applications or create new application instances	Yes	Yes
Provide secure communication to the target system through SSL	Yes	Yes

1.8 Connector Features

The features of the connector include support for connector server, full reconciliation, limited reconciliation, reconciliation of deleted account data, support for cloning applications and creating instance applications, and secure communication to the target system.

- Support for Both Target and Authoritative Applications
- Support for Full and Incremental Reconciliation
- Support for Limited (Filtered) Reconciliation
- Support for the Connector Server
- Transformation and Validation of Account Data
- Support for Cloning Applications and Creating Instance Applications
- Secure Communication to the Target System

1.8.1 Support for Both Target and Authoritative Applications

You can use the connector to create and manage Target applications and Authoritative applications.

> **Note:**
>
> To create and manage Authoritative applications, ensure that you have applied patch 29874542 from My Oracle Support.

1.8.2 Support for 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. You can perform incremental reconciliation only for an Authoritative application.

After you create the application, you can first perform full reconciliation. For an authoritative application, incremental reconciliation is automatically enabled after the first full reconciliation run, if you entered a value for the Incremental Recon Attribute parameter of the ServiceNow User Trusted Reconciliation job.

You can perform a full reconciliation run at any time. See Performing Full and Incremental Reconciliation

1.8.3 Support for Limited (Filtered) Reconciliation

You can reconcile records from the target system based on a specified filter criterion.

You can set a reconciliation filter as the value of the Filter Suffix attribute of the user reconciliation scheduled job. This filter specifies the subset of newly added and modified target system records that must be reconciled. The Filter Suffix attribute helps you to assign filters to the API based on which you will get a filtered response from the target system.

See Performing Limited Reconciliation.

1.8.4 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 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*.

1.8.5 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*.

1.8.6 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 Instance Applications in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.8.7 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.

See Configuring SSL for the Connector.

2

Creating an Application by Using the ServiceNow Connector

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

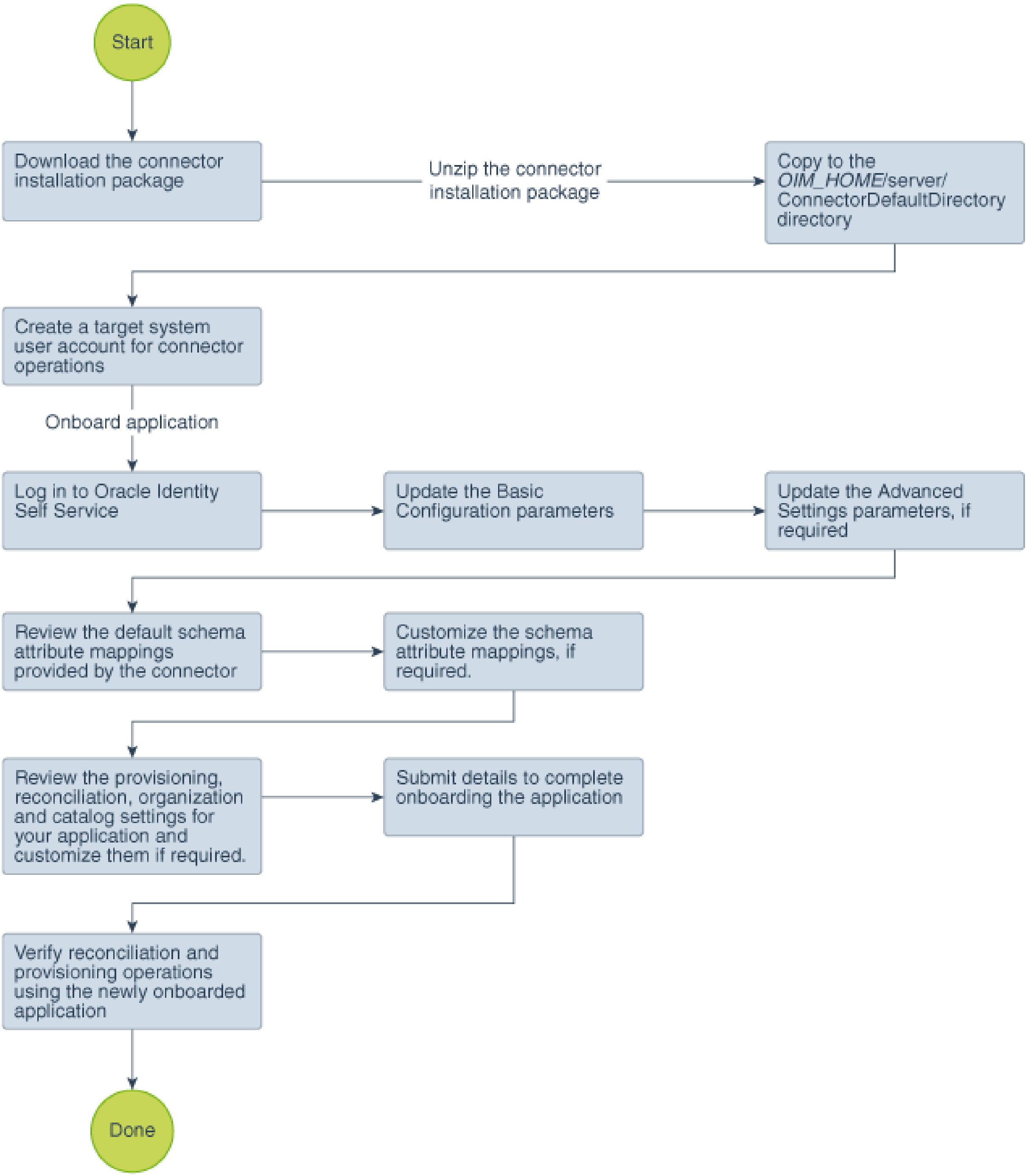
- Process Flow for Creating an Application By Using the Connector
- Prerequisites for Creating an Application By Using the Connector
- Creating an Application By Using the Connector

2.1 Process Flow for Creating an Application By Using the Connector

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

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

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


Start
Download the connector installation package
Unzip the connector installation package
Copy to the *OIM_HOME*/server/ ConnectorDefaultDirectory directory
Create a target system user account for connector operations
Onboard application
Log in to Oracle Identity Self Service
Update the Basic Configuration parameters
Update the Advanced Settings parameters, if required
Review the default schema attribute mappings provided by the connector
Customize the schema attribute mappings, if required.
Review the provisioning, reconciliation, organization and catalog settings for your application and customize them if required.
Submit details to complete onboarding the application
Verify reconciliation and provisioning operations using the newly onboarded application
Done

2.2 Prerequisites for Creating an Application By Using the Connector

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

- Configuring the Target System
- Downloading the Connector Installation Package

2.2.1 Configuring the Target System

Configuring the target system involves registering a client application so that the connector can access ServiceNow REST APIs. It also involves creating a user account, modifying ACL values, and assigning specific roles to the user.

> **Note:**
>
> The detailed instructions for performing these preinstallation tasks are available in the ServiceNow product documentation at https://docs.servicenow.com.

To configure the target system:

1. Create a user account on the target system and assign the **user_admin** role. The connector uses this account to connect to the target system during reconciliation and provisioning operations.
2. Modify the access control list values (also referred as ACL values) for user role management. This step elevates the user access privilege for the target system user account earlier created. Edit the ACL values for assigning various user roles that are required for the target system user account.
3. Register the ServiceNow connector as a client application with the ServiceNow instance to provide secure sign-in and authorization for your services. To do so:
   a. Activate the OAuth 2.0 plugin in the ServiceNow instance. This step is required for generating the client ID and client secret values.
   b. Create an OAuth application to generate the client ID and client secret values. Note down these values as they are required while configuring the `clientId` and `clientSecret` basic configuration parameters.

2.2.2 Downloading the Connector Installation Package

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

To download the connector installation package:

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

3. Select the **Accept License Agreement** option.

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

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

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

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

2.3 Creating an Application By Using the Connector

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

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

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

1. Create an application in Identity Self Service. The high-level steps are as follows:

   a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.

   b. Ensure that the **Connector Package** option is selected when creating an application.

   c. Update the basic configuration parameters to include connectivity-related information.

   d. If required, update the advanced setting parameters to update configuration entries related to connector operations.

   e. Review the default user account attribute mappings. If required, add new attributes or you can edit or delete existing attributes.

   f. Review the provisioning, reconciliation, organization, and catalog settings for your application and customize them if required. For example, you can customize the default correlation rules for your application if required.

   g. Review the details of the application and click **Finish** to submit the application details.

      The application is created in Oracle Identity Governance.

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

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

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

> **See Also:**
>
> - Configuring the ServiceNow Connector for details on basic configuration and advanced settings parameters, default user account attribute mappings, default correlation rules, and reconciliation jobs that are predefined for this connector
> - Configuring Oracle Identity Governance for details on creating a new form and associating it with your application, if you chose not to create the default form

3

Configuring the ServiceNow Connector

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

- Basic Configuration Parameters
- Advanced Settings Parameters
- Attribute Mappings
- Correlation Rules
- Reconciliation Jobs

3.1 Basic Configuration Parameters

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

Table 3-1 Basic Configuration Parameters for the ServiceNow Connector

Parameter	Mandatory?	Description
host	Yes	Enter the host name of the computer hosting your target system. **Sample value**: `ven01623.service-now.com`
authenticationType	Yes	Enter the type of authentication used by your target system. **Sample value**: `password`
Connector Server Name	No	By default, 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.
authenticationServerUrl	No	Enter the URL of the authentication server that validates the client ID and client secret for your target system. **Sample value**: `https://ven01622.service-now.com/oauth_token.do`
clientId	No	Enter the client identifier (a unique string) issued by the authorization server to your domain while registering your client application with the target system. **Sample value**: `ab0781d7c00a120039f0dbb350692319` See Configuring the Target System for details on obtaining the clientId value.

Table 3-1 (Cont.) Basic Configuration Parameters for the ServiceNow Connector

Parameter	Mandatory?	Description
clientSecret	No	Enter the value used to authenticate the identity of your domain. This value is generated while registering your client application with the target system. **Sample value**: `?*AV79Zx}` See Configuring the Target System for details on obtaining the clientSecret value.
username	No	Enter the user name of the target system that you create for performing connector operations. **Sample value**: `johnsmith`
password	No	Enter the password of the target system user account that you create for connector operations. **Sample value**: `password`
port	No	Enter the port number at which the target system is listening. **Sample value**: `443`
sslEnabled	No	If the target system requires SSL connectivity, then set the value of this parameter to `true`. Otherwise set the value to `false`.
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 of the proxy user ID of the target system user account that Oracle Identity Governance uses to connect to the target system.
proxyPort	No	Enter the proxy port number. **Sample value**: `80`
proxyUser	No	Enter the proxy user name of the target system user account that Oracle Identity Governance uses to connect to the target system.
uriPlaceHolder	No	Enter a comma-separated list of key-value pairs for replacing place holders in the relURIs in the following format: *KEY*;*VALUE* **Sample value**: `"tenant_id;domain name","api_version;apiversion=1.6"`

3.2 Advanced Settings Parameters

Advanced configuration parameters vary depending on whether you are creating a target application or an authoritative application.

- Advanced Settings Parameters for a Target Application
- Advanced Settings Parameters for an Authoritative Application

3.2.1 Advanced Settings Parameters for a Target Application

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

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

Table 3-2 Advanced Settings Parameters for a Target Application

Parameter	Mandatory?	Description

relURIs	Yes	This entry holds the relative URL of every object class supported by this connector and the connector operations that can be performed on these object classes.
		Default value:
		`"__ACCOUNT__.CREATEOP=/api/now/v2/table/sys_user?sysparm_input_display_value=true",`
		`"__ACCOUNT__.SEARCHOP=/api/now/v2/table/sys_user?$(Filter Suffix)$&sysparm_limit=$(PAGE_SIZE)$&sysparm_offset=$(PAGE_OFFSET)$",`
		`"__ACCOUNT__=/api/now/v2/table/sys_user/$(__UID__)$?sysparm_input_display_value=true",`
		`"__GROUP__.CREATEOP=/api/now/v2/table/sys_user_group","__GROUPLKP__.SEARCHOP=/api/now/v2/table/sys_user_group?$(Filter Suffix)$&sysparm_limit=$(PAGE_SIZE)$$&sysparm_offset=$(PAGE_OFFSET)$",`
		`"__GROUPLKP__=/api/now/v2/table/sys_user_group/$(__UID__)$","__ROLELKP__.SEARCHOP=/api/now/v2/table/sys_user_role?$(Filter Suffix)$&sysparm_limit=$(PAGE_SIZE)$$&sysparm_offset=$(PAGE_OFFSET)$",`
		`"__ACCOUNT__.__GROUP__.UPDATEOP=/api/now/table/sys_user_grmember","__ACCOUNT__.__ROLE__.UPDATEOP=/api/now/table/sys_user_has_role",`
		`"__ACCOUNT__.__GROUP__.SEARCHOP=/api/now/v2/table/sys_user_grmember?sysparm_query=user.sys_id=$(__UID__)$&sysparm_limit=$(PAGE_SIZE)$$&sysparm_offset=$(PAGE_OFFSET)$",`
		`"__ACCOUNT__.__ROLE__.SEARCHOP=/api/now/table/sys_user_has_role?sysparm_query=user.sys_id=$(__UID__)$&sysparm_limit=$(PAGE_SIZE)$$&sysparm_offset=$(PAGE_OFFSET)$",`
		`"__ACCOUNT__.__GROUP__.DELETEOP=/api/now/table/sys_user_grmember/$(__MEMBERSHIP__.sys_id)$",`
		`"__ACCOUNT__.__MEMBERSHIP__.__GROUP__.SEARCHOP=/api/now/v2/table/sys_user_grmember?sysparm_query=user.sys_id=$(__UID__)$%5Egroup.sys_id=$(__GROUP__.sys_id)$",`
		`"__ACCOUNT__.__ROLE__.DELETEOP=/api/now/table/sys_user_has_role/$(__MEMBERSHIP__.sys_id)$",`
		`"__ACCOUNT__.__MEMBERSHIP__.__ROLE__.SEARCHOP=/api/now/v2/table/sys_user_has_role?sysparm_query=user.sys_id=$(__UID__)$%5Erole.sys_id=$(__ROLE__.sys_id)$",`
		`"Department.SEARCHOP=/api/now/v2/table/cmn_department?sysparm_limit=$(PAGE_SIZE)$$&sysparm_offset=$(PAGE_OFFSET)$","__ACCOUNT__.__ENABLE__.UPDATEOP=/api/now/v2/table/sys_user/$(__UID__)$?sysparm_input_display_value=true",`
		`"__ACCOUNT__.__ENABLE__.UPDATEOP=/api/now/v2/table/sys_user/$(__UID__)$?sysparm_input_display_value=true"`

Table 3-2 (Cont.) Advanced Settings Parameters for a Target Application

Parameter	Mandatory?	Description
nameAttributes	Yes	This entry holds the name attribute for all the objects that are handled by this connector. For example, for the __ACCOUNT__ object class that it used for User accounts, the name attribute is user_name. **Default value**: `"__ACCOUNT__.user_name","__GROUP__.name","__GROUPLKP__.name","__ROLE__.name","__ROLELKP__.name","Department.name"`
uidAttributes	Yes	This entry holds the uid attribute for all the objects that are handled by this connector. **Default value**: `__ACCOUNT__.sys_id","__GROUP__.value","__GROUPLKP__.sys_id","__ROLE__.value","__ROLELKP__.sys_id","Department.sys_id"`
Bundle Name	No	This entry holds the name of the connector bundle. **Default value**: `org.identityconnectors.genericrest`
Bundle Version	No	This entry holds the version of the connector bundle. **Default value:** `12.3.0`
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**: `"__ACCOUNT__.__GROUP__.UPDATEOP=POST","__ACCOUNT__.__ROLE__.UPDATEOP=POST"`
Connector Name	No	This entry holds the name of the connector. **Default value**: `org.identityconnectors.genericrest.GenericRESTConnector`
Any Incremental Recon Attribute Type	No	By default, Oracle Identity Governance accepts timestamp information sent from the target system only in Long datatype format. A decode value of True for the Incremental Recon Attribute Type entry indicates that Oracle Identity Governance accepts timestamp information in any datatype format. **Default value**: `true`
pageSize	No	This entry holds how many resources appears on a page for a search operation. **Default value**: `100`

jsonResourcesTag	No	This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload.
		Default value:
		`"__ACCOUNT__=result","__GROUP__=result","__GROUPLKP__=result","__ACCOUNT__.__GROUP__=result","__ACCOUNT__.__ROLE__=result","__ROLE__=result",`
		`"__ROLELKP__=result","Department=result","__ACCOUNT__.__MEMBERSHIP__.__GROUP__=result","__ACCOUNT__.__MEMBERSHIP__.__ROLE__=result"`

httpHeaderContentType	No	This entry holds the content type expected by the target system in the header. **Default value**: `application/json`

Table 3-2 (Cont.) Advanced Settings Parameters for a Target Application

Parameter	Mandatory?	Description
httpHeaderAccept	No	This entry holds the accept type expected from the target system in the header. **Default value**: `application/json`
specialAttributeTargetFormat	No	This entry lists the format in which an attribute is present in the target system endpoint. Values are comma separated and are presented in the following format: OBJ_CLASS.ATTR_NAME= TARGET_FORMAT. **Default value**: `"__ACCOUNT__.__GROUP__=group","__ACCOUNT__.__ROLE__=role"`

specialAttributeHandling	No	This entry lists the special attributes whose values should be sent to target one by one ("SINGLE"). Values are comma separated and are in the following format: *OBJ_CLASS.ATTR_NAME.PROV_OP*=SINGLE
		For example, the __ACCOUNT__.__ENABLE__.CREATEOP value in decode implies that during an update provisioning operation, the GROUP attribute of the __ACCOUNT__ object class must be sent to the target.
		Default value:
		`"__ACCOUNT__.__GROUP__.UPDATEOP=SINGLE","__ACCOUNT__.__ROLE__.UPDATEOP=SINGLE","__ACCOUNT__.__ENABLE__.CREATEOP=SINGLE",`
		`"__ACCOUNT__.__ENABLE__.UPDATEOP=SINGLE"`

customPayload	No	This entry lists the payloads for all operations that are not in the standard format. **Default value**: `"__ACCOUNT__.__GROUP__.UPDATEOP={\"user\": \"$(__UID__)$\",\"group\": \"$(“value”)$\"}","__ACCOUNT__.__ROLE__.UPDATEOP={\"user\": \"$(__UID__)$\",\"role\": \"$(“value”)$\"}","__ACCOUNT__.__ENABLE__.UPDATEOP={\"active\":\"$(__ENABLE__)$\",\"locked_out\":\"false\"}"`
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 active. **Default value**: `"__ACCOUNT__.active"`
passwordAttribute	No	This entry holds the name of the target system attribute that is mapped to the __PASSWORD__ attribute of the connector. **Default value**: `"user_password"`
enableEmptyString	No	This entry holds the boolean value and indicates that an empty string needs to be sent to the target system. When the ServiceNow Table API receives a null value for any parameter, and if the enableEmptyString attribute is set to true, then an empty string is sent to the target system. **Default value**: `true`

3.2.2 Advanced Settings Parameters for an Authoritative Application

These are the configuration-related entries that the connector uses during reconciliation runs against an Authoritative application.

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

Table 3-3 Advanced Settings Parameters for an Authoritative Application

Parameter	Mandatory?	Description
relURIs	Yes	This entry holds the relative URL of every object class supported by this connector and the connector operations that can be performed on these object classes. **Default value**: `"__ACCOUNT__.SEARCHOP=/api/now/v2/table/sys_user?$(FilterSuffix)$&sysparm_limit=$(PAGE_SIZE)$&sysparm_offset=$(PAGE_OFFSET)$","__ACCOUNT__=/api/now/v2/table/sys_user/$(__UID__)$?sysparm_input_display_value=true"`
nameAttributes	Yes	This entry holds the name attribute for all the objects that are handled by this connector. For example, for the __ACCOUNT__ object class that it used for User accounts, the name attribute is user_name. **Default value**: `"__ACCOUNT__.user_name"`
uidAttributes	Yes	This entry holds the uid attribute for all the objects that are handled by this connector. **Default value**: `"__ACCOUNT__.sys_id"`
Bundle Name	No	This entry holds the name of the connector bundle. **Default value**: `org.identityconnectors.genericrest`
Bundle Version	No	This entry holds the version of the connector bundle. **Default value:** `12.3.0`
Connector Name	No	This entry holds the name of the connector. **Default value**: `org.identityconnectors.genericrest.GenericRESTConnector`
Any Incremental Recon Attribute Type	No	By default, Oracle Identity Governance accepts timestamp information sent from the target system only in Long datatype format. The value of `True` for this parameter indicates that Oracle Identity Governance accepts timestamp information in any datatype format. **Default value**: `true`
pageSize	No	This entry holds the number of resources that can appear on a page for a search operation. **Default value**: `100`

Table 3-3 (Cont.) Advanced Settings Parameters for an Authoritative Application

Parameter	Mandatory?	Description
jsonResourcesTag	No	This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload. **Default value**: `"__ACCOUNT__=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`
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 `active`. **Default value**: `"__ACCOUNT__.active"`
enableEmptyString	No	This entry holds the boolean value and indicates that an empty string needs to be sent to the target system. When the ServiceNow Table API receives a null value for any parameter, and if the enableEmptyString attribute is set to `true`, then an empty string is sent to the target system. **Default value**: `true`

3.3 Attribute Mappings

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

- Attribute Mappings for a Target Application
- Attribute Mappings for an Authoritative Application

3.3.1 Attribute Mappings for a 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.

ServiceNow User Account Attributes

Table 3-4 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and ServiceNow application columns.

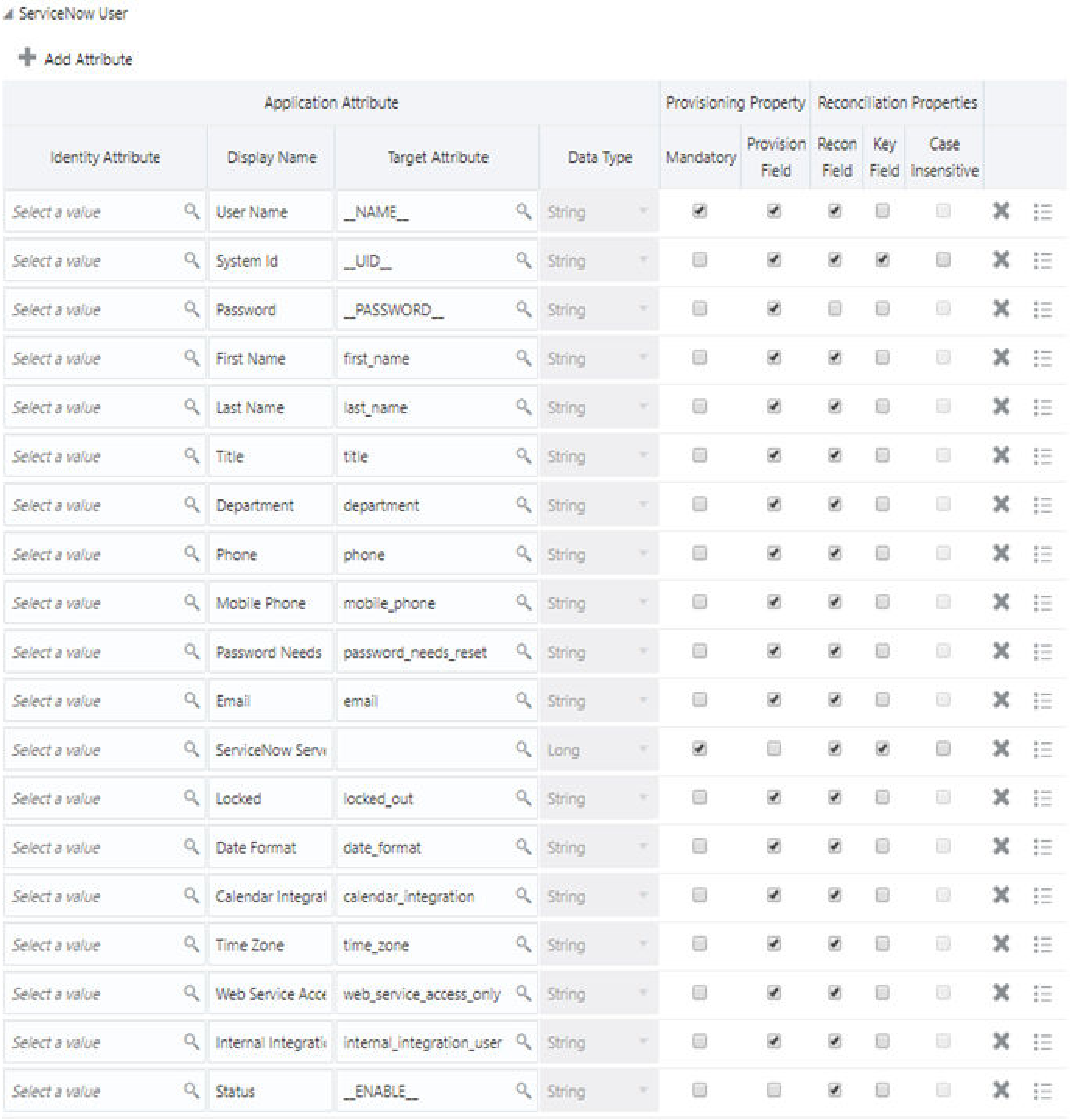
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-4 Default Attribute Mappings for ServiceNow User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
User Name	__NAME__	String	Yes	Yes	Yes	No	No
System Id	__UID__	String	No	Yes	Yes	Yes	No
Password	__PASSWORD__	String	No	Yes	No	No	No
First Name	first_name	String	No	Yes	Yes	No	No
Last Name	last_name	String	No	Yes	Yes	No	No
Title	title	String	No	Yes	Yes	No	No
Department	department	String	No	Yes	Yes	No	No
Phone	phone	String	No	Yes	Yes	No	No
Mobile Phone	mobile_phone	String	No	Yes	Yes	No	No
Password Needs Reset	password_needs_reset	String	No	Yes	Yes	No	No
Email	email	String	No	Yes	Yes	No	No
ServiceNow Server	NA	Long	Yes	No	Yes	Yes	No
Locked	locked_out	String	No	Yes	Yes	No	No
Date Format	date_format	String	No	Yes	Yes	No	No
Calendar Integration	calendar_integration	String	No	Yes	Yes	No	No
Time Zone	time_zone	String	No	Yes	Yes	No	No
Web Service Access Only	web_service_access_only	String	No	Yes	Yes	No	No
Internal Integration User	internal_integration_user	String	No	Yes	Yes	No	No
Status	__ENABLE__	String	No	No	Yes	No	No

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

Figure 3-1 Default Attribute Mappings for ServiceNow User Account



◢ ServiceNow User

➕ Add Attribute

Application Attribute				Provisioning Property		Reconciliation Properties				
Identity Attribute	Display Name	Target Attribute	Data Type	Mandatory	Provision Field	Recon Field	Key Field	Case Insensitive		
Select a value	User Name	__NAME__	String	☑	☑	☑	□	□	✖	☰
Select a value	System Id	__UID__	String	□	☑	☑	☑	□	✖	☰
Select a value	Password	__PASSWORD__	String	□	☑	□	□	□	✖	☰
Select a value	First Name	first_name	String	□	☑	☑	□	□	✖	☰
Select a value	Last Name	last_name	String	□	☑	☑	□	□	✖	☰
Select a value	Title	title	String	□	☑	☑	□	□	✖	☰
Select a value	Department	department	String	□	☑	☑	□	□	✖	☰
Select a value	Phone	phone	String	□	☑	☑	□	□	✖	☰
Select a value	Mobile Phone	mobile_phone	String	□	☑	☑	□	□	✖	☰
Select a value	Password Needs	password_needs_reset	String	□	☑	☑	□	□	✖	☰
Select a value	Email	email	String	□	☑	☑	□	□	✖	☰
Select a value	ServiceNow Serv		Long	☑	□	☑	☑	□	✖	☰
Select a value	Locked	locked_out	String	□	☑	☑	□	□	✖	☰
Select a value	Date Format	date_format	String	□	☑	☑	□	□	✖	☰
Select a value	Calendar Integrat	calendar_integration	String	□	☑	☑	□	□	✖	☰
Select a value	Time Zone	time_zone	String	□	☑	☑	□	□	✖	☰
Select a value	Web Service Acce	web_service_access_only	String	□	☑	☑	□	□	✖	☰
Select a value	Internal Integrati	internal_integration_user	String	□	☑	☑	□	□	✖	☰
Select a value	Status	__ENABLE__	String	□	□	☑	□	□	✖	☰

Role Entitlement Attributes

Table 3-5 lists the roles-specific attribute mappings between the process form fields in Oracle Identity Governance and ServiceNow 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.

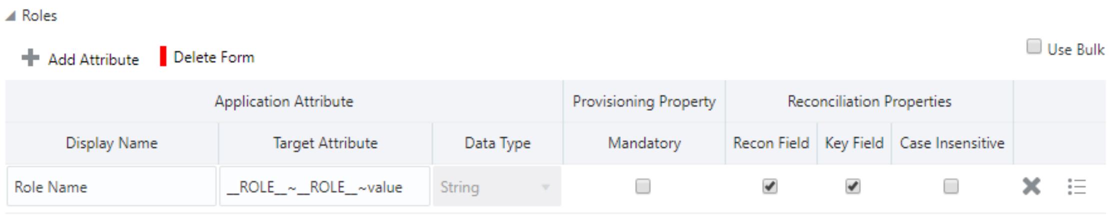
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-5 Default Attribute Mappings for Role Entitlement

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Role Name	__ROLE__~__ROLE__~value	String	No	Yes	Yes	No

Figure 3-2 shows the default roles entitlement mapping.

Figure 3-2 Default Attribute Mappings for Role Entitlement



◢ Roles

✚ Add Attribute | Delete Form

□ Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Role Name	__ROLE__~__ROLE__~value	String	□	☑	☑	□	✖	☰

Groups Entitlement Attributes

Table 3-6 lists the attribute mappings for group names between the process form fields in Oracle Identity Governance and ServiceNow 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.

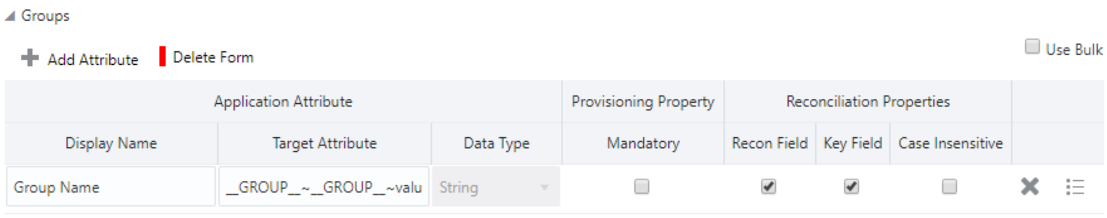
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-6 Default Attribute Mappings for Groups

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Group Name	__GROUP__~__GROUP__~value	String	No	Yes	Yes	No

Figure 3-3 shows the attribute mappings for group names between the process form fields in Oracle Identity Governance and ServiceNow target application attributes.

Figure 3-3 Default Attribute Mappings for Groups



Application Attribute			Provisioning Property	Reconciliation Properties			
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive	
Group Name	__GROUP__~__GROUP__~valu	String	□	☑	☑	□	✕ ☰

3.3.2 Attribute Mappings for an Authoritative Application

The Schema page for an authoritative 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 operations.

Table 3-7 lists the user-specific attribute mappings between the reconciliation fields in Oracle Identity Governance and ServiceNow. The table also lists the data type for a given attribute and specified whether it is a mandatory attribute for reconciliation.

If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating an Authoritative Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

You may use the default schema that has been set for you or update and change it before continuing to the next step.

The Organization Name, Xellerate Type, and Role identity attributes are mandatory fields on the OIG User form. They cannot be left blank during reconciliation. The target attribute mappings for these identity attributes are empty by default because there are no corresponding columns in the target system. Therefore, the connector provides default values (as listed in the “Default Value for Identity Display Name” column of Table 3-7) that it can use during reconciliation. For example, the default target attribute value for the Organization Name attribute is Xellerate Users. This implies that the connector reconciles all target system user accounts into the Xellerate Users organization in Oracle Identity Governance. Similarly, the default attribute value for Xellerate Type attribute is End-User, which implies that all reconciled user records are marked as end users.

Table 3-7 ServiceNow User Account Schema Attributes

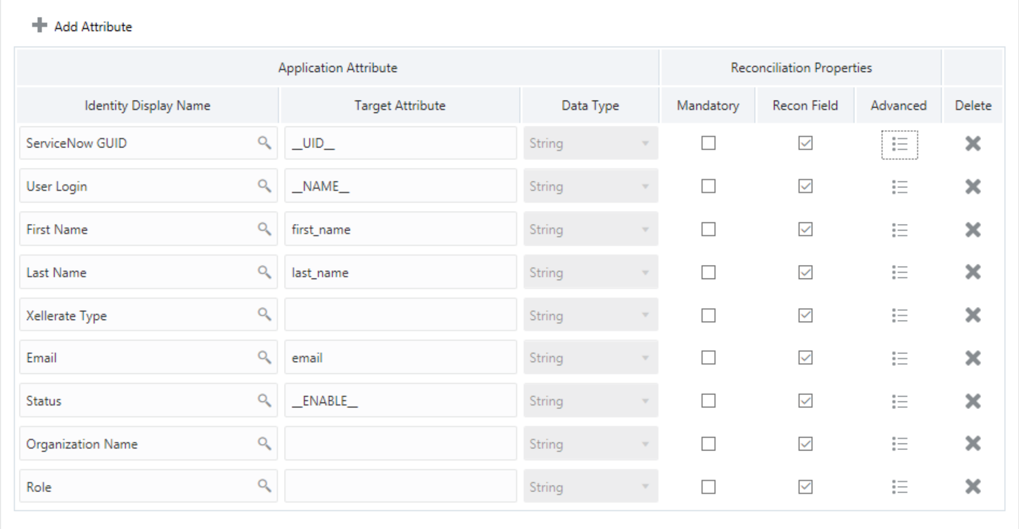
Identity Display Name	Target Attribute	Data Type	Mandatory Reconciliation Property?	Recon Field?	Default Value for Identity Display Name
ServiceNow GUID	__UID__	String	No	Yes	NA
User Login	__NAME__	String	No	Yes	NA
First Name	first_name	String	No	Yes	NA
Last Name	last_name	String	No	Yes	NA

Table 3-7 (Cont.) ServiceNow User Account Schema Attributes

Identity Display Name	Target Attribute	Data Type	Mandatory Reconciliation Property?	Recon Field?	Default Value for Identity Display Name
Xellerate Type	NA	String	No	Yes	End-User
Email	email	String	No	Yes	NA
Status	__ENABLE__	String	No	Yes	NA
Oragnization Name	NA	String	No	Yes	Xellerate Users
Role	NA	String	No	Yes	Full-Time

Figure 3-4 shows the default User account attribute mappings.

Figure 3-4 Default Attribute Mappings for an Authoritative Application



Application Attribute			Reconciliation Properties			
Identity Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Advanced	Delete
ServiceNow GUID	__UID__	String	□	☑	☰	✖
User Login	__NAME__	String	□	☑	☰	✖
First Name	first_name	String	□	☑	☰	✖
Last Name	last_name	String	□	☑	☰	✖
Xellerate Type		String	□	☑	☰	✖
Email	email	String	□	☑	☰	✖
Status	__ENABLE__	String	□	☑	☰	✖
Organization Name		String	□	☑	☰	✖
Role		String	□	☑	☰	✖

3.4 Correlation Rules

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

- Correlation Rules, Situations, and Responses for a Target Application
- Correlation Rules, Situations, and Responses for an Authoritative Application

3.4.1 Correlation Rules, Situations, and Responses for a 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 ServiceNow connector provides a simple correlation rule when you create a target application. The connector uses this correlation rule to compare the entries in Oracle Identity Governance repository and the target system repository, determine the difference between the two repositories, and apply the latest changes to Oracle Identity Governance.

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

Table 3-8 Predefined Identity Correlation Rule for a ServiceNow Target Application

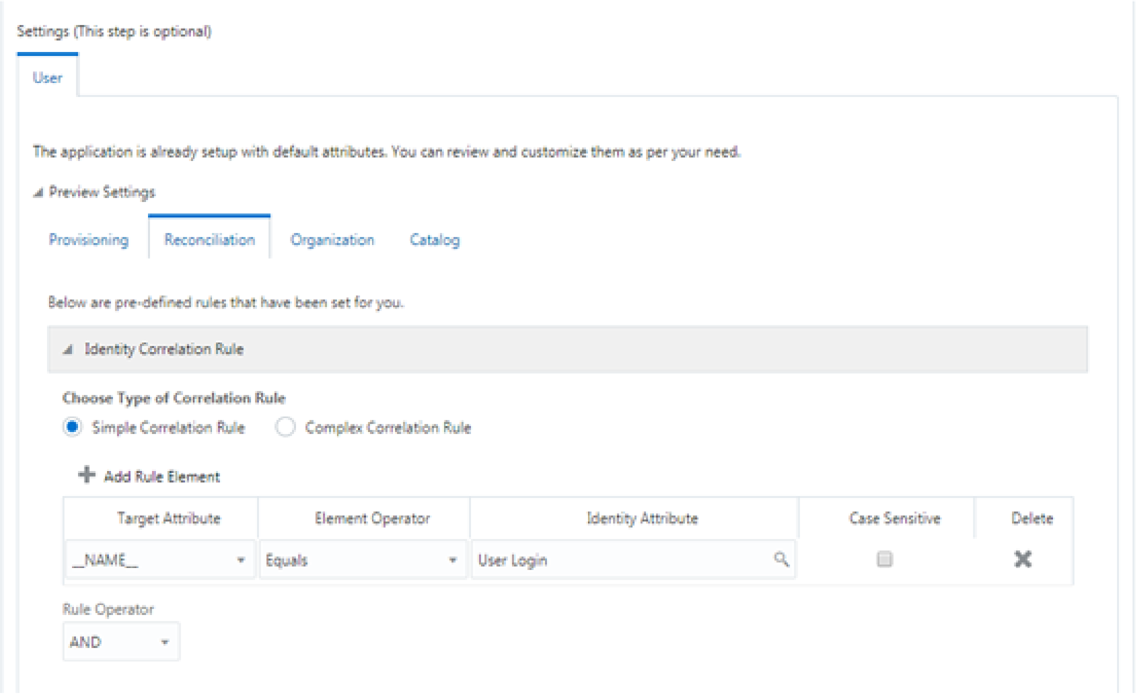
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?	Rule Operator
__NAME__	Equals	User Login	No	AND

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.
- Rule Operator is AND

Figure 3-5 shows the simple correlation rule for a ServiceNow target application.

Figure 3-5 Simple Correlation Rule for a ServiceNow Target Application



Settings (This step is optional)

The application is already setup with default attributes. You can review and customize them as per your need.

Below are pre-defined rules that have been set for you.

Choose Type of Correlation Rule
● Simple Correlation Rule ○ Complex Correlation Rule

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
__NAME__	Equals	User Login	□	✖

Rule Operator: AND

Predefined Situations and Responses

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

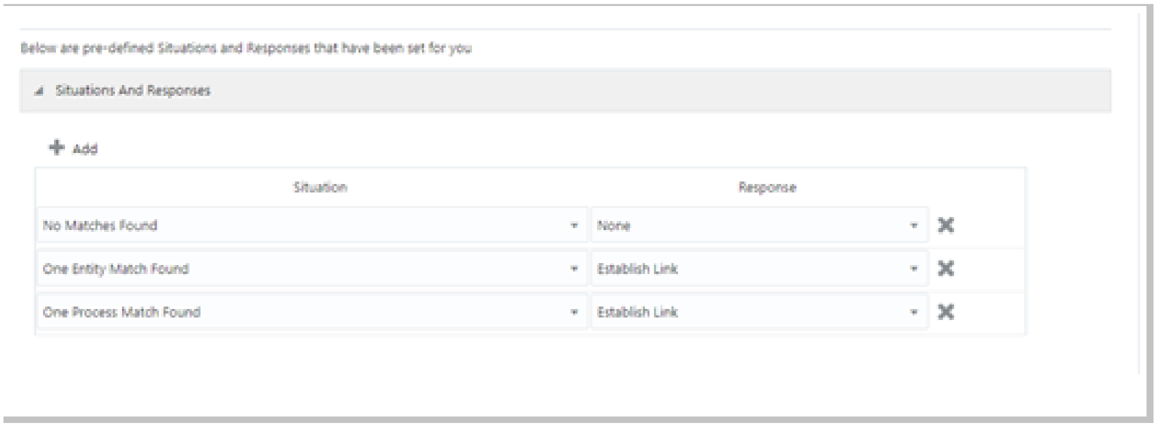
Table 3-9 lists the default situations and responses for ServiceNow target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

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

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

Figure 3-6 shows the situations and responses for ServiceNow that the connector provides by default.

Figure 3-6 Predefined Situations and Responses for a ServiceNow Target Application



Below are pre-defined Situations and Responses that have been set for you

Situations And Responses

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

3.4.2 Correlation Rules, Situations, and Responses for an Authoritative Application

When you create an authoritative 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 ServiceNow connector provides a simple correlation rule when you create an authoritative application. The connector uses this correlation rule to compare the entries in Oracle Identity Governance repository and the authoritative application repository, determine the difference between the two repositories, and apply the latest changes to Oracle Identity Governance.

Table 3-10 lists the default simple correlation rule for ServiceNow 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 Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-10 Predefined Identity Correlation Rule for ServiceNow Authoritative Application

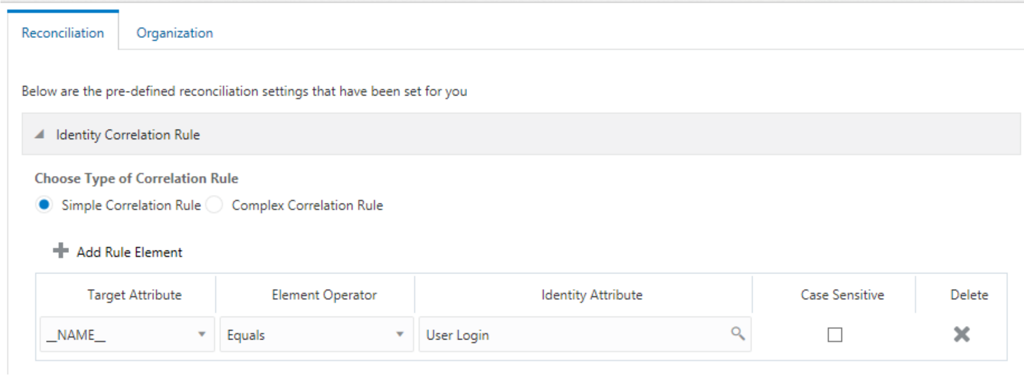
Authoritative Attribute	Element Operator	Identity Attribute	Case Sensitive?
Name	Equals	User Login	No

In the correlation rule element:

- __Name__ is an attribute on the target system that uniquely identifies the user account.
- User Login is the field on the OIM User form.
- Rule operator: AND

The following figure shows the simple correlation rule for ServiceNow Authoritative application.

Figure 3-7 Simple Correlation Rule for a ServiceNow Authoritative Application



Below are the pre-defined reconciliation settings that have been set for you

Identity Correlation Rule

Choose Type of Correlation Rule

● Simple Correlation Rule ○ Complex Correlation Rule

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
NAME	Equals	User Login	□	✖

Predefined Situations and Responses

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

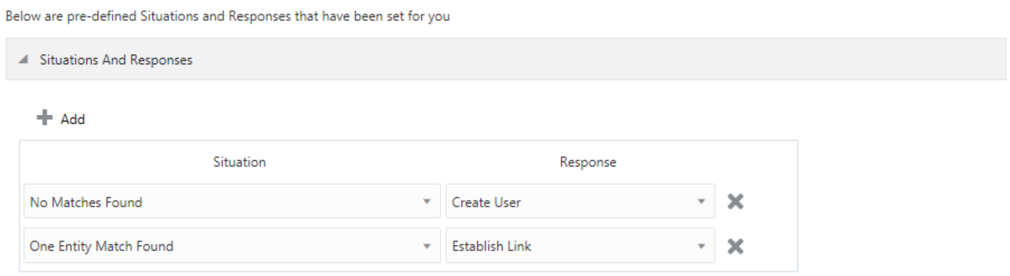
Table 3-11 lists the default situations and responses for the ServiceNow Authoritative Application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.*

Table 3-11 Predefined Situations and Responses for a ServiceNow Authoritative Application

Situation	Response
No Matches Found	Create User
One Entity Match Found	Establish Link

Figure 3-8 shows the situations and responses for ServiceNow that the connector provides by default.

Figure 3-8 Predefined Situations and Responses for a ServiceNow Authoritative Application



Below are pre-defined Situations and Responses that have been set for you

Situations And Responses

Situation	Response	
No Matches Found	Create User	✖
One Entity Match Found	Establish Link	✖

3.5 Reconciliation Jobs

These are the reconciliation jobs that the connector creates after you create a target or an authoritative application.

- Reconciliation Jobs for a Target Application
- Reconciliation Jobs for an Authoritative Application

3.5.1 Reconciliation Jobs for a Target Application

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

You must specify values for the parameters of user reconciliation jobs.

ServiceNow Full User Reconciliation Job

The ServiceNow Full User Reconciliation job is used to fetch all user records from the target system.

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

Table 3-12 describes the parameters of the ServiceNow Full User Reconciliation job.

Table 3-12 Parameters of the ServiceNow Full User Reconciliation Job

Attribute	Description
Filter Suffix	Enter the search filter for fetching records from the target system during a reconciliation run. **Sample value**: `/0e220301db039a00b88df7a0cf9619` See Performing Limited Reconciliation for more information about filtered reconciliation.
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* modify this value.
Object Type	Type of object you want to reconcile. **Default value**: `User`
Scheduled Task Name	Enter the name of the scheduled task that is used for reconciliation. **Default value**: `<Application Name> ServiceNow Full User Reconciliation`
Latest Token	Enter the value of the attribute that is specified as the value of the Incremental Recon Attribute attribute. The Latest Token attribute is used for internal purposes. By default, this value is empty. **Note**: If an appropriate Increment Recon attribute has been specified, then do not enter a value for this attribute. **Sample value**: `2017-11-30T04:44:2 9Z`

Reconciliation Jobs for Lookup Field Synchronization

These lookup definitions are used as an input source for lookup fields in Oracle Identity Governance.

The following scheduled jobs are used for lookup fields synchronization:

- ServiceNow Group Lookup Reconciliation Scheduled Job: This scheduled task is used to fetch data about groups during target resource reconciliation.
- ServiceNow Role Lookup Reconciliation Scheduled Job: This scheduled task is used to fetch data about roles during target resource reconciliation.
- ServiceNow Department Lookup Reconciliation Scheduled Job: This scheduled task is used to fetch data about departments during target resource reconciliation.

The parameters for all the reconciliation jobs are the same.

The parameters for all the scheduled jobs for lookup field synchronization are the same. Table 3-13 describes the parameters of the scheduled jobs.

Table 3-13   Parameters of the Reconciliation Jobs for Lookup Field Synchronization

Attribute	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* modify this value.
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 you are using, the default values are as follows: • For ServiceNow Group Lookup Reconciliation: `Lookup.ServiceNow.Groups` • For ServiceNow Role Lookup Reconciliation: `Lookup.ServiceNow.Role` • For ServiceNow Department Lookup Reconciliation: `Lookup.ServiceNow.Department`
Object Type	Enter the type of object whose values must be synchronized. Depending on the scheduled job you are using, the default values are as follows: • For ServiceNow Group Lookup Reconciliation: `__GROUPLKP__` • For ServiceNow Role Lookup Reconciliation: `__ROLELKP__` • For ServiceNow Department Lookup Reconciliation: `Department`

Table 3-13 (Cont.) Parameters of the Reconciliation Jobs for Lookup Field Synchronization

Attribute	Description
Code Key Attribute	Enter the 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__`
Decode Attribute	Enter the 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__`

3.5.2 Reconciliation Jobs for an Authoritative Application

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

You must specify values for the parameters of user reconciliation jobs.

ServiceNow User Trusted Reconciliation Job

The ServiceNow User Trusted Reconciliation job is used to fetch all user records from the target system.

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

Table 3-12 describes the parameters of the user reconciliation job for trusted reconciliation.

Table 3-14 Parameters of the ServiceNow User Trusted Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* modify this value.
Filter Suffix	Enter the search filter for fetching records from the target system during a reconciliation run. **Sample value**: `/0e220301db039a00b88df7a0cf9619` See Performing Limited Reconciliation for more information about filtered reconciliation.
Object Type	Type of object you want to reconcile. **Default value**: `User`

Table 3-14 (Cont.) Parameters of the ServiceNow User Trusted Reconciliation Job

Parameter	Description
Scheduled Task Name	Enter the name of the scheduled task that is used for reconciliation. **Default value**: *`Application Name`* `ServiceNow User Trusted Reconciliation`
Incremental Recon Attribute	Enter `sys_updated_on` as the value of this parameter. `sys_updated_on` is the name of the target system attribute that holds the timestamp at which the user record was modified.
Latest Token	Enter the value of the attribute that is specified as the value of the Incremental Recon Attribute attribute. The Latest Token attribute is used for internal purposes. By default, this value is empty. **Note**: If an appropriate Increment Recon attribute has been specified, then do not enter a value for this attribute. **Sample value**: `<String>2019-11-13 05:33:36</String>`

4 Performing the Postconfiguration Tasks for the ServiceNow Connector

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

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

4.1 Configuring Oracle Identity Governance

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

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

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

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

4.1.1 Creating and Activating a Sandbox

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

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

4.1.2 Creating a New UI Form

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

See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

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

4.1.3 Publishing a Sandbox

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

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

4.1.4 Updating an Existing Application Instance with a New Form

For any changes that you do in the schema of your application in Identity Self Service, you must create a new UI form and update the changes in an application instance.

To update an existing application instance with a new form:

1. Create and activate a sandbox.
2. Create a new UI form for the resource.
3. Open the existing application instance.
4. In the Form field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox.

See Also:

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

4.2 Harvesting Entitlements and Sync Catalog

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

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Reconciliation Jobs for a Target Application.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.
3. Run the Catalog Synchronization Job scheduled job.

See Also:

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

4.3 Managing Logging for the Connector

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

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

4.3.1 Understanding Log Levels

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

ODL is the principle logging service used by Oracle Identity Governance and is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.
- SEVERE

  This level enables logging of information about errors that might allow Oracle Identity Governance to continue running.
- WARNING

  This level enables logging of information about potentially harmful situations.
- INFO

  This level enables logging of messages that highlight the progress of the application.
- CONFIG

  This level enables logging of information about fine-grained events that are useful for debugging.
- FINE, FINER, FINEST

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

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

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

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

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

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

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

4.3.2 Enabling Logging

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='servicenow-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="servicenow-handler"/>
     <handler name="console-handler"/>
   </logger>

<logger name="ORG.IDENTITYCONNECTORS.RESTCOMMON" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="servicenow-handler"/>
     <handler name="console-handler"/>
   </logger>
```

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. .

   Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages specific to connector operations to be recorded.

   The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]** :

```
<log_handler name='servicenow-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path' value='/<%OIM_DOMAIN%>/servers/oim_server1/
logs/serviceNowScriptLogs.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="servicenow-handler"/>
     <handler name="console-handler"/>
   </logger>
```

```
<logger name="ORG.IDENTITYCONNECTORS.RESTCOMMON" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="servicenow-handler"/>
     <handler name="console-handler"/>
   </logger>
```

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

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

   For Microsoft Windows:

   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:

   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

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

4.4 Configuring the IT Resource for the Connector Server

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

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

In Oracle Identity System Administration, search for and edit the ServiceNow 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*.

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

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. **Sample value**: `HostName`
Key	Enter the key for the Connector Server.
Port	Enter the number of the port at which the Connector Server is listening. **Sample value**: `8763`
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the Connector Server and Oracle Identity Governance times out. If the value is zero or if no value is specified, the timeout is unlimited. **Sample value**: `0` (recommended value)

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

Parameter	Description
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Governance and the Connector Server. Otherwise, enter `false.` **Default value**: `false` **Note**: It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see Setting SSL for Connector Server and OIM 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 label that is added to the UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:

   SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf
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 ServiceNow application instance. The original code is:

```
<trans-unit
id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.userEO.UD_SN_USR_USERNAME__c_description']}">
<source>User Name</source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.snform.entity.snf
ormEO.UD_SN_USR_USERNAME__c_LABEL">
<source>First Name</source>
<target/>
</trans-unit>
```

d. Open the properties file from resource folder in the connector package, for example `ServiceNow_ja.properties`, and get the value of the attribute from the file, for example,

```
global.udf.UD_SNA_USR_ USER_NAME
=\u30A2\u30AB\u30A6\u30F3\u30C8\u540D
```

e. Replace the original code shown in Step 7.c with the following:

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.use
rEO.UD_SN_USR_ USER_NAME __c_description']}">
<source>Account Name</source>
<target>u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.Servicenow.entity
sEO.UD_SN_USR_UserName__c_LABEL">
<source>Account Name</source>
<target>\u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target>
</trans-unit>
```

f. Repeat Steps 7.a through 7.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.

h. 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

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

4.6 Configuring SSL for the Connector

Configure SSL to secure data communication between Oracle Identity Governance and ServiceNow 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 ServiceNow.
2. Copy the public key certificate of ServiceNow to the computer hosting Oracle Identity Governance.
3. Run the following `keytool` command to import the public key certificate into the identity key store in Oracle Identity Governance:

   ```
   keytool -import -alias ALIAS -trustcacerts -file CERT_FILE_NAME -
   keystore KEYSTORE_NAME -storepass PASSWORD
   ```

   In this command:

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

   The following is a sample value for this command:

   ```
   keytool -import -alias serverwl -trustcacerts -file supportcert.pem -
   keystore client_store.jks -storepass example_password
   ```

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.

5

Using the ServiceNow Connector

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

- Configuring Reconciliation
- Configuring Reconciliation Jobs
- Configuring Provisioning
- Uninstalling the Connector

5.1 Configuring Reconciliation

You can configure the connector to specify the type of reconciliation and its schedule.

This section provides details on the following topics related to configuring reconciliation:

- Performing Full and Incremental Reconciliation
- Performing Limited Reconciliation

5.1.1 Performing Full and Incremental Reconciliation

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

For a Target application, you can only perform full reconciliation. For an Authoritative application, you can perform both full and incremental reconciliation.

To perform a full reconciliation run, ensure that no value is specified for the Filter attribute of the scheduled job for reconciling users.

To perform an incremental reconciliation run, set the value of the Incremental Recon Attribute to `sys_updated_on`, and then run the ServiceNow User Trusted Reconciliation job. At the end of the reconciliation run, the Latest Token parameter of the reconciliation job for the 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.

See Reconciliation Jobs for information about this reconciliation jobs.

5.1.2 Performing Limited Reconciliation

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

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

All users are associated with a unique system ID, also known as `sys_id`. The `sys_id` attribute is present in the target system and OIG. Filtered reconciliation is performed using the `sys_id` as a filter suffix attribute.

> **Note:**
>
> In the current connector release, the `sys_id` attribute is the only filter suffix supported for filtering records.

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 the `sys_id` attribute of the target system to filter target system records. The `sys_id` is appended to the endpoint URL. When this endpoint URL is reconciled, all record reconciliation is limited to this filter suffix attribute. A sample filter suffix value is `/0e220301db039a00b88df7a0cf9619`. The value provided in the filter suffix parameter varies in accordance with the target system.

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

While creating the application, follow the instructions in Configuring Reconciliation to specify attribute values.

5.2 Configuring Reconciliation Jobs

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

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

To configure a reconciliation job:

1. Log in to Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled job as follows:
   a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the parameters of the scheduled task:

- **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
- **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type. See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

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

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

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

6. Click **Apply** to save the changes.

> **Note:**
>
> You can use the Scheduler Status page in Identity System Administration to either start, stop, or reinitialize the scheduler.

5.3 Configuring Provisioning

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

- Guidelines on Performing Provisioning Operations
- Performing Provisioning Operations

5.3.1 Guidelines on Performing Provisioning Operations

These guidelines provide information on what to do when performing provisioning operations.

For a Create User provisioning operation, you must specify a value for the User Name field. For example, John Doe. It is a mandatory field.

5.3.2 Performing Provisioning Operations

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

To perform provisioning operations in Oracle Identity Governance:

1. Log in to Identity Self Service.
2. Create a user as follows:

   a. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
   b. From the Actions menu, select **Create**. Alternatively, you can click **Create** on the toolbar. The Create User page is displayed with input fields for user profile attributes.
   c. Enter details of the user in the Create User page.
3. On the Account tab, click **Request Accounts**.
4. In the Catalog page, search for and add to cart the application instance for the connector that you configured earlier, and then click **Checkout**.
5. Specify value for fields in the application form and then click **Ready to Submit**.
6. Click **Submit**.

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

5.4 Uninstalling the Connector

Uninstalling the 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 (for example, `ServiceNow User; ServiceNow Group`) as the value of the `ObjectValues` property.

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

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

6

Extending the Functionality of the ServiceNow Connector

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

- Configuring Transformation and Validation of Data
- Configuring Action Scripts
- Configuring the Connector for Multiple Installations of the Target System

6.1 Configuring Transformation and Validation of Data

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

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

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

To configure transformation or validation of user account data, you must write Groovy scripts while creating your application. For more information about writing Groovy script-based validation and transformation logic, see Validation and Transformation of Provisioning and Reconciliation Attributes of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

6.2 Configuring Action Scripts

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

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

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

6.3 Configuring the Connector for Multiple Installations of the Target System

You must create copies of configurations of your base application to configure it for multiple installations of the target system.

The following example illustrates this requirement:
The London and New York offices of Example Multinational Inc. have their own installations of the target system, including independent schema for each. The company has recently installed Oracle Identity Governance, and they want to configure it to link all the installations of the target system.

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

7 Upgrading the ServiceNow Connector

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

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

The following sections discuss the procedure to upgrade the connector:

- Preupgrade Steps
- Upgrade Steps
- Postupgrade Steps

> **See Also:**
>
> About Upgrading Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information on these steps

7.1 Preupgrade Steps

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

Perform the following preupgrade steps:

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

to the connector. See Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information.

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

7.2 Upgrade Steps

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

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

- Staging Environment

  Perform the upgrade procedure by using the wizard mode.

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

- Production Environment

  Perform the upgrade procedure by using the silent mode.

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

7.3 Postupgrade Steps

Postupgrade steps involve uploading new connector JAR to Oracle Identity Manager database, deleting duplicate entries for lookup definitions, verifying attribute mappings for custom attributes, and so on.

Perform the following procedure:

1. Delete the old Connector JARs. Run the Oracle Identity Manager Delete JARs `($ORACLE_HOME/bin /DeleteJars.sh)` utility to delete the existing ICF bundle `org.identityconnectors.genericrest-1.0.11150.jar` from the Oracle Identity Manager database.

   When you run the Delete JARs utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being deleted, and the name of the JAR file to be removed. Specify 4 as the value of the JAR type.

2. Upload the new connector JARs:
   a. Run the Oracle Identity Manager Upload JARs `($ORACLE_HOME/bin/UploadJars.sh)` utility to upload the connector JARs.
   b. Upload the `org.identityconnectors.genericrest-12.3.0.jar` bundle as an ICF Bundle. Run the Oracle Identity

Manager Upload JARs utility to post the new ICF bundle `org.identityconnectors.genericrest-12.3.0.jar` file to the Oracle Identity Manager database.

When you run the Upload JARs utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 4 as the value of the JAR type.

3. If any of the previous connector artifacts are retained after a successful upgrade operation, then log in to Oracle Identity Manager Design Console and delete the following duplicate entries:

   - For the Lookup.ServiceNow.Configuration lookup definition:

Code Key	Decode
Bundle Version	1.0.1115
relURIs	"__ACCOUNT__.CREATEOP=/api/now/v1/table/sys_user?sysparm_input_display_value=true", "__ACCOUNT__.SEARCHOP=/api/now/v1/table/sys_user/$(FilterSuffix)$", "__ACCOUNT__=/api/now/v1/table/sys_user/$(__UID__)$?sysparm_input_display_value=true", "__GROUP__.CREATEOP=/api/now/v1/table/sys_user_group", "__GROUP__.SEARCHOP=/api/now/v1/table/sys_user_group/$(FilterSuffix)$", "__GROUP__=/api/now/v1/table/sys_user_group/$(__UID__)$", "__ROLE__.SEARCHOP=/api/now/v1/table/sys_user_role/$(FilterSuffix)$", "__ACCOUNT__.__GROUP__.UPDATEOP=/api/now/table/sys_user_grmember", "__ACCOUNT__.__ROLE__.UPDATEOP=/api/now/table/sys_user_has_role", "__ACCOUNT__.__GROUP__.SEARCHOP=/api/now/v1/table/sys_user_grmember?sysparm_query=user.sys_id=$(__UID__)$", "__ACCOUNT__.__ROLE__.SEARCHOP=/api/now/table/sys_user_has_role?sysparm_query=user.sys_id=$(__UID__)$", "__ACCOUNT__.__GROUP__.DELETEOP=/api/now/table/sys_user_grmember/$(__MEMBERSHIP__.sys_id)$", "__ACCOUNT__.__MEMBERSHIP__.__GROUP__.SEARCHOP =/api/now/v1/table/sys_user_grmember?sysparm_query=user.sys_id=$ (__UID__)$%5E (__UID__)$%5Egroup.sys_id=$(__GROUP__.sys_id) $&sysparm__fields=sys_id", "__ACCOUNT__.__ROLE__.DELETEOP=/api/now/table/sys_user_has_role$(__MEMBERSHIP__.sys_id)$", "__ACCOUNT__.__MEMBERSHIP__.__ROLE__.SEARCHOP=/api/now/v1/table/sys_user_has_role?sysparm_query=user.sys_id=$(__UID__)$%5Erole.sys_id=$(__ROLE__.sys_id) $&sysparm _fields=sys_id", "Department.SEARCHOP =/api/now/v1/table/cmn_department", "__ACCOUNT__.__ENABLE__.UPDATEOP=/api/now/v1/table/sys_user/$(__UID__)$?sysparm__input_display_value=true", "__ACCOUNT__.__ENABLE__.UPDATEOP=/api/now/v1/table/sys_user/$(__UID__)$?sysparm__input_display_value=true"

Code Key	Decode

customPayload	"__ACCOUNT__.__GROUP__.UPDATEOP={\"user\": \"$(__UID__)$\",\"group\": \"(sys_id)\"}","
	__ACCOUNT__.__ROLE__.UPDATEOP={\"user\": \"$(__UID__)$\",\"role\": \"(sys_id)\"}","
	__ACCOUNT__.__ENABLE__.UPDATEOP={\"active\":\"$(__ENABLE__)$\",\"locked_out\":\"false\"}"

jsonResourcesTag	"__ACCOUNT__=result","__GROUP__=result", "__ACCOUNT__.__GROUP__=result", "__ACCOUNT__.__ROLE__=result","__ROLE__=result","Department=result", "__ACCOUNT__.__MEMBERSHIP__.__GROUP__=result", "__ACCOUNT__.__MEMBERSHIP__.__ROLE__=result"
nameAttributes	"__ACCOUNT__.user_name", "__GROUP__.name", "__ROLE__.name","Department.name"
specialAttributeTargetFormat	"__ACCOUNT__.__GROUP__=group", "__ACCOUNT__.__ROLE__=role"
uidAttributes	"__ACCOUNT__.sys_id", "__GROUP__.sys_id", "__ROLE__.sys_id", "Department.sys_id"

- For the Lookup.ServiceNow.UM.ReconAttrMap lookup definition:

Code Key	Decode
UD_SN_UGP~Group Name[LOOKUP]	__GROUP__~__GROUP__~sys_id
UD_SN_URO~Role Name[LOOKUP]	__ROLE__~__ROLE__~sys_id

4. If any attribute mappings are missing for custom attributes, log in to Oracle Identity Manager Design Console and update the mappings.
5. Restart Oracle Identity Manager.
6. If the connector is deployed on a Connector Server, then:
   a. Stop the Connector Server.
   b. Replace the existing bundle JAR file `org.identityconnectors.genericrest-1.0.1115.jar` with the new bundle JAR file `org.identityconnectors.genericrest-12.3.0.jar`.
   c. Start the Connector Server.

After upgrading the connector, you can perform either full reconciliation or limited reconciliation. This ensures that records created or modified since the last reconciliation run are fetched into Oracle Identity Manager.

See Also:

- Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about deploying the Connector Server
- Configuring Reconciliation for more information about performing full or incremental reconciliation

8

Known Issues and Limitations of the ServiceNow Connector

These are the known issues and limitations associated with the ServiceNow connector.

Limitations Related to Target System Features

Target attribute to provide the time-stamp of last updated time of both parent and child attributes is not available. Therefore, incremental reconciliation feature cannot be implemented.

Unable to Remove Roles

An error is encountered when you try to delete a role that is assigned to a user twice, that is, both as a parent role as well as an inherited role.

Workaround: The workaround is to update the relURIs parameter of the Advanced Settings section for role membership to include the `inherited=false` value. In the following line, the value that you need to add is in bold font:

```
"__ACCOUNT__.__MEMBERSHIP__.__ROLE__.SEARCHOP=/api/now/v2/table/
sys_user_has_role?sysparm_query=user.sys_id=$(__UID__)$%5Erole.sys_id=$
(__ROLE__.sys_id)$","__ACCOUNT__.__MEMBERSHIP__.__ROLE__.SEARCHOP=/api/n
ow/v2/table/sys_user_has_role?sysparm_query=user.sys_id=$(__UID__)$
%5Erole.sys_id=$
(__ROLE__.sys_id)$&sysparm_fields=sys_id&inherited=false"
```

A

Files and Directories in the Connector Installation Package

These are the files and directories on the connector installation package that comprise the ServiceNow connector.

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

File in the Installation Media Directory	Description
/bundle/ org.identityconnectors.genericrest-12.3.0.jar	This JAR file is the ICF connector bundle.
configuration/ServiceNow-CI.xml	This file is used for installing a CI-based connector. This XML file contains configuration information that is used by the Connector Installer during connector installation.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the Oracle Identity 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/ServiceNow-auth-template.xml **Note:** This file is available only if you have applied patch 29874542 from My Oracle Support to create and manage Authoritative applications.	This file contains definitions for the connector objects required for creating an Authoritative application. It includes certain details required to connect Oracle Identity Governance with the target system . It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/ServiceNow-ConnectorConfig.xml	This XML file contains definitions for the connector components. These components include the following: • IT resource type • Process forms • Process tasks and adapters (along with their mappings) • Lookup definitions • Resource objects • Process definition • Scheduled tasks • Reconciliation rules

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

File in the Installation Media Directory	Description
xml/ServiceNow-pre-config.xml	This XML file contains definitions for the connector objects associated with any non-User object such as Groups.
xml/ServiceNow-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.