Oracle® Fusion Middleware

Performing Self Service Tasks with Oracle Identity Governance

12c (12.2.1.4.0)
E95920-08

ORACLE

Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance, 12c (12.2.1.4.0)

E95920-08

Copyright © 2022, 2023, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

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

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

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

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

Contents

Preface

Audience xxii
Documentation Accessibility xxii
Related Documents xxii
Conventions xxiii

What's New In This Guide

Updates in October 2023 Documentation Refresh for 12c (12.2.1.4.0) xxiv
Updates in April 2023 Documentation Refresh for 12c (12.2.1.4.0) xxiv
Updates in October 2022 Documentation Refresh for 12c (12.2.1.4.0) xxv
Updates in October 2021 Documentation Refresh for 12c (12.2.1.4.0) xxv
Updates in April 2021 Documentation Refresh for 12c (12.2.1.4.0) xxv
Updates in October 2020 Documentation Refresh for 12c (12.2.1.4.0) xxvi
Updates in July 2020 Documentation Refresh for 12c (12.2.1.4.0) xxvi
New and Changed Features for 12c (12.2.1.4.0) xxvi

1 Understanding the Oracle Identity Self Service Interface

1.1 About Oracle Identity Self Service Interface 1-1
1.2 Top Panel of Oracle Identity Self Service Interface 1-3
1.3 About Help Link 1-4
1.3.1 About Help System 1-4
1.3.2 About Top Pane in Help Page 1-5
1.3.3 About Lower Left Pane in Help Page 1-6
1.3.4 About Lower Right Pane in Help Page 1-6
1.4 Self Service Home page in Oracle Identity Self Service Interface 1-7
1.5 Compliance Home Page in Oracle Identity Self Service Interface 1-7
1.6 Manage Home page in Oracle Identity Self Service Interface 1-9

Part I Getting Started

2 Registering to Oracle Identity Governance

2.1 Submitting Registration Requests 2-1
2.2 Tracking Registration Requests 2-1

3 Accessing Oracle Identity Self Service

3.1 Connecting to Oracle Identity Self Service 3-1
3.2 Retrieving Forgotten User Login 3-2
3.3 Resetting Forgotten Password 3-3
3.4 Challenge Questions and Responses After First Login 3-3
3.5 Setting Challenge Questions and Responses After First Login 3-4

Part II Working with Self Service

4 Managing Profile Information

4.1 Opening My Information Page 4-1
4.2 Managing Basic User Information 4-1
4.3 Changing Enterprise Password 4-2
4.4 Setting Challenge Questions and Responses 4-2
4.5 Viewing and Modifying Direct Reports 4-2
4.6 Managing Proxies 4-3
4.6.1 About Proxies 4-3
4.6.2 Adding a Proxy 4-3
4.6.3 Editing a Proxy 4-4
4.6.4 Removing a Proxy 4-5

5 Managing Access for Self

5.1 Managing Roles 5-1
5.1.1 Requesting for Roles 5-1
5.1.2 Removing Roles 5-2
5.1.3 Modifying Role Grant Duration 5-3
5.2 Managing Entitlements 5-3
5.2.1 Requesting for Entitlements 5-4
5.2.2 Modifying Entitlements 5-5
5.2.3 Removing Entitlements 5-5
5.2.4 Modifying Entitlement Grant Duration 5-6
5.3 Managing Accounts 5-6
5.3.1 Requesting for Accounts 5-7

5.3.2 Modifying Accounts 5-7
5.3.3 Removing Accounts 5-8
5.3.4 Disabling an Account 5-8
5.3.5 Enabling an Account 5-8
5.3.6 Resetting Password for an Account 5-9
5.3.7 Modifying Account Grant Duration 5-9
5.4 Viewing Admin Roles 5-9

6 Requesting Access

6.1 Requesting New Access 6-1
6.1.1 Requesting Access for Self 6-1
6.1.2 Requesting Access for Other Users 6-4
6.1.3 Requesting Access By Using a Request Profile 6-6
6.1.4 Keyword Search in the Access Catalog 6-6
6.1.5 Specifying Application Instances in Entitlements Search 6-7
6.1.6 Refining Search Results 6-8
6.2 Viewing Hierarchical Attributes of Entitlements 6-8
6.3 Adding and Removing Catalog Items to and from the Cart 6-9
6.4 Adding and Removing Grant Duration 6-9
6.4.1 Specifying Grant Duration 6-9
6.4.2 Modifying Grant Duration 6-10
6.4.3 Revoking Access 6-10
6.5 Managing Request Profiles 6-11
6.5.1 About Request Profile 6-11
6.5.2 Creating a Request Profile 6-11
6.5.3 Modifying a Request Profile 6-12
6.5.4 Deleting a Request Profile 6-12
6.6 Tracking a Request 6-13
6.6.1 Searching Track Request 6-13
6.6.2 Tracking a Draft Request 6-15
6.7 Deleting a Request 6-16
6.8 Withdrawing a Request 6-16
6.9 Closing a Request 6-17
6.10 Requesting Access With Policy Violations 6-18
6.10.1 About Requesting Access With Policy Violations 6-18
6.10.2 Migrating the Policy Violations and Submitting the Requesting 6-19
6.10.3 Predictive Policy Validation for In-Flight Requests 6-20

7 Using the Unified Inbox

7.1 Understanding the Task Types in Oracle Identity Governance 7-1
7.1.1 About Pending Approval Tasks 7-1
7.1.2 About Provisioning Tasks (or Manual Provisioning) 7-1
7.1.3 About Certification Tasks (or Pending Certifications) 7-2
7.1.4 About Audit Violation Tasks (or Pending Violations) 7-2
7.2 About the Unified Inbox 7-2
7.3 Creating a View Definition 7-2
7.4 Editing the Task Chart 7-3
7.5 Editing Inbox Settings 7-4

8 Managing Pending Approvals

8.1 About Pending Approvals 8-1
8.2 Viewing Pending Approval Tasks 8-2
8.3 Adding Comments and Attachments 8-3
8.4 Approving a Task 8-4
8.5 Rejecting a Task 8-5
8.6 Reassigning a Task 8-5
8.7 Suspending a Task 8-6
8.8 Withdrawing a Task 8-6
8.9 Skipping Current Assignment 8-6
8.10 Claiming a Task 8-6
8.11 Modifying Grant Duration 8-7

9 Managing Provisioning Tasks

9.1 About Provisioning Tasks 9-1
9.2 Managing Pending Provisioning Tasks 9-2
9.2.1 Searching Provisioning Tasks 9-2
9.2.1.1 Basic Search for Provisioning Tasks 9-2
9.2.1.2 Advanced Search for Provisioning Tasks 9-3
9.2.2 Viewing Provisioning Task Details 9-4
9.2.3 Setting Response for a Task 9-5
9.2.4 Adding Notes to a Task 9-5
9.2.5 Reassigning a Task 9-6
9.2.6 Viewing Task Assignment History 9-6
9.2.7 Viewing Form Details 9-7
9.2.8 Modifying Form Details 9-7
9.2.9 Retrying a Task 9-7
9.2.10 Manually Completing a Task 9-8

9.2.10.1 Different Types of Provisioning Operations 9-8
9.2.10.2 Completing Manual Fulfillment Task 9-8
9.3 Managing Manual Fulfillment Tasks 9-9
9.3.1 About Manual Fulfillment Task 9-9
9.3.2 Viewing and Editing Task Details 9-9
9.3.3 Completing a Task 9-10
9.3.4 Rejecting a Task 9-10
9.3.5 Adding Comments and Attachments 9-11
9.3.6 Requesting for Information 9-11
9.3.7 Reassigning a Task 9-12
9.3.8 Modifying Grant Duration 9-12

10 Managing Certification Review Tasks

10.1 Searching and Viewing Certifications 10-1
10.1.1 Searching Certifications in the Pending Certifications Page 10-1
10.1.2 Accessing Certification Tasks From the Pending Certifications Page 10-2
10.1.2.1 Viewing User Certification Details 10-3
10.1.2.2 Viewing Role Certification Details 10-6
10.1.2.3 Viewing Application Instance Certification Details 10-7
10.1.2.4 Viewing Entitlement Certification Details 10-7
10.2 Completing Certifications 10-8
10.2.1 Completing User Certifications 10-9
10.2.1.1 Making Certification Decision on the Users 10-9
10.2.1.2 Reviewing Roles and Entitlements 10-11
10.2.1.3 Finishing the User Certification 10-11
10.2.2 Completing Role Certifications 10-12
10.2.2.1 Making Certification Decisions on the Roles 10-12
10.2.2.2 Reviewing the Contents of the Roles 10-13
10.2.2.3 Finishing the Role Certification 10-14
10.2.3 Completing Application Instance Certifications 10-14
10.2.3.1 Making Certification Decisions on the Application Instances 10-14
10.2.3.2 Reviewing Account and Entitlement Assignments 10-16
10.2.3.3 Finishing the Application Instance Certification 10-17
10.2.4 Completing Entitlement Certifications 10-17
10.2.4.1 Making Certification Decisions on the Entitlements 10-17
10.2.4.2 Reviewing the Entitlement Assignments 10-19
10.2.4.3 Finishing the Entitlement Certification 10-19
10.3 Claiming and Releasing Group Certifier Assignments 10-20
10.3.1 Claiming Group Certifier Assignments 10-20

10.3.2 Releasing Group Certifier Assignments 10-20

11 Managing Pending Violations

11.1 Viewing Policy Violations 11-1
11.2 Searching Pending Violations 11-1
11.3 Completing Policy Violations 11-2
11.4 Reassigning or Delegating Policy Violations 11-3

Part III Working with Compliance

12 Using Identity Certification

12.1 Identity Certification Overview 12-1
12.1.1 What Is Identity Certification? 12-1
12.1.2 Who Is Involved in Completing Identity Certifications? 12-3
12.2 Certification UI 12-4
12.3 Certification Name Formats 12-5
12.4 Searching and Viewing Certifications 12-7
12.4.1 Searching Certifications in the Dashboard 12-7
12.4.1.1 Performing Basic Search for Certification 12-7
12.4.1.2 Performing Advanced Search for Certification 12-8
12.4.2 Sorting Certification Search Results 12-9
12.4.3 Viewing Certifications From the Dashboard 12-9
12.4.4 Accessing Pre-Upgrade Certifications in the Dashboard 12-10
12.5 Completing User Certifications in Offline Mode 12-11
12.5.1 Understanding User Certifications in Offline Mode 12-11
12.5.2 Working on a User Certification in Offline Mode 12-12
12.6 Generating Certification Reports 12-14
12.6.1 About Generating Certification 12-14
12.6.2 Generating Certification Reports From the Dashboard 12-14
12.6.3 Generating Exported Certification Reports From the Certification Pages 12-15

13 Managing Identity Certification

13.1 Certification Concepts 13-1
13.1.1 Line of Business and Line Item 13-2
13.1.2 Certification Task 13-2
13.1.3 Certification Object 13-2
13.1.4 Certification Definition 13-2
13.1.5 Certification Jobs 13-2

13.1.6 Closed-Loop Remediation 13-3
13.1.7 Remediation Tracking 13-3
13.1.8 Event Listener 13-3
13.1.9 Certification Authorization 13-3
13.1.10 Custom Reviewer for User Certifications 13-4
13.1.10.1 About Custom Access Reviewer 13-4
13.1.10.2 Conditions for Using Custom Access Reviewer 13-5
13.1.10.3 Sample CERT_CUSTOM_ACCESS_REVIEWERS Table 13-5
13.1.10.4 Custom Access Reviewer Scenarios 13-6
13.2 Configuring Certifications 13-8
13.2.1 Prerequisites for Configuring Certifications 13-8
13.2.1.1 Marking a Catalog Item as Certifiable 13-9
13.2.1.2 Setting the Certifier in the Request Catalog 13-9
13.2.1.3 Setting User Manager and Organization Certifier 13-10
13.2.1.4 Setting User Attributes for Certification Snapshot 13-11
13.2.1.5 Setting Risk Levels for Individual Entities 13-11
13.2.1.6 Tagging Attributes 13-12
13.2.1.7 Configuring the Availability of Identity Certification 13-13
13.2.1.8 Configuring Reminders, Notifications, Escalations, and Expiry for Certifications (Optional) 13-13
13.2.2 Configuring Certification Options 13-14
13.3 Managing Certification Definitions 13-16
13.3.1 Creating Certification Definitions 13-17
13.3.1.1 Creating a User Certification Definition 13-17
13.3.1.2 Creating a Role Certification Definition 13-23
13.3.1.3 Creating an Application Instance Certification Definition 13-25
13.3.1.4 Creating an Entitlement Certification Definition 13-28
13.3.2 Modifying Certification Definitions 13-31
13.3.3 Deleting Certification Definitions 13-31
13.4 Scheduling Certifications 13-32
13.5 About How Risk Summaries are Calculated 13-32
13.5.1 Understanding Item Risk and Risk-Factor Mappings 13-33
13.5.1.1 Setting Item Risk 13-33
13.5.1.2 About Risk-Level Mappings (Risk Factors) 13-34
13.5.2 About Risk Aggregation and Risk Summaries 13-35
13.5.3 About How Changing Risk Configuration Values Impacts the System 13-36
13.6 About Closed-Loop Remediation and Remediation Tracking 13-37
13.7 Configuring Challenge Workflows 13-38
13.7.1 About Challenge Workflows 13-38
13.7.2 Modifying Rules of Auto-Approval 13-39
13.8 About Event Listeners 13-39

13.9 Configuring Event Listeners and Certification Event Trigger Jobs 13-41
13.9.1 Creating an Event Listener 13-41
13.9.2 Modifying an Event Listener 13-43
13.9.3 Deleting an Event Listener 13-43
13.9.4 Configuring Certification Event Trigger Jobs 13-43
13.9.4.1 Setting the Event Listener Name List 13-44
13.9.4.2 Adding More Trigger Jobs 13-44
13.10 Configuring Certification Reports 13-45
13.11 Understanding Multi-Phased Review in User Certification 13-45
13.11.1 About Functionality of Two-Phased Review with Advanced Delegation 13-45
13.11.2 Multiple Phases of Review 13-46
13.11.3 Delegation to Multiple Reviewers Within Each Phase 13-46
13.11.4 Stages of Certification in TPAD 13-47
13.11.4.1 About Stages of Certification in TPAD 13-47
13.11.4.2 Phase One With Verification 13-49
13.11.4.3 Phase Two With Verification 13-53
13.11.4.4 Final Review 13-55
13.12 About Pre-populate Certification Comments 13-57
13.13 About Certification UI New Features 13-58
13.14 About Certification Oversight 13-60
13.15 Troubleshooting Identity Certification 13-61

14 Managing Identity Audit

14.1 About Identity Audit 14-1
14.2 Understanding Identity Audit Concepts 14-1
14.2.1 About Modes of Detection 14-2
14.2.2 About Identity Audit Rules 14-2
14.2.3 About Rule Condition 14-3
14.2.4 About Identity Audit Policies 14-3
14.2.5 About Scan Definitions 14-4
14.2.6 About Scan Jobs 14-5
14.2.7 About Policy Violations 14-5
14.2.8 About Remediators 14-5
14.2.9 Understanding Policy Violation Remediation 14-5
14.2.9.1 About Policy Violation Remediation 14-6
14.2.9.2 About Violation Causes 14-6
14.2.9.3 About Policy Violation States 14-7
14.2.10 About Policy Violation Reports 14-7
14.3 Enabling Identity Audit 14-7
14.4 Configuring Identity Audit 14-8

14.4.1 Setting Identity Audit Options 14-8
14.4.2 Understanding Configuring Reminders, Notifications, Escalations, and Expiry for Identity Audit 14-9
14.4.2.1 Understanding Email Notification and Reminders for Identity Audit 14-10
14.4.2.2 Configuring Reminders, Notifications, Escalations, and Expiry for Identity Audit (Optional) 14-10
14.5 Managing Identity Audit Rules 14-10
14.5.1 Searching Identity Audit Rules 14-11
14.5.1.1 Performing Basic Search for Identity Audit Rules 14-11
14.5.1.2 Performing Advanced Search for Identity Audit Rules 14-11
14.5.2 Creating Identity Audit Rules 14-12
14.5.3 Understanding Identity Audit Rule Expressions 14-15
14.5.4 Modifying Identity Audit Rules 14-15
14.5.5 Duplicating Identity Audit Rules 14-16
14.5.6 Deleting Identity Audit Rules 14-17
14.6 Managing Identity Audit Policies 14-17
14.6.1 Searching Identity Audit Policies 14-17
14.6.1.1 Performing Basic Search for Identity Audit Policies 14-17
14.6.1.2 Performing Advanced Search for Identity Audit Policies 14-18
14.6.2 Creating Identity Audit Policies 14-18
14.6.3 Modifying Identity Audit Policies 14-20
14.6.4 Duplicating Identity Audit Policies 14-20
14.6.5 Deleting Identity Audit Policies 14-20
14.6.6 Previewing the Results of Identity Audit Policies 14-21
14.7 Managing Scan Definitions 14-22
14.7.1 Searching Scan Definitions 14-22
14.7.1.1 Performing Basic Search for Scan Definitions 14-22
14.7.1.2 Performing Advanced Search for Scan Definitions 14-23
14.7.2 Creating Scan Definitions 14-23
14.7.3 Modifying Scan Definitions 14-25
14.7.4 Running and Viewing Scans 14-25
14.8 Managing Policy Violations 14-26
14.8.1 Introducing Identity Audit Policy Violation Page in Identity Self Service 14-26
14.8.2 Searching Policy Violations 14-27
14.8.2.1 Performing Basic Search for Policy Violations 14-27
14.8.2.2 Performing Advanced Search for Policy Violations 14-27
14.8.3 Opening Policy Violation Details 14-28
14.8.4 Completing Policy Violations 14-28
14.8.5 Closing Policy Violations 14-29
14.8.6 Remediating or Closing Policy Violations Causes 14-29
14.8.7 Generating Identity Audit Policy Violation Reports 14-30

Part IV Working with Identity Administration

15 Managing Users

15.1 Searching Users 15-1
15.1.1 Performing Basic Search for Users 15-1
15.1.2 Performing Advanced Search for Users 15-2
15.1.3 Operations on Search Results 15-3
15.2 Creating a User 15-4
15.3 Viewing User Details 15-6
15.4 Modifying Users 15-7
15.4.1 Editing User Attributes 15-8
15.4.2 Requesting, Removing, and Modifying Roles 15-8
15.4.2.1 Requesting Roles for a User 15-8
15.4.2.2 Modifying a Role 15-9
15.4.2.3 Removing Roles from a User 15-9
15.4.2.4 Modifying Role Grant Duration 15-9
15.4.3 Requesting and Removing Entitlements 15-10
15.4.3.1 Requesting Entitlements for a User 15-10
15.4.3.2 Removing Entitlements from a User 15-11
15.4.3.3 Modifying Entitlement Grant Duration 15-11
15.4.4 Requesting, Removing, and Modifying Accounts 15-12
15.4.4.1 Understanding Requesting for an Account 15-12
15.4.4.2 Modifying an Account 15-13
15.4.4.3 Removing an Account 15-13
15.4.4.4 About Multiple Accounts in Single Application Instance 15-13
15.4.4.5 Marking an Account as Primary 15-14
15.4.4.6 Disabling an Account 15-14
15.4.4.7 Enabling an Account 15-14
15.4.4.8 Modifying Account Grant Duration 15-14
15.4.5 Modifying Details of Direct Reports 15-15
15.4.6 Managing Proxies 15-15
15.4.6.1 Adding a Proxy User 15-16
15.4.6.2 Editing a Proxy User 15-17
15.4.6.3 Removing a Proxy User 15-17
15.5 Disabling a User 15-18
15.6 Enabling a User 15-18
15.7 Deleting a User 15-19
15.8 Locking a User Account 15-19
15.9 Unlocking a User Account 15-20

15.10 Resetting the User Password 15-21

16 Managing Roles

16.1 About Roles 16-1
16.2 Role Membership Inheritance 16-1
16.2.1 About Role Membership Inheritance 16-2
16.2.2 Evaluating Access Granted to User Through Role Inheritance 16-4
16.3 Default Roles 16-4
16.4 Creating Roles 16-5
16.5 Managing Roles 16-10
16.5.1 Searching for Roles 16-10
16.5.1.1 Performing Basic Search for Roles 16-10
16.5.1.2 Performing Advanced Search for Roles 16-11
16.5.2 Viewing and Administering Roles 16-12
16.5.2.1 Opening Role Page 16-12
16.5.2.2 About Attributes Tab 16-13
16.5.2.3 Understanding Hierarchy Tab 16-13
16.5.2.4 The Access Policy Tab 16-15
16.5.2.5 The Members Tab 16-16
16.5.2.6 The Organizations Tab 16-20
16.5.2.7 The History Tab 16-21
16.5.3 Displaying Role Analytics 16-23
16.5.3.1 About Viewing Role Analytics 16-23
16.5.3.2 Viewing Role Analytics 16-24
16.5.4 Deleting Roles 16-26

17 Managing Access Policies

17.1 Terminologies Used in Access Policies 17-1
17.2 Features of Access Policies 17-2
17.2.1 Direct Provisioning 17-2
17.2.2 Revoking or Disabling the Policy 17-2
17.2.3 Role Hierarchy 17-3
17.2.4 Denying a Resource 17-3
17.2.5 Evaluating Policies 17-4
17.2.6 Evaluating Policies for Reconciled and Bulk Load-Created Accounts 17-5
17.2.7 Evaluating Policies for Direct Provisioned and Request Created Accounts 17-6
17.2.8 Access Policy Priority 17-7
17.2.9 Access Policy Data 17-8
17.2.10 Provisioning Multiple Instances of the Same Resource via Access Policy by Using Account Discriminator 17-8

17.2.11 Access Policy Authorization 17-9
17.3 Creating Access Policies 17-10
17.4 Managing Access Policies 17-12
17.5 Deleting Access Policies 17-12
17.6 Provisioning Multiple Instances of the Same Resource via Access Policy 17-13
17.6.1 Enabling Multiple Account Provisioning 17-13
17.6.2 Creating Separate Accounts for the Same User and Same Resource on a Single Target System 17-14
17.6.3 Provisioning Multiple Instances of a Resource to Multiple Target Systems 17-15
17.6.4 Limitation of Provisioning Multiple Instances of a Resource via Access Policy 17-15
17.7 Troubleshooting Issues with Evaluate User Policy Scheduled Job 17-16

18 Managing Organizations

18.1 About Organization Entity 18-1
18.2 Searching Organizations 18-1
18.2.1 Performing Basic Search for Organization 18-2
18.2.2 Performing Advanced Search for Organization 18-2
18.3 Creating an Organization 18-3
18.4 Viewing and Modifying Organizations 18-4
18.4.1 Opening Organization Details 18-5
18.4.2 Modifying Organization Attributes 18-5
18.4.3 Managing Child Organizations 18-5
18.4.3.1 Creating a Child Organization 18-5
18.4.3.2 Deleting a Child Organization 18-6
18.4.3.3 Disabling a Child Organization 18-6
18.4.3.4 Enabling a Child Organization 18-6
18.4.3.5 Opening a Child Organization 18-6
18.4.4 Viewing Organization Membership 18-6
18.4.5 Managing Dynamic Organization Membership 18-7
18.4.5.1 About Dynamic Organization Membership Rule 18-7
18.4.5.2 Creating a Dynamic Organization Membership Rule 18-7
18.4.5.3 Modifying a Dynamic Organization Membership Rule 18-9
18.4.5.4 Deleting a Dynamic Organization Membership Rule 18-9
18.4.6 Managing Admin Roles 18-9
18.4.6.1 About Admin Role in Organization Details 18-10
18.4.6.2 Granting an Admin Role 18-10
18.4.6.3 Revoking an Admin Role 18-10
18.4.7 Viewing Available Accounts 18-11
18.4.8 Viewing Provisioned Accounts 18-11
18.4.8.1 Provisioning a Resource 18-11
18.4.8.2 Revoking a Resource 18-12

18.4.8.3 Viewing the Details of a Provisioned Resource 18-12
18.4.8.4 Disabling a Provisioned Resource 18-12
18.4.8.5 Enabling a Provisioned Resource 18-12
18.4.8.6 Viewing Resource History 18-12
18.4.9 Viewing Available Entitlements 18-13
18.5 Creating a User Member 18-13
18.6 Creating a Sub-Organization 18-14
18.7 Disabling and Enabling Organizations 18-14
18.7.1 Disabling an Organization 18-14
18.7.2 Enabling an Organization 18-15
18.8 Deleting an Organization 18-15

19 Managing Administration Roles

19.1 About Administration Roles in Oracle Identity Governance 19-1
19.2 Introducing Admin Roles 19-2
19.3 Understanding the Admin Role Attributes 19-2
19.3.1 About Admin Role Capability 19-2
19.3.2 About Admin Role Scope of Control 19-3
19.3.3 About Admin Role Publication 19-3
19.4 Searching Admin Role 19-3
19.4.1 Performing Basic Search for Admin Role 19-4
19.4.2 Performing Advanced Search for Admin Role 19-4
19.5 Creating an Admin Role 19-5
19.6 Viewing and Modifying Admin Role 19-7
19.7 Deleting Admin Role 19-8
19.8 Controlling End User Actions 19-9

20 Managing Password Policies

20.1 About Password Policies 20-1
20.2 Searching Password Policies 20-1
20.2.1 Performing Basic Search for Password Policies 20-2
20.2.2 Performing Advanced Search for Password Policies 20-2
20.3 Creating a Password Policy 20-2
20.4 Understanding Password Policy Rules 20-3
20.4.1 Password Policy Rules 20-4
20.4.2 Setting Password Policy Rules 20-4
20.5 Evaluating Password Policies 20-11
20.6 Setting Challenge Options 20-11
20.7 Deleting a Password Policy 20-13

20.8 Associating Password Policies with Organization 20-13

21 Managing Application Onboarding

21.1 About Application Onboarding 21-1
21.1.1 What Is Application Onboarding? 21-2
21.1.2 Application Onboarding Concepts 21-2
21.1.2.1 Application Authorization 21-2
21.1.2.2 Application Types 21-3
21.1.2.3 Application Templates 21-3
21.1.2.4 Disconnected Applications 21-4
21.1.2.5 Instance Creation 21-4
21.1.2.6 Cloning Applications 21-5
21.1.2.7 Validation and Transformation of Provisioning and Reconciliation Attributes 21-5
21.1.2.8 Important Elements in the Application Template XML 21-6
21.2 Searching Applications 21-9
21.3 Creating Applications 21-10
21.3.1 Creating a Target Application 21-10
21.3.1.1 Providing Basic Information for Target Application 21-10
21.3.1.2 Providing Schema Information for Target Application 21-12
21.3.1.3 Providing Settings Information for Target Application 21-14
21.3.1.4 Verifying the Target Application Details 21-21
21.3.2 Creating an Authoritative Application 21-21
21.3.2.1 Providing Basic Information for Authoritative Applications 21-21
21.3.2.2 Providing Schema Information for Authoritative Application 21-22
21.3.2.3 Providing Settings Information for Authoritative Application 21-23
21.3.2.4 Verifying the Authoritative Application Details 21-27
21.4 Creating Templates 21-27
21.4.1 Creating an Authoritative Template 21-27
21.4.2 Creating a Target Template 21-28
21.5 Modifying Applications 21-28
21.5.1 Editing an Application That Was Created by Using the Connector Installation Wizard 21-28
21.5.2 Editing Applications 21-29
21.5.3 Editing Templates 21-29
21.6 Cloning Applications 21-29
21.7 Creating Instance Applications 21-30
21.8 Creating Applications in Bulk 21-31
21.9 Configuring Flat Files 21-32
21.9.1 Providing Basic Information for Flat Files 21-32
21.9.2 Providing Settings Information for Flat Files 21-33

21.9.3 Adding a New Field to the Schema for a Disconnected Application 21-33
21.10 Managing Flat File Configurations 21-34
21.11 Managing Jobs 21-35
21.12 Upgrading Connector Applications 21-36
21.12.1 About Upgrading Applications 21-36
21.12.2 Upgrading Applications 21-36
21.12.3 Viewing the Upgrade Status 21-39
21.13 Deleting Applications 21-40
21.14 About Customizing Groovy Scripts 21-40
21.15 Troubleshooting Application Onboarding 21-43

22 Managing the Scheduler

22.1 About Scheduler 22-1
22.2 Configuring the oim-config.xml File 22-2
22.3 Review Dashboard 22-3
22.4 Scheduled Tasks 22-4
22.4.1 About Scheduled Tasks 22-4
22.4.2 Predefined Scheduled Tasks 22-5
22.4.3 Creating Custom Scheduled Tasks 22-25
22.5 Managing Jobs 22-26
22.5.1 Searching for Jobs 22-27
22.5.2 Creating Jobs 22-27
22.5.3 Editing and Viewing Jobs 22-29
22.5.4 Modifying Jobs 22-31
22.5.5 Disabling and Enabling Jobs 22-31
22.5.6 Running the Jobs 22-31
22.5.7 Deleting Jobs 22-32
22.6 Diagnosing Scheduled Jobs 22-32
22.6.1 Schedule Job Errors 22-32
22.6.2 Resolving the Schedule Job Errors 22-33
22.6.3 Configuring a Custom Property to Avoid Delay in Scheduled Job Run 22-34

23 Managing System Properties

23.1 About System Properties 23-1
23.2 Types of System Properties 23-1
23.2.1 Default System Properties in Oracle Identity Governance 23-1
23.2.2 Non-Default System Properties in Oracle Identity Governance 23-23
23.3 Managing System Properties 23-25
23.3.1 Searching for System Properties 23-25

23.3.2 Adding System Properties 23-26
23.3.3 Editing System Properties 23-26
23.3.4 Deleting System Properties 23-27
23.3.5 Purging Cache 23-27

24 Managing Notifications Template Services

24.1 About Notification Providers 24-1
24.2 Default Notification Template 24-2
24.3 Managing Notification Templates 24-2
24.3.1 Searching for a Notification Template 24-3
24.3.1.1 Performing Template Name Search for a Notification 24-3
24.3.1.2 Performing Locale Specific Notification Template Search 24-3
24.3.2 Adding a Template 24-4
24.3.3 Modifying a Notification Template 24-5
24.3.4 Enabling or Disabling a Notification Template 24-5
24.3.5 Deleting Notification Templates 24-6
24.3.5.1 Deleting a Notification Template 24-6
24.3.5.2 Deleting a Locale Specific Notification Template 24-7

Part V Reporting

25 Running Reports

25.1 Running Oracle Identity Governance Reports 25-1
25.2 Running Policy Violation Reports 25-2

Part VI Appendix

A Personalizing Self Service

A.1 Performing Search in Self Service A-1
A.1.1 Performing Basic Search in Self Service A-1
A.1.2 Performing Advanced Search in Self Service A-2
A.2 Adding and Removing Attributes in Advanced Search Criteria A-3
A.3 Personalizing the Search Result A-3
A.4 Using Saved Search A-4
A.4.1 Creating a Saved Search A-4
A.4.2 Personalizing Saved Search A-5
A.4.3 Deleting a Saved Search A-5

A.4.4 Using Saved Search to Perform a Search Operation A-6
A.5 Sorting Data in Search Results A-6
A.6 Using Query By Example A-6

B Functional Capabilities

B.1 List of Authorization Functional Capabilities B-1
B.2 List of Self Capabilities B-17

C Sample Application Template XML

List of Figures

1-1	Login Page of Oracle Identity Self Service	1-2
1-2	Home Page of Oracle Identity Manager Self Service Interface	1-3
1-3	Layout of the Help Interface	1-5
6-1	Policy Violation	6-19
6-2	The Policy Violations Dialog Box	6-19
12-1	The Certification Tab	12-13
13-1	Rule for Auto-approval	13-39
13-2	Stages of Certification in TPAD	13-48
13-3	Phase One With Verification	13-50
13-4	Phase Two With Verification	13-54
13-5	Final Review Phase	13-56
13-6	Certification Comments	13-58
14-1	Rule Conditions	14-16
16-1	Role Membership Inheritance	16-3
16-2	The Expression Builder	16-18
17-1	Access Policy Evaluation	17-4
17-2	Access Policy Harvesting Flow	17-6
18-1	Dynamic Organization Membership Rule	18-8
21-1	Flat File Full	21-19

List of Tables

6-1	Icons Denoting Catalog Item Type	6-2
8-1	Columns in the My Tasks Page	8-2
9-1	Fields in the Provisioning Tasks Search Results Table	9-3
9-2	Fields in the Task Details Window	9-4
9-3	Fields in the Task History Window	9-7
12-1	The Four Types of Identity Certification	12-2
12-2	Identity Certification Reviewers	12-3
12-3	Certification Name Formats	12-6
13-1	CERT_CUSTOM_ACCESS_REVIEWERS Table Definition	13-4
13-2	Sample CERT_CUSTOM_ACCESS_REVIEWERS Table	13-6
13-3	Configuration Properties	13-14
13-4	Risk Factors	13-34
13-5	Actions or System Events That can Impact Risk Summary Values	13-37
13-6	Troubleshooting Identity Certification Issues	13-61
14-1	Identity Audit or IDA Configuration Settings	14-9
14-2	Fields in the Create Policy Page	14-19
15-1	Fields in the Create User Page	15-4
16-1	Default Roles in Oracle Identity Manager	16-4
20-1	Fields in the Policy Rules Section	20-5
20-2	Fields in Custom Policy Section	20-7
20-3	Fields in the Challenge Option Section	20-12
22-1	Child Elements of the Scheduler Element	22-2
22-2	Predefined Scheduled Tasks	22-5
23-1	Default System Properties in Oracle Identity Governance	23-2
23-2	Non-Default System Properties	23-23
24-1	Default Notification Templates	24-2
B-1	Authorization Functional Capabilities	B-1
B-2	Self Capabilities	B-17

Preface

The Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance introduces you to Oracle Identity Self Service tasks, and delegated administration functionalities.

Audience

This guide is intended for users who can log in to Oracle Identity Self Service and perform self-service operations, request for roles and resources, and manage various approval, provisioning, and certification tasks. This guide is also intended for delegated administrators who can perform identity administration tasks and define authorization policies to delegate administration privileges. In addition, a user with any role can refer to this guide for an introduction and conceptual information about Oracle Identity Governance.

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 more information, see the other documents in the Oracle Identity Management documentation set for this release.

- *Oracle Fusion Middleware Administering Oracle Identity Governance*
- *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*
- *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*

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

This section summarizes the new features and significant changes in *Performing Self Service Tasks with Oracle Identity Governance* in the Oracle Fusion Middleware 12c (12.2.1.4.0).

Follow the pointers into this guide to get more information about the features and how to use them.

Updates in October 2023 Documentation Refresh for 12c (12.2.1.4.0)

In addition to bug fixes and editorial corrections, this revision of *Performing Self Service Tasks with Oracle Identity Governance* contains the following changes:

- Admin users can create membership rules by assigning members to a role using an SQL query.
  For more information refer to Creating Roles.
- The following new system properties are available, see Default System Properties in Oracle Identity Governance for more information.
  - Enable SQL query based Role Membership
  - Evaluate All Role for SQL Membership Rule in Refresh Role Membership Job
  - Shows Revoked Accounts In the Accounts Tab
  - Proxy Delegate Enabled

Updates in April 2023 Documentation Refresh for 12c (12.2.1.4.0)

In addition to bug fixes and editorial corrections, this revision of *Performing Self Service Tasks with Oracle Identity Governance* contains the following changes:

- To enhance the user experience, the following UI option is now available under the **Oracle Identity Self Service** which was earlier available under the **System Administration** section.
  - **Manage Notification Templates**

  For more information refer to Managing Notifications Template Services .
- The **Proxy Users** tab is now available under the **Oracle Identity Self Service**, option as part of the **User Details** page.
  For more information, refer to Managing Proxies.

- While creating Identity Audit Policies, you can disable the **Close as Risk Accepted** action.
  For more information, refer Creating Identity Audit Policies.

Updates in October 2022 Documentation Refresh for 12c (12.2.1.4.0)

In addition to bug fixes and editorial corrections, this revision of *Performing Self Service Tasks with Oracle Identity Governance* contains the following changes:

- To enhance the user experience, the following UI options are now available under the **Oracle Identity Self Service** which were earlier available under the **System Administration** section.
  - **Manage Scheduler**
  - **Manage System Properties**

  For more information refer to the topics Managing the Scheduler and Managing System Properties.
- While configuring Certification, you can now disable Accounts for the revoke action. For more information, see Configuring Certification Options.

Updates in October 2021 Documentation Refresh for 12c (12.2.1.4.0)

In addition to bug fixes and editorial corrections, this revision of *Performing Self Service Tasks with Oracle Identity Governance* contains the following changes:

- After you apply Oracle Identity Governance Bundle Patch 12.2.1.4.211010, a new option is available that enables the account as active when the user has entitlements provisioned outside of the Access Policies. See Revoking or Disabling the Policy.
- After you apply Oracle Identity Governance Bundle Patch 12.2.1.4.211010, the Certification review supports mandatory certification comments on certify and non certify operations. See About Pre-poulate Certification Comments.

Updates in April 2021 Documentation Refresh for 12c (12.2.1.4.0)

In addition to bug fixes and editorial corrections, this revision of *Performing Self Service Tasks with Oracle Identity Governance* contains the following changes:

- After you apply Oracle Identity Governance Bundle Patch 12.2.1.4.210428, identity sudit policy validation takes place for in-flight requests. See Predictive Policy Validation for In-Flight Requests.
- After applying Oracle Identity Governance Bundle Patch 12.2.1.4.210428, a new **Revoke Access** option is available for completing user certifications to revoke the roles and entitlements of the active user. See Making Certification Decision on the Users.

- After applying Oracle Identity Governance Bundle Patch 12.2.1.4.210428, the Content Selection page for creating user certification definition provides the **Roles Outside Rules** and **High Risk Outside Rules** options. See step 10 of Creating a User Certification Definition.

Updates in October 2020 Documentation Refresh for 12c (12.2.1.4.0)

In addition to bug fixes and editorial corrections, this revision of *Performing Self Service Tasks with Oracle Identity Governance* contains the following change:

- After applying Oracle Identity Governance Bundle Patch 12.2.1.4.201011, a new system property XL.APHarvesting.AllowAccountDataUpdate is available that you can use to update the account data with the policy defaults for the accounts linked to the access policies. See Evaluating Policies for Direct Provisioned and Request Created Accounts.

Updates in July 2020 Documentation Refresh for 12c (12.2.1.4.0)

In addition to bug fixes and editorial corrections, this revision of *Performing Self Service Tasks with Oracle Identity Governance* contains the following change:

- After applying Oracle Identity Governance Bundle Patch 12.2.1.4.200624, a new system property `OIM Complex Password Policy compatible with Active Directory` is available that lets you replace the last rule (inclusion of user ID, first name, or last name in password) of the OIG complex password policy with the Active Directory (AD) password policy (inclusion of Display Name and User Login in password). See Setting Password Policy Rules.

New and Changed Features for 12c (12.2.1.4.0)

Oracle Identity Governance 12c (12.2.1.4.0) includes the following new and changed self service features for this document.

- The application onboarding capability in Identity Self Service has been enhanced to enable you to configure and manage flat files, manage jobs, and upgrade connector applications. See Configuring Flat Files, Managing Flat File Configurations, Managing Jobs, and Upgrading Connector Applications.
- List of challenge questions is updated for this release. See Challenge Questions and Responses After First Login.
- Setting challenge questions requires authentication. See Setting Challenge Questions and Responses.
- For parent or child form modification requests, a change indicator indicates the modified fields in the approval form. See Approving a Task.

  Similarly, for parent form modification requests, a change indicator indicates the modified fields in the manual fulfillment form. See Completing a Task.

- In the base selection for user, role, and entitlement certification definitions, you can filter the criteria based on various user, role, and entitlement attributes and user defined fields (UDFs). You can also save the filter criteria and use it for creating other user, role, and entitlement certification definitions. See Creating a User Certification Definition, Creating a Role Certification Definition, and Creating an Entitlement Certification Definition.
- Access policies are linked to accounts created by requests and to accounts that are provisioned directly. See Evaluating Policies for Reconciled and Bulk Load-Created Accounts.

1

Understanding the Oracle Identity Self Service Interface

Oracle Identity Self Service interface provides users access to self service and delegated identity administration features of Oracle Identity Governance.
This chapter will help you familiarize with Oracle Identity Self Service. This will enable you to quickly find the information you need and complete the required tasks easily.

The interface of Identity Self Service is composed of the following areas:

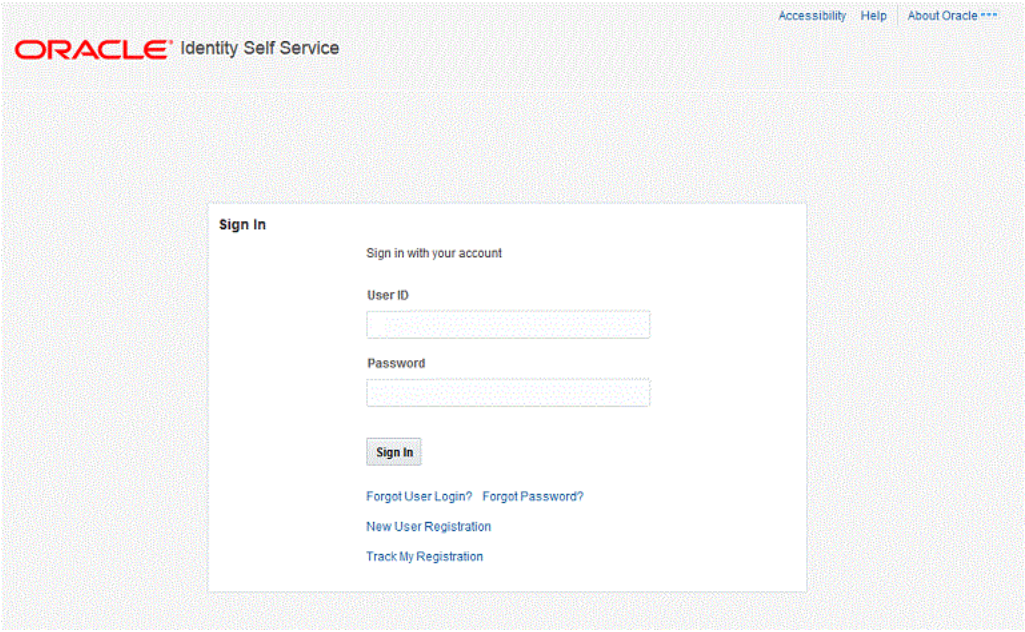
- About Oracle Identity Self Service Interface
- Top Panel of Oracle Identity Self Service Interface
- About Help Link
- Self Service Home page in Oracle Identity Self Service Interface
- Compliance Home Page in Oracle Identity Self Service Interface
- Manage Home page in Oracle Identity Self Service Interface

1.1 About Oracle Identity Self Service Interface

Unauthenticated self service tasks are the ones you can perform before logging in to Identity Self Service, such as registering and signing in. Authenticated self service tasks are the ones you can perform after logging in to Identity Self Service, such as self service and identity administration tasks.

Figure 1-1 shows the page to access authenticated self service and unauthenticated self service interface.

Figure 1-1 Login Page of Oracle Identity Self Service

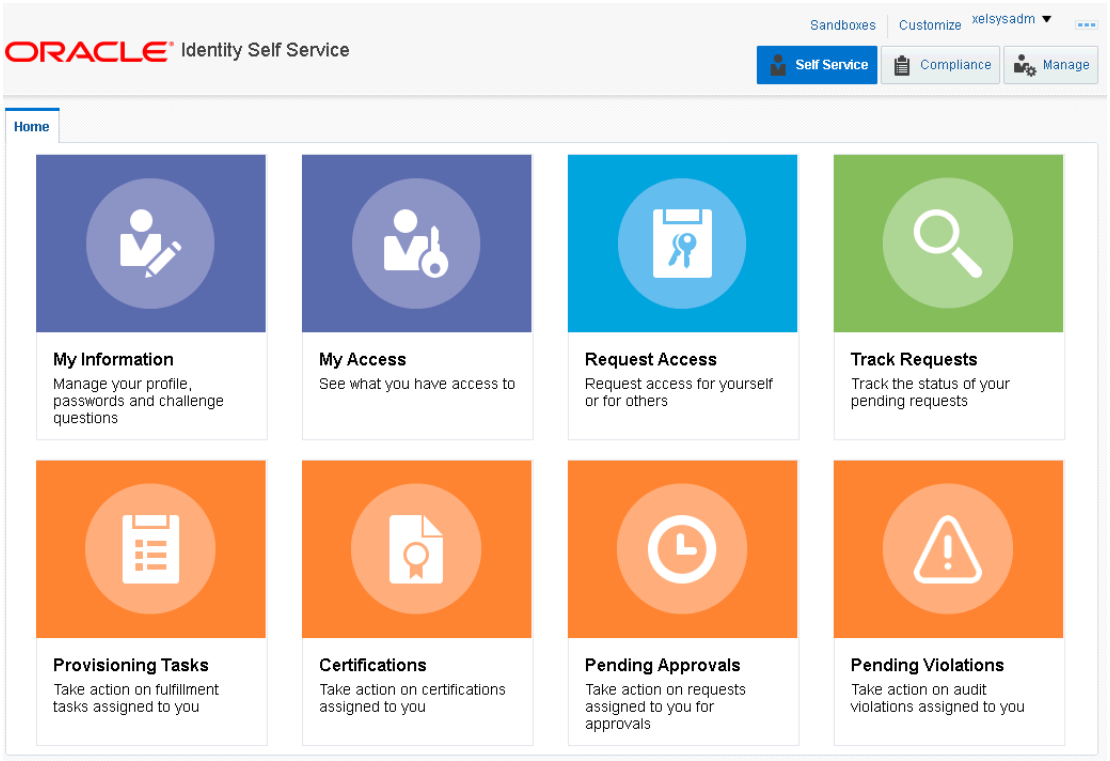


Identity Self Service supports access to unauthenticated self-service tasks in the Unauthenticated Self Service interface. Users who have not authenticated into, or not logged in to Identity Self Service can access the Unauthenticated Self Service Interface by clicking the Forgot User Login?, Forgot Password?, New User Registration, or Track My Information links. This interface enables an unauthenticated user to retrieve a forgotten user login ID or password, register to the Oracle Identity Manager environment, and track the registration.

For more information, see Registering to Oracle Identity Governance and Accessing Oracle Identity Self Service.

Access to authenticated self-service tasks is available by logging in to Identity Self Service shown in Figure 1-2.

Figure 1-2 Home Page of Oracle Identity Manager Self Service Interface



1.2 Top Panel of Oracle Identity Self Service Interface

The top panel of Identity Self Service contains links, such as Sandboxes, Customize, Accessibility, Help, Inbox, and Sign Out.

The options that are available are described below:

- **Accessibility Link:** Identity Self Service has been designed to adhere to the standards set in Section 508 of the Rehabilitation Act and the World Wide Web Consortium's Web Content Accessibility Guidelines 2.0 AA (WCAG 2.0 'AA").

  When you click the Accessibility link in the upper right corner of the page, the Accessibility dialog box is displayed. You can select none or more from the following options in the Accessibility dialog box:

  - **I use a screen reader:** Select this option if you want to use a screen reader.
  - **I use high contrast colors:** Select this option to use the high-contract color scheme that you have specified in your operating system, rather than using the default color scheme specified in Identity Self Service.
  - **I use large fonts:** Select this option if you want to change the font size for easy viewing and readability.
- **Sandboxes Link:** When you click the Sandboxes link in the upper right corner of the page, the Manage Sandboxes page is displayed. Sandboxes allow you to isolate and experiment with customization without affecting other users environments. To customize, create and/or activate a sandbox. After customizations are complete you can publish the sandbox to make the customizations available to other users.

- **Customize Link:** When you click the Customize link in the upper right corner of the page, the WebCenter Composer is opened. The currently active page opens in customization mode. You can customize the page in design or source view.
- **Inbox Link:** Use the Inbox to perform the following:
  - View and manage approval tasks that correspond to requests that are in the user or administrator's queue to be approved.

    For more information, see Managing Pending Approvals .
  - View and manage certification review tasks assigned to the logged-in user.

    For more information, see Using the Unified Inbox and Managing Certification Review Tasks .
- **Signing Out of Identity Self Service:** Click the Sign Out link to log out of Identity Self Service.

1.3 About Help Link

The default view of the help system consists of three panes, Top Pane, Lower Left Pane, and Lower Right Pane. They are described in the following topics:

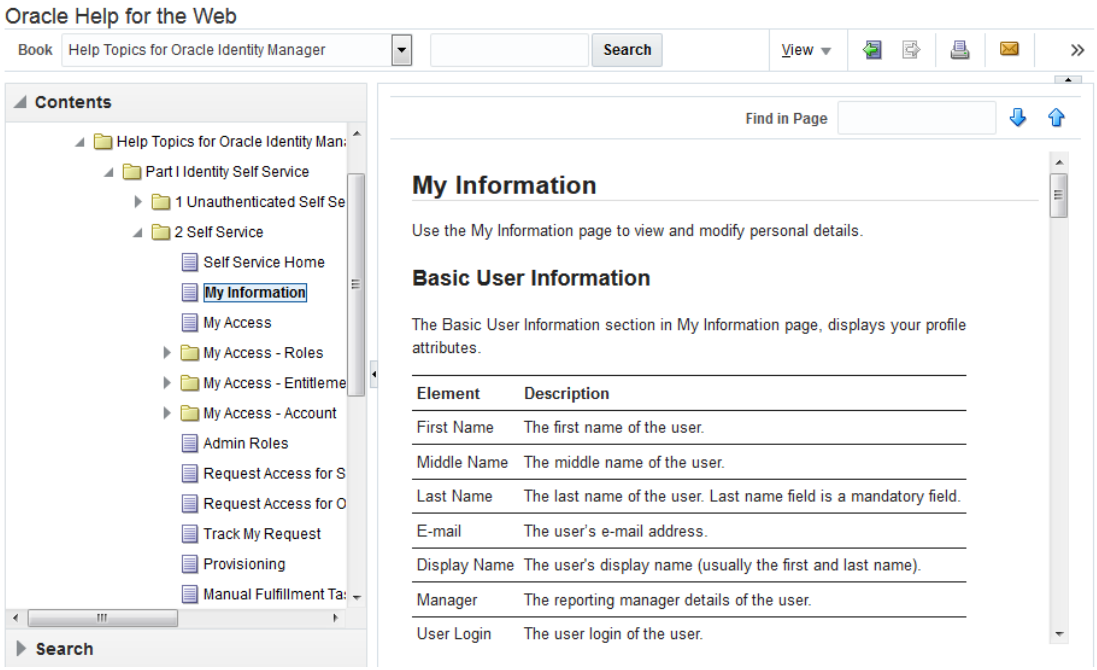
- About Help System
- About Top Pane in Help Page
- About Lower Left Pane in Help Page
- About Lower Right Pane in Help Page

1.3.1 About Help System

Identity Self Service includes a help system. Clicking the Help link opens the help system in a new window. In addition, Identity Self Service provides context-sensitive help. For example, if you are in the Catalog page and click the Help link, then help content related to the request catalog is displayed.

Figure 1-3 shows a sample page and default layout of the help interface.

Figure 1-3 Layout of the Help Interface



1.3.2 About Top Pane in Help Page

The top pane consists of the following:

- Book drop-down list: From this drop-down list you can select one of the following values:
  - **Help Topics for Oracle Identity Manager:** Select this value to open all help topics for Oracle Identity Manager.
  - **User's Guide for Oracle Identity Manager:** Select this value to open the online help version of Oracle Fusion Middleware User's Guide for Oracle Identity Manager.
  - **Custom Help Topics for Oracle Identity Manager:** Select this value to open any custom help topics.
- Search field: Specify any word or term to search for in the help system.
- View: From the View menu, you can select any one of the following options:
  - **Maximize Reading Pane:** Collapses the lower left pane to maximize the reading pane, which is the lower right pane.
  - **Restore Default Window Layout:** Restore the current layout of the help system to the default layout.
  - **Contents:** Restores the lower left pane to display the Contents region along with the help topics, if it is not already being displayed.
  - **Search:** Displays the Search region in the lower left pane. In the Search region, you can search for help topic and the search results are displayed in a tabular format. Here are a few guidelines on performing a search:
    - Search criterion specified in the Search field can be made case sensitive by selecting the **Case Sensitive** option.

        - To define your search precisely, you can specify the boolean operators & (for AND), |(for OR), ! (for NOT) in your search criterion, select the **Boolean expression** option, and then click **Search.**
        - To search for help topics containing all words specified in the search criterion, select **All words.**
        - To search for help topics containing any word specified in the search criterion, select **Any words.**
    - **Show permanent link for this topic page:** If you want to save the link to a help topic for future reference, then from the View menu, select **Show permanent link for this topic page.** In the dialog box that is displayed, right-click the link to the help topic and select one of the following options:
        - **Bookmark This Link:** Adds the help topic URL to the browser bookmarks.
        - **Copy Link Location:** Copies the help topic URL to the clipboard.
- Toolbar: The help system contains a toolbar that provides action buttons for certain tasks. You can view the name of the button by moving the mouse pointer over the button. The following buttons are available:
    - **Go back one page:** Takes you back to the page containing the previous help topic.
    - **Go forward one page:** This icon is enabled only if you have clicked the **Go back one page** icon. Clicking the **Go forward one page icon** takes you to the next page in the sequence of topics you visited.
    - **Print this topic page:** Prints the current help topic.
    - **Email this topic page:** Drafts an email with a link to the help topic currently displayed in the help system. This draft can be sent to the desired email recipient.
    - **Link to this topic page:** Saves the link to a help topic for future reference by right-clicking the link to the help topic in the dialog box that is displayed, and then selecting one of the following options:
        - **Bookmark This Link:** Adds the help topic URL to the browser bookmarks.
        - **Copy Link Location:** Copies the help topic URL to the clipboard.

1.3.3 About Lower Left Pane in Help Page

The left pane contains the Contents and Search regions. By default, the Contents region is expanded. The Contents region displays links to help topics depending on the option you select from the Book drop-down list in the top pane. You can click the arrow icon beside Contents to expand or collapse the Contents region.

1.3.4 About Lower Right Pane in Help Page

The lower right pane displays any help topic that you search for or open from the Contents and Search regions in the lower left pane. This pane is also known as the reading pane.

1.4 Self Service Home page in Oracle Identity Self Service Interface

The Self Service Home page provides access to the various regions of the Self Service tab.

The Services that are available are listed below:

- **My Information:** Use this page to view and modify personal details of your profile such as changing passwords, setting challenge questions and response, and so on. For more information, see Managing Profile Information .
- **My Access:** This page displays entities such as Roles, Entitlements, Accounts, and Admin Roles, to which you have access. In this section, you can request for, remove, or modify entities. For more information, see Managing Access for Self .
- **Request Access:** Use this page to request for access for self or for other users. For more information, see Requesting Access .
- **Track Request:** Use this page to search for and track requests raised by you and requests raised for you. You can search for requests based on request ID, status, request type, requested date, beneficiary, and requester. For more information, see Tracking a Request.
- **Provisioning Tasks:** Use this page to take action on fulfillment tasks assigned to you. For more information, see Managing Provisioning Tasks .
- **Certifications:** Use this page to review and take action on pending certification review tasks. For more information, see Managing Certification Review Tasks .

> **Note:**
>
> This feature is available if Identity Audit feature is enabled.

- **Pending Approvals:** Use this page to take action on requests assigned to you for approvals. For more information, see Managing Pending Approvals .
- **Pending Violations:** Use this page to take action on identity audit policy violations assigned to you. For more information, see Managing Pending Violations .

> **Note:**
>
> This feature is available if Identity Audit feature is enabled.

1.5 Compliance Home Page in Oracle Identity Self Service Interface

The Compliance Home page provides links to identity certification and identity audit features of Identity Self Service.

The Compliance Home page is displayed only when the identity audit feature is enabled. See Enabling Identity Audit for information about enabling the identity audit feature.

The options available in Compliance Home page are:

- **Identity Certification:** This region provides the following options:
  - **Dashboard:** Click this to open the Certification Dashboard that provides an overview of new, in-progress, and completed certifications and allows administrators to effectively manage certification review campaigns in the system.
  - **Certification Configuration:** Click this to open the Certification Configuration page that enables you to set default options in Oracle Identity Self Service that are used during certification creation based on the type of certification.
  - **Definitions:** Click this to open the Certification Definitions page that enables you to create and manage certification definitions and launch certification campaigns.
  - **Event Listeners:** Click this to open the Event Listeners page that enables you to create and manage event listeners for event-based certifications.
  - **Risk Configuration:** Click this open the Risk Configuration page that enables you to set default item risk levels that you can assign to roles, application instances, and entitlements.

  For information, see Using Identity Certification and Managing Identity Certification .
- **Reports:** This sections contains Identity Audit Reports. For more information, see About Policy Violation Reports.

  In order for Identity Audit Reports to work, Oracle BI Publisher must be configured. For more information, see "Configuring Reports" in the *Developing and Customizing Applications for Oracle Identity Governance*.
- **Identity Audit:** This region provides the following options:
  - **Configuration:** Click this to open the Configuration page that provides the options to configure the general settings and set up the identity audit feature.
  - **Rules:** Click this to open the Rules page to create and manage identity audit rules.
  - **Policies:** Click this to open the Policies page to create and manage identity audit policies.
  - **Scan Definitions:** Click this to open the Scan Definitions page that enables you to create and manage scan definitions.
  - **Policy Violations:** Click this link to open the Policy Violations page that enables you to search, view, manage, and take action on identity audit policy violations via an interactive dashboard.

  For information, see Managing Identity Audit.

1.6 Manage Home page in Oracle Identity Self Service Interface

The Manage Home page provides access to various regions of the Manage tab.

The options that are available in Manage Home Page are:

- **Users Pane:** Use this page to view and manage users. Some of the user management tasks that you can perform in this page include creating, modifying, deleting, enabling, and disabling users. For information, see Managing Users.
- **Roles and Access Policies Pane:** Use this page to view and manage:
  - **Roles:** Some of the role management tasks that you can perform in this page include viewing, administering, creating, updating, and deleting roles. For information, see Managing Roles .
  - **Access Policies:** Some of the access policy tasks that you can perform in this page include create and manage access policy, manage provisioning multiple instances of the same resources via access policy. For information, see Managing Access Policies.
- **Organization Pane:** Use this page to view and manage organizations. Some of the organization management tasks include creating, viewing, modifying, and deleting organizations. For information, see Managing Organizations.
- **Administration Roles Pane:** Use this page to view and manage admin roles. For information, see Managing Administration Roles .
- **Password Policies Pane:** Use this page to view and manage password policy. For information, see Managing Password Policies.
- **Applications Pane:** Use this page to create and manage applications, templates, instances of applications, and clone applications. For information, see Managing Application Onboarding.

> **Note:**
>
> The Administration Roles pane and the Application pane can be viewed only by the user with respective admin role capabilities provided through the Admin Roles page of the Idetity Self Service. See Managing Administration Roles for details.

Part I
Getting Started

Oracle Identity Manager enables you to perform certain tasks from the Identity Self Service login page, such as registering to Oracle Identity Manager, logging in, retrieving forgotten user login and password, and setting challenge questions after first login.

This part describes the concepts related to Oracle Identity Manager in the following chapters:

- Registering to Oracle Identity Governance
- Accessing Oracle Identity Self Service

2
Registering to Oracle Identity Governance

Oracle Identity Governance requires you to register yourself with Oracle Identity Governance to perform self service and identity administration tasks through the Identity Self Service. This chapter discusses about registering with Oracle Identity Governance in the following topics:

- Submitting Registration Requests
- Tracking Registration Requests

2.1 Submitting Registration Requests

You can use the New User Registration option to register yourself with Oracle Identity Manager. When you register to Oracle Identity Manager, a request is generated that is subject to approval.

To register yourself with Oracle Identity Manager:

1. In the Oracle Identity Self Service login page, click **New User Registration**. The User Registration page is displayed.
2. In the **Basic Information** section, enter first name, middle name, last name, email, common name, display name, and Telephone Number in the respective fields.

   Display name is the name of the user displayed in the UI. If not specified, then it is auto-generated while creating the user.
3. In the **Enter User ID and Password** section, enter the user login name, password, and confirm password in the respective fields.
4. In the **Select your challenge questions and answers** section, select the challenge question and set an answer for each question.

   > **Note:**
   >
   > No default challenge questions are displayed if password policy has been configured with user-defined challenge questions, and you must provided your own challenge questions. For information about password policies, see Managing Password Policies.

5. Click **Register**. In the confirmation message, you are provided with a tracking Registration Request Number that you can use to track the status of your registration process.

2.2 Tracking Registration Requests

You can track your self-registration request status by using the Track My Registration option.

To track your self-registration request status:

1. In the Identity Self Service login page, click **Track My Registration**. The Track Requests page is displayed.
2. In the Tracking ID field, enter the tracking Registration Request Number that has been assigned to your registration request. Then click **Submit**. The registration request status is displayed with the following details:
   - Current status of the request

     Every self-registration request that is submitted has to go through approvals for it to be processed completely.

     If a user tracks the current status of the request, the status is shown with a description of the stage the request is in. The status would be one of the following:

     – **Pending:** This state indicates that the request is submitted and the approval is pending. In case of default approval, the following status message is displayed:

       "Obtaining request-level approval for registration."

       If the request level approval is pending. Once the request level approval is obtained, the following status message is displayed:

       "Obtaining operation-level approval for registration."

     – **Rejected:** This state indicates that the request is rejected during approval. The description indicates the reason of rejection. In case of default approval levels, if the request got disapproved at the request approval level, then the following status message is displayed:

       "Request rejected. Please call Help-Desk."

       If the request gets disapproved at the operation level or request level, then the following status message is displayed:

       "Operation approval rejected for registration."

     – **Completed:** This state indicates that the request is completed. If all the approvals have been provided and the request is successfully completed, the following status message is displayed:

       "Request has been completed."

     – **Failed:** This state indicates that the request is failed during submission. If the request submission is failed, the following status message is displayed:

       "The request registration failed."

   - Date

     This is the last request update date. When the request is submitted and approval is not done, the date shown is the request submission date. In all cases, the date always reflects the last update date.

   - Tracking ID

     This is the request number to be entered to track registration status.
3. Click **Track Another Registration** to display the status of another registration request.

   Or, click **Back to Login** to display the login page.

Note:

From this page you can only track the statuses of Self Registration Requests. If the current status indicates success, then you can go to Identity Self Service, and then enter your username and password to log in.

3

Accessing Oracle Identity Self Service

The login page provides the ability to log in, and provides a starting point for all unauthenticated operations, such as retrieving forgotten user login and password and setting challenge questions after first login.
The login page is displayed when you access Identity Self Service without authenticating either natively to Oracle Identity Manager or by using SSO. The tasks you can perform before logging in to Identity Self Service include:

- Connecting to Oracle Identity Self Service
- Retrieving Forgotten User Login
- Resetting Forgotten Password
- Challenge Questions and Responses After First Login
- Setting Challenge Questions and Responses After First Login

> **Note:**
>
> Challenge Question should be set by the User immediately after logging in to Identity Self Service for the first time.

3.1 Connecting to Oracle Identity Self Service

Provide correct user login and password to sign in to Oracle Identity Manager. You can successfully sign in if your login credentials are correct, and your user account is not locked or disabled.

To log in to Oracle Identity Self Service:

> **Note:**
>
> - If Oracle Identity Manager is configured to support native authentication, then the login link redirects you to a form in which you can authenticate by using your Oracle Identity Manager username and password.
> - If Oracle Identity Manager is configured to support Single Sign-On (SSO), then the login link redirects you to the SSO application login page.

1. Go to the Identity Self Service login page.

   For example: http://*OIM_HOST*.com:*PORT*/identity/
2. In the User ID field, enter your user login.
3. In the Password field, enter your password.

4. Click **Sign In**. If you are successfully authenticated, then you are logged in and directed to the home page in the authenticated context.

   The login attempt might generate an error, such as "Invalid sign in", because of the following reasons:

   - **Incorrect credentials:** If the user name and password entered are not correct, then an error message is displayed. This may be because of the following reasons:
     - User login does not exist
     - Password is incorrect
     - User login exists but the user is deleted

     User account will get locked if invalid login attempts exceeds maximum allowed login attempts counter. If user account gets locked, user will be allowed to login only when the lock out duration expires.
   - **Locked account:** If your user account is locked, then you are not allowed to log in even if the credentials are correct.
   - **Disabled user:** If your user account is disabled, then you are not allowed to log in.

5. If your password has expired, then the Change Password form is displayed. You are not allowed to proceed to the main page of the console without changing the password. Enter a new password, and click **Submit**.

6. If the system requires you to specify challenge responses, then specify it and click **Submit.**

   Alternatively, you can click **Cancel** if you want to avoid setting challenge questions and logging on to Identity Self Service. You set challenge questions to reset your password without calling the helpdesk. Note that these challenge questions are a unique set of questions and answers. For more information about setting challenge questions and response, see Challenge Questions and Responses After First Login.

If you attempting to access a page, for example the Pending Approvals page, and you are checking for the pending approvals from a link and you are not logged in already, then you are redirected to the login page. Follow the login instruction provided in this section to log in to Oracle Identity Manager. However, you will be directed to the page you are attempting to access, the Pending Approvals page, instead of the main page of Identity Self Service.

3.2 Retrieving Forgotten User Login

You can click the Forgot User Login option and enter your email address to retrieve your forgotten user login.

To retrieve your forgotten user login:

1. In the Identity Self Service login page, click **Forgot User Login**. The Forgot User Login page is displayed.
2. In the Email Address field, enter the email address associated with your user login.
3. Click **Submit**. An email is sent to the specified email address with further instructions.

If you enter an incorrect email address, then no error message is displayed stating that the specified user details do not exist. Therefore, ensure that the email address you enter is valid.

3.3 Resetting Forgotten Password

User password gets locked as the result of too many invalid login attempts. You can click the Forgot Password? option to reset locked password.

The Forgot Password? option is not available in the following cases:

- User is disabled or deleted
- User is locked (for reasons other than, too many invalid login attempts)
- User has not set or has set insufficient number of challenge answers
- Applicable Challenge Policy for the user is disabled

To reset your forgotten password:

1. In the Identity Self Service login page, click **Forgot Password?**. The Forgot Password page is displayed.
2. In the Identify Yourself page, enter **User Login** details and then click **Next**.

   If validation of User Login is successful then, an Email is sent to you with a link to reset your password.

   If this validation fails then, you cannot proceed to reset password and will have to contact System Administrator for assistance.
3. Open the Email you have received and click on the reset password link. The Forgot Password, Answer Challenge Questions page is displayed.
4. The Answer Challenge Questions page lists the challenge questions that you set during user registration to verify your user identity. Enter your responses to the challenge questions, and then click **Next**. The Please enter new password page is displayed.
5. In this step, enter the new password that you want to set, re-enter new password to confirm it, and then click **Save**. The following are the possible outcomes of these steps:
   - If the challenge responses specified do not match the ones set during user registration, then the following error message is displayed:

     "The number of questions answered correctly does not match the number of correct answers required. Please ensure if all questions are answered correctly."
   - If you satisfy the identity verification criteria (in other words, identifying yourself and answering the challenge questions), but the new password failed to satisfy configured password policies, then an error message is displayed.
   - If you satisfy the identity verification criteria and the password is successfully set, then the next page is displayed with a message that the password has been changed. This also unlocks your user account if it was locked by self (not locked by the system administrator manually). Click **Back to Login** to view the login screen from where you can log in to Oracle Identity Governance.

3.4 Challenge Questions and Responses After First Login

The challenge-response service allows you to set up a series of challenge questions that can be used to validate the user's identity to reset a forgotten password.

Questions and answers are stored as part of the user's profile as a name-value pair list, where the name is the question, and the value is the answer to that question. Only the user should know the correct answers to the challenge questions. For example, for user John Doe, the challenge-response set could be as follows:

Challenge	Response
Who was your fifth grade teacher?	Jean Doe
Where were you New Year’s 2000?	New York
What is the name of a city where you got lost?	New York
Where were you when you had your first kiss?	New York

> **Note:**
>
> Oracle recommends defining answers to challenge questions that cannot be guessed easily by collecting information about the user from the Internet or other public sources.

When a user's identity needs to be validated without relying on the authentication scheme, the challenge questions are asked, and the user must provide the necessary number of correct answers. Challenge questions are set in the following way:

- The System Administrator configures a predefined set of questions. See Setting Challenge Options.
- User configures the challenge questions and answers from the My Information page of the Identity Self Service. See Setting Challenge Questions and Responses.
- The System Administrator and the user configures the challenge questions. The System Administrator can configure a predefined set of questions, and the user can configure the answers for these questions from the My Information tab or immediately after logging in to Identity Self Service for the first time.

3.5 Setting Challenge Questions and Responses After First Login

You can set challenge questions and responses when Identity Self Service prompts you to do so, immediately after first login.

To set the challenge questions and responses:

1. Select questions from the Question 1, Question 2, and Question 3 fields.
2. In the corresponding Answer 1, Answer 2, and Answer 3 fields, enter the answers.
3. Click **Apply**.

Note:

Challenge questions and responses once set are not visible in this section. If you see the following message in the Challenge Questions section, then you have already set your challenge questions and responses:

Your secret questions and answers are already set.

You can modify the challenge questions and responses that you have already set by performing the procedure described earlier in this section.

Part II
Working with Self Service

Oracle Identity Manager allows you to manage personal details, approval, certification, and provisioning tasks. You can view access requests and task instances and request for entities.

It contains the following chapters:

- Managing Profile Information
- Managing Access for Self
- Requesting Access
- Using the Unified Inbox
- Managing Pending Approvals
- Managing Provisioning Tasks
- Managing Certification Review Tasks
- Managing Pending Violations

4

Managing Profile Information

Oracle Identity Self Service enables you to view and modify personal details, such as basic user information, changing enterprise password, setting challenge questions and response, viewing and modifying direct reports, and manage proxies.

The My Information page has the following sections:

- Opening My Information Page
- Managing Basic User Information
- Changing Enterprise Password
- Setting Challenge Questions and Responses
- Viewing and Modifying Direct Reports
- Managing Proxies

4.1 Opening My Information Page

To open the My Information page:

1. Log in to Identity Self Service.
2. Click the **Self Service** tab, click **My Information** box. The My Information page is displayed with sections for modifying profile attributes, changing password, setting challenge questions, viewing direct reports and their attributes, and viewing and modifying proxy users.

4.2 Managing Basic User Information

The My Information page displays the profile attributes in the Basic User Information section. You can make changes to the editable attributes. Based on product configuration the changes might need approval.

When you open the My Information page, your profile attributes are displayed in the Basic User Information section. If the section is not expanded by default, then click the arrow icon beside Basic User Information to expand the section.

Editable attributes are displayed in editable text boxes or appropriate UI widgets, such as lookup fields. You can provide new values and click the **Apply** button to submit a change.

When the profile is updated, a request may be submitted depending upon product configuration. If a request is submitted, the request number is displayed as part of the confirmation. The status of the request can be seen on the Tracking Requests page of Identity Self Service. For more information about requests and tracking, see Requesting Access .

After submitting the request for modifying profile attributes, you can click the down arrow icon beside Basic User Information to collapse the section.

4.3 Changing Enterprise Password

The My Information page displays the Change Password section that allows you to reset your enterprise password. You can specify your old password, enter a new password and re-confirm the new passwords.

The new password is evaluated for compliance against the applicable password policy. If the new password does not comply with the password policies, then the password change is rejected and you are informed of the failing condition(s). If the password evaluates successfully against all policies, then the password is changed.

To change the password:

1. In the My Information page, expand the Change Password section.
2. Specify values for the following fields:
   - **Old Password:** Enter the existing password.
   - **New Password:** Enter the new password that you want to set. Click the icon to the right of the New Password field. A list of conditions to set the password is displayed. These conditions are being specified in the password policy, and you must comply with the conditions to specify a password.
   - **Confirm New Password:** Re-enter the new password.

   For information about password policies, see Managing Password Policies.
3. Click **Apply**. If the old password is valid and the new password is in compliance with the password policy, then the password is changed. Otherwise, an error message is displayed.

4.4 Setting Challenge Questions and Responses

The My Information page displays the Challenge Questions section. A message is displayed if you have set the challenge questions and responses previously. If required, you can reset your challenge questions and responses.

To set the challenge questions and responses:

1. In the My Information page, expand the Challenge Questions section.
2. Select questions from the Question 1, Question 2, and Question 3 fields.
3. In the corresponding Answer 1, Answer 2, and Answer 3 fields, enter the answers.
4. Click **Apply**.
5. The cursor focus moves to the Password column of the Challenge Questions section. Enter your password.

4.5 Viewing and Modifying Direct Reports

The My Information page displays the user's direct report in the management hierarchy in the Direct Reports section. When you open the user details of a direct report, you can perform tasks, such as enable, disable, modify, and delete the user.

The Direct Reports section allows you to view the details of each direct report. For each user in the list, the following are displayed:

- Display Name
- User Login
- Identity Status
- Organization

If there are a large number of users as your direct reports, then you can query and find a direct report by using the Query By Example feature. For more information, see Using Query By Example.

To view and modify direct reports:

1. In the My Information page, expand the **Direct Reports** section.
2. Select a user or direct report by clicking the record of the direct report.
3. From the Actions menu, select **Open.** Alternatively, click the **Open** icon on the toolbar. The details of the user is displayed in a new tab. This tab displays the details of the user in various subtabs, such as Attributes, Roles, Entitlements, Accounts, and so on. You can click each tab to review the details of the user.

   When you open the user details of a direct report, you can perform certain tasks such as enable, disable, modify, and delete the user. You can also view the details of the direct reports of the open user, and perform certain tasks for the user, who is your indirect report. For more information, see Modifying Users.

4.6 Managing Proxies

Oracle Identity Self Service allows you to act as a proxy for another user. The My Information page displays the Proxies section that allows you to view and manage the proxy information.

This section contains the following topics:

- About Proxies
- Adding a Proxy
- Editing a Proxy
- Removing a Proxy

4.6.1 About Proxies

The Proxies section in the My Information page allows you to view and manage the proxy information. It displays the proxies currently set up within Oracle Identity Manager for you, and also allows you to view previously set up proxies. The past proxies view, which displays all proxies that were added in the past, is read-only, and no modifications are allowed.

The existing proxy view allows you to cancel an upcoming proxy whose start date is in the future. You can also edit only the end date of an in-progress proxy whose start date is in the past and end date is in future.

In the section for current proxies, you can also add new proxies. When adding new proxies, you must specify a start date, an end date, and the proxy user.

4.6.2 Adding a Proxy

To add a proxy:

1. In the My Information page, expand the **Proxies** section.

   The **Current** section displays a list of users currently set up as your proxy. The **Past** section displays a list of past proxies.

2. In the Current section, from the Actions menu, select **Add.** Alternatively, you can click **Add** on the toolbar.

   The Add Proxy dialog box is displayed.

3. For Proxy Name, select any one of the following:

   - **My Manager:** To specify your manager as proxy.
   - **Other User:** To specify any other user as proxy. To do so, click the lookup icon to search for the user you want to specify as proxy. Search for and select the user, and then click **Select** in the Search and select dialog box.

4. In the **Start Date** field, specify a start date. To do so, click the Select Date icon to the right of the Start Date field, and select a date from the calendar.
5. In the **End Date** field, specify an end date.
6. Click **Apply**. The proxy is added to the list of proxies in the Proxies section.

> **Note:**
>
> Oracle Identity Manager does not allow adding another proxy whose start and end dates overlap with the existing proxy.

Oracle Identity Manager will prevent user to add proxy which will result in recursive proxy condition.

Recursive proxy condition is when, User A is proxy for User B (for a time duration, say 17th Nov to 25th Nov), User B is proxy for User C (for a time duration, say 18th Nov to 20th Nov) and during a overlapping time duration (say 19th Nov to 26th Nov) User C is proxy for User A.

An email notification is sent on adding a proxy. The add proxy notification has the following characteristics:

- The date value in the notification is always in GMT timezone.
- The start date and end date value during proxy user creation are based on Oracle Identity Manager server timezone. For example, if the start date is specified as "6/28/2013 00:00:00 PDT", then this value is converted to GMT timezone as "06/28/2013 07:00:00 AM GMT".
- The date format in the notification is always in LONG Date/Time format and cannot be modified in its notification template.

4.6.3 Editing a Proxy

To edit a proxy:

1. In the Current section, select a proxy that you want to edit.
2. From the Actions menu, select **Edit.** Alternatively, you can click **Edit** on the toolbar.

The Edit Details dialog box is displayed.

3. In the Proxy Name field, select **My Manager** to specify your manager as proxy. Otherwise, select **Other User** to specify any other user as proxy. You can search for the user name.

> **Note:**
>
> - To change the proxy user, you can search only those users for which you have search permission.
> - You cannot modify the Proxy Name field for proxy that is in the "In Progress" state.

4. In the Start Date and End Date fields, if required, specify revised dates.

> **Note:**
>
> You cannot modify the Start Date field for a proxy that is in the "In Progress" state.

5. Click **Apply**. The edited proxy information is saved.

4.6.4 Removing a Proxy

To remove a proxy:

1. In the Current section, select a proxy that you want to remove.
2. From the Actions menu, select **Remove**. Alternatively, you can click **Remove** on the toolbar.

   When a current proxy is deleted, its end date is set as the date when it is deleted and when a future proxy is deleted, it is removed from the system.

   To remove all proxies, click **Remove All** on the toolbar, or select **Remove All** from the Actions menu.

   A message is displayed asking for confirmation.
3. Click **Yes**. The selected proxy is removed from the Current section.

5
Managing Access for Self

Oracle Identity Self Service enables you to access entities, such as roles, entitlements, accounts, and administrator roles. The entities to which you have access are listed in the My Access section.
The tasks you perform in the My Access section are described in the following topics:

- Managing Roles
- Managing Entitlements
- Managing Accounts
- Viewing Admin Roles

> **Tip:**
>
> Before you perform the steps to manage your access to entities, it is recommended that you see Requesting Access for detailed information about requests in Oracle Identity Manager

5.1 Managing Roles

Roles are used to define the access rights that an entity may have. Roles determine the links and menus that are available to users when they log in to Identity Self Service.

In the Roles tab, you can perform the following:

- Requesting for Roles
- Removing Roles
- Modifying Role Grant Duration

5.1.1 Requesting for Roles

When you submit your request for roles, it is submitted for approval. When the request is approved at all approval levels, the role is assigned to you.

To request for roles from the My Access page:

1. Log in to Identity Self Service.
2. Click **Self Service**. Self service Home page is displayed.
3. Click **My Access** box. The My Access page is displayed.
4. Click the **Roles** tab. A list of roles assigned to you are displayed.

   Click the **Granted** tab to view the roles that are granted to you. This includes both direct and indirect roles.

Click the **Pending** tab to view the roles that are approved and are pending on their future starting dates. When the starting date arrives, after the Process Pending Role Grants scheduled job runs, these roles are processed and displayed in the Granted tab. Roles that are not yet approved are not displayed in the Pending tab. You can use track request to view the status and details of such roles.

> **Note:**
>
> In all the tabs in the My Access page, you can refine your search by using Query By Example. For information see, Using Query By Example.

5. From the Actions menu, select **Request**. Alternatively, click **Request** on the toolbar. The **Role Access Request** page opens. **Catalog** tab is displayed.
6. Select a catalog item that you want to request. You can also select multiple items in the table.

   If the user wants to see information about a catalog item then, click the **i** icon next to the **Add to Cart** button. A new tab with the details about the catalog item is displayed.
7. Click **Add to Cart** that is present against the catalog item.

   The selected items are added to the request cart.
8. If you want to remove any requested catalog item from the cart, click the **Cart** icon. The **Cart Details** page is displayed. Click **Remove** button present against the request. If you want to remove all items from the cart then, click **Remove All**.
9. Click **Checkout** or click **Next**. The **Cart Details** page is displayed.
10. Enter **Request Information**.
11. Enter Grant Duration details such as **Start Date** and **End Date** or specify if grant is effective immediately by selecting the **Grant will be effective immediately upon request completion** option.

    If you do not specify a value in the **Start Date** field, then the role is assigned immediately as soon as the role is created either directly or after role creation request approval.

    If the **Start Date** is of future then grant will happen on that day, when the *Process Pending Role Grants* job is run, which is scheduled to run daily. On the **End Date** the grant on the role is revoked when the *Process Pending Role Grants* job is run.
12. Click **Submit**.

5.1.2 Removing Roles

When you submit your request for removing a role that is assigned to you, it is submitted for approval. The role is removed after the request is approved.

To remove roles assigned to you:

1. Log in to Identity Self Service.
2. Click **Self Service**. Self service Home page is displayed.
3. Click **My Access** box. The My Access page is displayed.

4. Click the **Roles** tab. A list of roles assigned to you is displayed. Select a role that you want to remove.
5. From the Actions menu, select **Remove**. Alternatively, click **Remove Roles** on the toolbar. The Remove Roles catalog page is displayed.
6. Submit the request to remove roles. The role will be removed after the request is approved.

5.1.3 Modifying Role Grant Duration

When you submit your request for change of role grant duration, the Roles tab are updated with the values you specified immediately if no approver is assigned else if approver is assigned it is updated after the approval.

To modify the grant duration of the role assigned to you or to be assigned to you:

1. Log in to Identity Self Service.
2. Click **Self Service**. Self service Home page is displayed.
3. Click **My Access** box. The My Access page is displayed.
4. Click the **Roles** tab. A list of roles assigned to you is displayed. Select a role for which you want to modify the grant duration.

   The grant duration fields, Start Date and End Date, are displayed in the Roles tab.
5. From the Actions menu, select **Modify Grant Duration**. The Modify Grant Duration dialog box is displayed.
6. In the Justification box, enter a justification for modifying the start date, or end date, or both.
7. Enter values in any one or both of the following fields:
   - **Start Date:** The start date when the role will be provisioned. This must be a future date. This field is not available for modification if the role is already assigned.
   - **End Date:** The end date when the role will be revoked.
8. Click **OK**.

   The Start Date and End Date fields in the Roles tab are updated with the values you specified immediately if no approver is assigned else if approver is assigned it is updated after the approval.

5.2 Managing Entitlements

An entitlement can be a role, responsibility, or group membership assigned to a user. The Entitlements tab in the My Access page allows you to manage the entitlements assigned to you.

In the Entitlements tab, you can perform the following:

- Requesting for Entitlements
- Modifying Entitlements
- Removing Entitlements
- Modifying Entitlement Grant Duration

5.2.1 Requesting for Entitlements

When you submit your request for entitlements, it is submitted for approval. When the request is approved at all approval levels, the entitlement is assigned to you.

To request for entitlements:

1. In the My Access page, click the **Entitlements** tab. A list of entitlements assigned to you is displayed.

   > **Note:**
   >
   > The Entitlements tab displays entitlements with the Provisioned status and Future Granted status. The status displayed here is entitlement status and not the account status.

2. From the Actions menu, click **Request**. Alternatively, click the **Request** button on the toolbar or use the **Request Entitlement** option from the Accounts tab. The Catalog page is displayed.

   > **Note:**
   >
   > You can **Request Entitlement** after Application Instance is requested, otherwise the request for entitlement will fail.

3. Select a entitlement item that you want to request. You can also select multiple items in the list.
4. Click **Add Selected to Cart** or click **Add to Cart** beside the item to be added.

   You can add items one by one by clicking **Add to Cart** beside each item. The selected items are added to the request cart.
5. Click **Checkout** or click **Next**. The Cart Details page is displayed.
6. Enter **Request Information**.
7. Enter Grant Duration details such as **Start Date** and **End Date** or specify if grant is effective immediately by selecting the **Grant will be effective immediately upon request completion** option.
8. (Optional) For the requested entitlements, enter any additional information as needed. This additional information can be added using a form associated with the entitlement, provided the entitlement forms have been generated or re-generated by system administrators.

   For example, you can enter effective start and end dates for the entitlement. Then, the approver can review and/or modify this additional information and decide whether the entitlements can be provisioned or not.

> **Note:**
>
> The corresponding application instance will also be displayed in the cart if the application instance is not already provisioned to the user.

9. Click **Submit**. The entitlement will be assigned after the request is approved.

> **Note:**
>
> If you want to save the cart in the request for editing or submitting later, then click **Save as Draft.**

5.2.2 Modifying Entitlements

When you submit your request for modifying an entitlement that is assigned to you, it is submitted for approval. The entitlement is updated after the request is approved.

To modify an entitlement assigned to you:

1. In the Entitlements tab, select the entitlement that you want to modify.
2. From the Actions menu, click **Modify**.
3. Modify and submit the request to modify entitlement. The entitlement will be modified after the request is approved.

5.2.3 Removing Entitlements

When you submit your request for removing an entitlement that is assigned to you, it is submitted for approval. The entitlement is removed after the request is approved.

To remove entitlements assigned to you:

1. In the Entitlements tab, select the entitlement that you want to remove.
2. From the Actions menu, select **Remove**. Alternatively, click **Remove** from the toolbar. The Catalog page is displayed.
3. Submit the request. The entitlement will be removed after the request is approved. Removing an Entitlement can not be done for a future date. To remove a entitlement in future you need to set the end date field in Grant Duration to that date.

> **Note:**
>
> If an account is revoked, its entitlements will be revoked. However, if an account is disabled, then its entitlements will remain granted.If entitlements have end dates and the end dates are reached, then the entitlements that are not yet revoked will be revoked.

5.2.4 Modifying Entitlement Grant Duration

When you submit your request for change of entitlement grant duration, the Entitlements tab are updated with the values you specified immediately if no approver is assigned else if approver is assigned it is updated after the approval.

To modify the grant duration of the entitlement assigned to you or to be assigned to you:

1. In the Entitlements tab of the My Access page, select an entitlement for which you want to modify the grant duration.

   The grant duration fields, Start Date and End Date, are displayed in the Entitlements tab.
2. From the Actions menu, select **Modify Grant Duration**. The Modify Grant Duration dialog box is displayed.
3. In the Justification box, enter a justification for modifying the start date, or end date, or both.
4. Enter values in any one or both of the following fields:
   - **Start Date:** The start date when the entitlement will be provisioned. This must be a future date. This field is not available for modification if the entitlement is already assigned.
   - **End Date:** The end date when the entitlement will be revoked.
5. Click **OK**.

   The Start Date and End Date fields in the Roles tab are updated with the values you specified immediately if no approver is assigned else if approver is assigned it is updated after the approval.

5.3 Managing Accounts

An account is granted to a user to give the user the ability to log in to Oracle Identity Manager and access its features. The Accounts tab in the My Access page allows you to manage the accounts assigned to you.

In the Accounts tab, you can perform the following:

> **Note:**
>
> It is recommended not to update a field that is marked as an entitlement field in the child table. To update a field marked as an entitlement, you will have to revoke and grant an entitlement.

- Requesting for Accounts
- Modifying Accounts
- Removing Accounts
- Disabling an Account

- Enabling an Account
- Resetting Password for an Account
- Modifying Account Grant Duration

5.3.1 Requesting for Accounts

When you submit your request for an account, it is submitted for approval. When the request is approved at all approval levels, the account is assigned to you.

To request for accounts:

1. In the My Access page, click the **Accounts** tab. A list of accounts assigned to you is displayed.
2. From the Actions menu, click **Request**. Alternatively, click **Request** on the toolbar. The Catalog page is displayed.
3. Select a catalog item that you want to request. You can also select multiple items in the list.
4. Click **Add to Cart** that is present against the catalog item or **Add Selected to Cart**.

   The selected items are added to the request cart.
5. Click **Checkout** or click **Next** and provide additional information, however this is not mandatory. Ensure to provide unique values for User Id and Password, else the request will fail.
6. Click **Submit**. The account will be assigned after the request is approved.

   For more information, see Requesting Access .

5.3.2 Modifying Accounts

When you submit your request for modifying an account that is assigned to you, it is submitted for approval. The account is updated after the request is approved.

To modify accounts assigned to you:

1. In the Accounts tab, select an account that you want to modify.
2. From the Actions menu, select **Modify**. The Catalog page is displayed.
3. Edit the attributes of the account. Provide the **Effective Date** for the modifications to be propagated to the account. If it is left blank the account will be modified when the account is approved.
4. Submit the request from the Catalog page. The account will be modified after the request is approved.

> **Note:**
>
> Changing the account password as part of the Modify operation in the Account form page will have no effect on the password. The account password can be changed using the Reset Password operation.
>
> As a workaround, you can hide the account password fields by customizing the UI.

5.3.3 Removing Accounts

When you submit your request for removing an account that is assigned to you, it is submitted for approval. The account is removed after the request is approved.

To remove accounts assigned to you:

1. In the Accounts tab, select the account that you want to remove.
2. From the Actions menu, select **Remove**. Alternatively, click **Remove** from the toolbar. The Catalog page is displayed.
3. Submit the request to remove accounts. The accounts will be removed after the request is approved. Removing an Account can not be done for a future date. To remove a account in future you need to set the end date field in Grant Duration to that date.

5.3.4 Disabling an Account

When you submit your request to disable an account that is assigned to you, it is submitted for approval. The account is disabled after the request is approved.

To disable an account:

1. In the Accounts tab, select an account that you want to disable.
2. From the Actions menu, select **Disable**. The Catalog Page is displayed.
3. Specify **Effective Date**. This is the date when the account will be disabled.
4. Submit the request to disable accounts. The accounts will be disabled after the request is approved.

5.3.5 Enabling an Account

When you submit your request to enable an account that was assigned to you but is in disable state, it is submitted for approval. The account is enabled after the request is approved.

To enable an account:

1. In the Accounts tab, select an account that you want to enable.
2. From the Actions menu, select **Enable**. The Catalog Page is displayed.

> **Note:**
>
> The Enable icon will be active only when a disabled account is selected.

3. Specify **Effective Date**. This is the date when the account will be enabled.
4. Submit the request to enable accounts. The accounts will be enabled after the request is approved.

5.3.6 Resetting Password for an Account

To reset password for an account assigned to you, use one of the following ways:

- Go to the Accounts tab of the My Access page. Then, select an account and click **Reset Password.**
- If you are an admin user, go to the Accounts tab of the Users page. Then, select an account and click **Reset Password.**

5.3.7 Modifying Account Grant Duration

When you submit your request for change of account grant duration, the Accounts tab are updated with the values you specified immediately if no approver is assigned else if approver is assigned it is updated after the approval.

To modify the grant duration of the account assigned to you or to be assigned to you:

1. In the Accounts tab of the My Access page, select an account for which you want to modify the grant duration.

   The grant duration fields, Start Date and End Date, are displayed in the Accounts tab.
2. From the Actions menu, select **Modify Grant Duration**. The Modify Grant Duration dialog box is displayed.
3. In the Justification box, enter a justification for modifying the start date, or end date, or both.
4. Enter values in any one or both of the following fields:
   - **Start Date:** The start date when the account will be provisioned. This must be a future date. This field is not available for modification if the account is already assigned.
   - **End Date:** The end date when the account will be revoked.
5. Click **OK**.

   The Start Date and End Date fields in the Roles tab are updated with the values you specified immediately if no approver is assigned else if approver is assigned it is updated after the approval.

5.4 Viewing Admin Roles

The Admin Roles tab of the My Access page displays the admin roles you have. Admin roles determine the operations you can perform in Oracle Identity Manager.

6
Requesting Access

Oracle Identity Manager supports requesting for entities such as roles, application instances, and entitlements. You can request for these entities by using the access catalog.
This section describes the following topics:

- Requesting New Access
- Viewing Hierarchical Attributes of Entitlements
- Adding and Removing Catalog Items to and from the Cart
- Adding and Removing Grant Duration
- Managing Request Profiles
- Tracking a Request
- Deleting a Request
- Withdrawing a Request
- Closing a Request
- Requesting Access With Policy Violations

6.1 Requesting New Access

Based on permissions, you can request access for self or for other users by using the access catalog.

This section describes how to request access by using the access catalog in the following sections:

- Requesting Access for Self
- Requesting Access for Other Users
- Requesting Access By Using a Request Profile
- Keyword Search in the Access Catalog
- Specifying Application Instances in Entitlements Search
- Refining Search Results

6.1.1 Requesting Access for Self

You can request access for self by using the access catalog.

To request access for self:

1. Login to Oracle Identity Self Service.
2. In the Self Service tab, click the **Request Access** box, and select **Request for Self**. The Add Access page of the Request Access wizard is displayed. The Add Access page

enables you to search and select the items you want to request for. This page consists of the following tabs:

- **Catalog:** This tab enables you to search and add access (entities) to the request cart, and then create the request for access.
- **Request Profiles:** This tab enables you to search and view request profiles, and add profiles to the cart. See Managing Request Profiles for information about request profiles.

3. Click the **Catalog** tab, if it is not already active.
4. Search for the entities that you want to request for self. To do so:
   a. Select any one of the following options:
      - **All:** To specify that all entities are being searched, such as roles, application instances, and entitlements.
      - **Application:** To specify that only application instances are being searched.
      - **Entitlement:** To specify that entitlements are being searched. While searching for entitlements, you can specify the associated application instances. When you select the **Entitlement** option, the Application list is displayed. For information about selecting one or more application instances, see Specifying Application Instances in Entitlements Search.
      - **Role:** To specify that only roles are being searched.
   b. In the Search field, enter a search keyword, and click **Search**.

      For information about search keywords that you can specify, see Keyword Search in the Access Catalog.

      The items that match the search criteria are listed. An icon is displayed with each catalog item that denotes whether the item is a role, application instance, or entitlement, as listed in Table 6-1.

Table 6-1 Icons Denoting Catalog Item Type

Icon	Item Type
	Role
	Application Instance
	Entitlement

5. You can refine the catalog items to list all items or any one of the application instance, entitlement, or role entities. See Refining Search Results for more information.
6. To view the details of the catalog item, click the information icon for the item. The Detailed Information page is displayed that shows the attributes for the item.

   For application instances and entitlements, you can edit the values of the attributes in the Detailed Information page. To do so, click the information icon for

the application instance or entitlement, modify the values of the attributes in the Detailed Information page, and click **Apply**.

For roles, the attributes displayed in the Detailed Information page are read-only and cannot be modified. These attributes can only be edited by the Catalog Administrator. If Catalog Administrator wants to update any catalog attribute for role, then it can be done only from the role details page.

After modifying or reviewing the attribute values, close the page.

7. To add a catalog item to the request cart, click **Add to Cart** for that item.

   To add multiple catalog items to the request cart, select multiple items by clicking the items while pressing the `Ctrl` key, and then click **Add Selected to Cart**.

   > **Note:**
   >
   > If you switch workspace, then cart items are lost. For example, after adding items to the cart, if you click the **Manage** tab and then come back to **Self Service** again, then the items added to the cart are lost.

   The items are added to the cart. Scroll to the top of the page. The number of items added to the cart is displayed with the cart icon.

   To remove the selected items from the cart, see Adding and Removing Catalog Items to and from the Cart.

   When requesting access, each item in the cart can have its own temporal grant dates. If you want specific dates set for the cart items, then the dates must be set manually for each cart item. If no dates are entered, then the start date will default to the current date and the end date will be left empty indicating an indefinite access. See Adding and Removing Grant Duration for information about grant duration.

   > **Tip:**
   >
   > To add items to the cart by using request profiles, click the **Request Profiles** tab. For information about request profiles and using request profiles to create a request, see Managing Request Profiles and Requesting Access By Using a Request Profile.

8. Click **Next**. The Checkout page is displayed.
9. In the Cart Details section, expand **Request Information**, if it is not already expanded.
10. In the Justification field, enter a justification for the request. This is for the approver to review the justification, and then approve or reject the request.
11. Expand **Cart Items**, if it is not already expanded. This section lists the catalog items that you selected and have been added to the request cart. For each item, one of the following icons represents the submission readiness of the item:

    - The icon denotes that the item is ready for submission.
    - The icon denotes that the item is not ready for submission.

You can click the information icon for each item to display the details of the item in a pop-up window.

12. (Optional) If you want to remove any item from the cart, then click the cross icon for that item.
13. Click an item to display the request details of the item in the Request Details section. This section consists of the following tabs:

    - **Grant Duration:** This tab is represented by the icon and is displayed for all types of entities.
    - **Details:** This tab is represented by the icon and is displayed only for application instances and entitlements that require additional data.

14. Click the Grant Duration icon. The Grant Duration section provides options that enable you to control the duration when the access will be provisioned. To specify grant duration:

    a. Select the **Grant will be effective immediately upon request completion** option if you want the role, account, or entitlement to be provisioned immediately on request approval. By default, this option is selected.

    b. If the **Grant will be effective immediately upon request completion** option is not selected, then specify date values for the following fields:

        - **Start Date:** The start date when the role, account, or entitlement will be provisioned.
        - **End Date:** The end date when the role, account, or entitlement will be revoked.

        For detailed information about grant duration, see Adding and Removing Grant Duration.

15. Click the Details icon. The form associated with the application instance or complex entitlement is displayed. You can modify the attributes in this form. These attributes are the form fields of the application instance or complex entitlement, and is propagated to the target account after the provision/modify operation is completed.

    The Details icon is displayed only when you select a cart item that is an application instance or a complex entitlement.

16. Click **Update**. The values you entered for the selected cart item are updated in the cart.
17. Click **Submit** to submit the request.

    If the Identity Audit feature is enabled, then based on the Identity Audit rules configured, the Cart Items sections can display a warning for policy violations. For information about the policy violations displayed in the Cart Items section and how to mitigate the same, see Requesting Access With Policy Violations.

6.1.2 Requesting Access for Other Users

Based on permissions, you can request access for other users.

To request access for others:

1. Log in to Oracle Identity Self Service.
2. In the **Self Service** tab, click the **Request Access** box, and then select **Request for Others**. The Select Users page of the Request Access for Others wizard is displayed.
3. Search for the users for which you want to request access. You can perform a basic search or an advanced search for users.
   - To perform a basic search for users:
     a. If Advanced search is active, then click **Basic**. Otherwise, proceed to step 2.
     b. From the Search list, select an attribute based on which you want to search the users.
     c. In the Search field, enter a keyword for your search.
     d. Click the Search icon. The users that match the search keyword are listed in the Users pane.
   - To perform an advanced search for users:
     a. Click **Advanced**. A number of attributes are displayed based on which you can search the users.
     b. For one or more attributes, select the search operator from the lists, such as Starts With, Ends With, Equals, Does Not Equal, Contains, and Does Not Contain. For any date field, the search operators are Equals, Before, After, On or before, On or after, Between.
     c. Specify values for one or more attributes. The search result will be displayed based on the values that you specify for these attributes.
     d. Optionally, you can add fields to your search criteria by clicking Add Fields and selecting fields from the list. A cross icon is displayed with the added fields. You can click the cross icon to remove the added field.
     e. Click **Search**. The users that match the search criteria are listed in the Users pane.

   > **Note:**
   >
   > If you switch from basic to advanced search and fill in search criteria and then switch back to basic search again, the basic search still has the criteria from the advanced search. It is now no longer a basic search. This issue is applicable to search screens for all entities that have basic and advanced search.

4. In the Users pane, you can view the details of each user by clicking the information icon for that user. The User Details dialog box displays the user attributes, and the roles, accounts, and entitlements assigned to the user. Click Close to close the User Details dialog box.
5. For each user that you want to select, click **Add User**. The user is added to the Selected Users pane.
6. Click **Next**. The Add Access page of the Request Access wizard is displayed.
7. Complete the steps in the wizard, as described in Requesting Access for Self.

6.1.3 Requesting Access By Using a Request Profile

You can request access by using a request profile.

To do so:

> **Note:**
>
> For information about request profiles, see Managing Request Profiles.

1. In the Request Access box of the Self Service tab, click the **Request Access** box, and select **Request for Self**. The Add Access page of the Request Access wizard is displayed.
2. Click the **Request Profiles** tab.
3. Click the request profile name that you want to use to create the request. The Cart Details page is displayed.
4. The Target Users section displays the usernames of beneficiaries for the request. You can click information icon against each user to view the details.
5. To add beneficiaries to the request:
   a. Click the Add icon. The Advanced Search for Target Users dialog box is displayed.
   b. Search and select one or more users that you want to add.
   c. Click **Add Selected** to add the selected users to the Selected Users list. Alternatively, click **Add All** to add all the users in the Selected Users list.
   d. Click **Add**. The selected users or beneficiaries are added to the Users section of the Request Cart Details page.

   You can also select a user that you want to remove from the list of beneficiaries, and click the Remove icon.
6. If required, in the Justification and Effective Date section, in the respective fields, specify a justification and effective date when the request will be active.
7. In the Cart Items section, select a cart item to display the details of the item.
8. After reviewing and modifying the details for each request in the cart, click **Submit**. If the **Submit** button is not active, then click **Ready to Submit** for each cart item with Not Ready to Submit status.

   The request is submitted for approval, and the Request Summary page is displayed with summary information, target user or beneficiary information, and request and approval details.

6.1.4 Keyword Search in the Access Catalog

Using keyword search in the access catalog, you can search on the basis of entity name, entity display name, or user-defined tags that administrator has provided for that catalog item. Here, entity refers to role, application instance, and entitlement.

Catalog keyword search has the following characteristics:

- Appending wildcard characters, such as asterisk (*) or percentage sign (%), is not required.
- Catalog keyword search does not support * or % sign as a prefix.
- Search is performed as if with the `Begins With` operator.

For example, if you are searching for a role with role name as `Act Admin` and display name as `Accounts Administration`, then you can specify the search keyword as `Act` or `Acco` or `Accounts` or `Admin` . Searching with `*unts` will not work.Any catalog UDF that is marked as searchable is displayed automatically on the catalog search form as an attribute, by using which you can search catalog items. See "Creating a Custom Attribute" in the *Administering Oracle Identity Governance* for information about marking a UDF as searchable.

6.1.5 Specifying Application Instances in Entitlements Search

When you search for entitlements in the access catalog, you can specify one or more associated application instances based on which you want to search the entitlements.

To do so:

1. Navigate to the Catalog tab in the Add Access page of the Request Access wizard, as described in Requesting New Access.
2. To specify an entity type to be searched, select the **Entitlement** option. The Application list is displayed.
3. Select an application instance based on which you want to search the entitlement. The number of selected application instance is shown in the **Selected Apps** link. This number of selected application instances is updated if you again select more application instances from the list.
4. (Optional) Instead of selecting the application instances one by one, you can search and select multiple application instances. To do so:
   a. From the Application list, select **Search and select multiple**. The Choose Applications dialog box is displayed.
   b. In the Search box, enter a keyword to search for the application instances you want to select.
   c. Click the search icon. The application instances that match the search keyword are displayed.
   d. Click **Select** for each application instance that you want to select.

      > **Note:**
      >
      > You can select a maximum of 20 application instances at a time.

   e. If you want to remove application instances from your selection, then click Deselect for each application instance that you want to remove.
   f. To select or deselect all application instances at a time, you can click the **Select All** and **Deselect All** buttons respectively.
   g. Click **OK**. The application instances are selected.

5. (Optional) To remove the selected application instances, click the **Selected Apps** link, and then click the cross icons adjacent to the application instances that you want to remove. To remove all selected application instances, click **Clear All**.

You can Continue with the search by specifying a search keyword, as described in Requesting New Access.

6.1.6 Refining Search Results

You can refine your search results to make it more precise.

After searching for catalog items, as described in Requesting New Access, you can refine your search results to make it more precise. To do so, in the Categories section of the Catalog tab, select one or more categories to display the catalog items of those categories. You can select or deselect the **Select All** checkbox to display or hide all items belonging to the categories.

Categories are a way of organizing entities in the access catalog. Each catalog item is associated with one and only one category. Default categories of a catalog item can be roles, entitlements, or application instances. You can also define new custom categories by changing or updating the category of a catalog item in its detailed information page. For example, you can refine your search result to display catalog items belonging to the entitlements category only by selecting **Entitlements** in the Categories section.

6.2 Viewing Hierarchical Attributes of Entitlements

If viewing additional attributes for entitlements is configured, then the request details screen displays the additional attributes.

See "Configuring Hierarchical Attributes of Entitlements" in the *Administering Oracle Identity Governance* for information about configuring the display of additional attributes for entitlements.

To view the additional attributes for entitlements:

1. In the Catalog page, search for the catalog items that you want to view. The catalog items that are entitlements are displayed with an arrow icon. These are the entitlements that have XML files associated with them, as described in "Configuring Hierarchical Attributes of Entitlements" in the *Administering Oracle Identity Governance*.

   The arrow icon is not displayed for some catalog items because these catalog items do not have XML files associated with them.

2. Click the arrow icon. The additional details with the additional information or the technical glossary is displayed in a new tab. In the additional details tab, the child of the top node is shown. To view the details of the node, click the row.

3. Click the row to view the details. If additional details are present for the child node, then it is displayed on the right side.

   Breadcrumb icons are displayed at the top of the additional details popup. The texts in the breadcrumbs are hyperlinks. You can click the hyperlinks to navigate between the nodes.

6.3 Adding and Removing Catalog Items to and from the Cart

A request cart, also known as a cart, contains a set of catalog items that the user selects from the request catalog. Users can add catalog items to the request cart to submit a request for entities such as roles, entitlements, and application instances. The request cart does not persist across user sessions.

To add catalog items to the cart:

1. Open the access catalog, and search for the catalog items that you want to add to the cart. See Requesting New Access for the procedure to search for catalog items.
2. If required, narrow down your search result by selecting or deselecting one or more categories in the Categories section. You can select or deselect the **Select All** checkbox to display or hide all the items belonging to the categories.
3. Click **Add to Cart** on the catalog item that you want to request.

   You can also select multiple items from the catalog by following the standard multi-selection process for your system, then click **Add Selected to Cart**.

   The number of items added to the cart is displayed with the Cart icon at the top of the page.
4. On the top of the page, click **Cart**. The Request Cart window is displayed with a list of all the items that are added to the cart.
5. For each item that you want to remove from the cart, click **Remove** for that item.

   To remove all items from the cart, click **Remove All**.
6. Click **Close**.

6.4 Adding and Removing Grant Duration

The access catalog provides the Start Date and End Date fields for specifying the grant duration of roles, accounts, and entitlements to self or other users.

This section describes the following operations related to grant duration:

- Specifying Grant Duration
- Modifying Grant Duration
- Revoking Access

6.4.1 Specifying Grant Duration

Specifying grant duration for role/account/entitlements enable you to control the duration when the access will be provisioned.

When you add access to users, the grant duration fields have the following functionality:

- If both grant duration fields, Start Date and End Date, are specified, then it means that role/account/entitlement will be provisioned on the specified start date only, and it will be revoked on the specified end date.
- If only Start Date is specified, then role/account/entitlement will be provisioned on the specified start date, and there is no end date applicable for the access.

- If only End Date is specified, then role/account/entitlement will be provisioned immediately, and role/account/entitlement will be revoked automatically on end date.
- If both the grant duration fields are not specified, then role/account/entitlement will be provisioned immediately, and role/account/entitlement to entity remains with the user indefinitely.
- If the operation requires approval, then role/account/entitlement will be provisioned only after approval is done and start date is reached (if specified).
- If the operation does not require approval, then role/account/entitlement will be provisioned only after start date is reached (if specified).
- If the grant date is set to a future date, then the access is displayed in the following manner:
  - For roles: The Assigned on date is not displayed if a future start date is set.
  - For entitlements: The access is displayed with the `Future Grant` status in the user's entitlements tab.
  - For accounts: The account will be in disabled state until the start date is reached.

For information about specifying grant duration, see steps 13 and 14 of Requesting Access for Self for information about specifying grant duration when requesting roles/accounts/entitlements for self. The same steps apply for specifying grant duration while requesting access for other users.

6.4.2 Modifying Grant Duration

Start date can be modified only when roles/accounts/entitlements have not yet been provisioned. End date can be modified at any time.

Grant duration can be modified from the following sections in Identity Self Service:

- The My Access page: For information about modifying the grant duration fields from the My Access page, see Modifying Role Grant Duration, Modifying Entitlement Grant Duration, and Modifying Account Grant Duration.
- The User Details page: For information about modifying the grant duration fields from the User Details page, see Modifying Role Grant Duration, Modifying Entitlement Grant Duration, and Modifying Account Grant Duration.
- The Pending Approvals page: During the approval process of a request, the approver can modify the start and end dates. For details, see Modifying Grant Duration.

6.4.3 Revoking Access

Revoking access to an existing role/account/entitlement can be done immediately or in the future.

To revoke access immediately, select the role/account/entitlement from the corresponding table, and click **Remove**.

To revoke access on a future date, select the role/account/entitlement, from the Action menu, select **Modify Grant Duration**. In the Modify Grant Duration popup, set the End Date field to the date when the access should be revoked.

6.5 Managing Request Profiles

Request profiles are request carts that are saved for future reuse by the users. You can create a request profile, modify request profile and delete request profiles.

This section discusses the following topics:

- About Request Profile
- Creating a Request Profile
- Modifying a Request Profile
- Deleting a Request Profile

> **Note:**
>
> Creating, modifying, or deleting a request profile can be performed only by catalog administrators or system administrators.

6.5.1 About Request Profile

When you select catalog items for requesting, the items are added to a request cart. The request cart is similar to the shopping cart in web sites that sell products to customers. You can view the selected items in the cart, or edit the request cart to add or remove items.

Request profiles are request carts that are saved for future reuse by the users. The request cart is saved by the catalog administrator or system administrator so that the user can use it to request for entities without searching through thousands of catalog items.

6.5.2 Creating a Request Profile

You can create a request profile after adding catalog items to the cart.

To create a request profile:

1. Login to Oracle Identity Self Service.
2. Click the **Self Service** tab if it is not already active.
3. Click the **Request Access** box, and select **Request for Self**.
4. Select one or more catalog items, and click **Add to Cart**. The catalog items are added to the request cart.
5. Click **Next**. The Checkout page is displayed with the cart details. The selected catalog items are displayed in the Cart Items section.
6. Click the down arrow beside **Save As**, and then select **Profile**. The Save As Profile dialog box is displayed with a list of the items in the cart.
7. In the Profile Name field, enter a name for the request profile. This is a mandatory field.
8. In the Description field, enter a description of the request profile.
9. Click **Save**. The request profile is created.

> **Note:**
>
> If you create a request profile with cart items that have additional information and save the request profile, then the additional information is not saved.

6.5.3 Modifying a Request Profile

You can modify an existing request profile to update the cart items.

To modify a request profile:

1. Open the access catalog, and go to the Add Access page.
2. Click the **Request Profiles** tab.
3. Locate the request profile that you want to modify, and click **Add to Cart**. Click **Next** to move to the Checkout page.
4. Click **Save As Profile**. The Save as Profile dialog box is displayed.
5. In the Save Profile Name field, enter the name for the request profile that is being modified. If you enter a new name, then a new request profile is created. If you enter the name of an existing request profile, then that request profile is updated with the latest changes.
6. In the Description field, enter a description of the request profile.
7. Click **Save**. Depending on whether you have entered the name of an existing request profile or new name, the request profile is created or updated, respectively.

> **Note:**
>
> Values that you add or specify for Start Date, End Date, or Effective Date are not saved in a request profile.

6.5.4 Deleting a Request Profile

Delete the request profiles that are not required or are not in use.

To delete a request profile:

1. Open the Add Access page of the access catalog.
2. In the Request Profiles section of the Catalog page, click the cross icon in the row corresponding to the request profile.
3. In the Confirmation dialog box that is displayed, click **Yes.**

   The request profile is deleted.

6.6 Tracking a Request

You can search for requests that you want to track, view the details of the request. If you are the requester, then you can modify, submit, or delete the draft request.

This section describes how to search and track requests:

- Searching Track Request
- Tracking a Draft Request

6.6.1 Searching Track Request

Use the Track Requests page to perform simple and advanced search for requests.

To track a request:

1. In Identity Self Service, click the **Self Service** tab if it is not already active.
2. Click the icon in the **Track Requests** box. The Track Requests page is displayed.
3. Search for the requests you want to track. You can perform basic and advanced search for requests.

   To perform basic search for requests:

   a. From the Search list, select an attribute name based on which you want to specify the search parameter.

   b. In the Search box, enter a value for the selected attribute.

   c. Click the Search icon.

   To perform an advanced search for requests:

   a. Click **Advanced**.

   b. Select any one of the following:

      - **All:** On selecting this option, the search is performed with the AND condition. This means that the search operation returns requests that match all the search criteria that is specified.
      - **Any:** On selecting this option, the search is performed with the OR condition. This means that the search operation returns requests that match the search criterion that is specified.

   c. In the searchable request attribute fields, such as Request ID, specify a value. You can include wildcard characters (*) in the attribute value.

      For some attributes, select the attribute value from the lookup or drop down. For example, to search all requests with the `Request Awaiting Approval` status, from the Status list, select the **Equals** search operator, and then select **Request Awaiting Approval** from the adjacent list.

   d. For each attribute value that you specify, select a search operator from the list. For example, the following search operators are available for Request ID:

      - Starts with
      - Ends with
      - Equals

- Does not equal
- Contains
- Does not contain

For other fields, for example Status, Request Type, Beneficiary, and Requester, only Equals and Does not equal operators are available.

For fields of date type, the search operators are:

- Equals
- Does not equal
- Before
- After
- On or before
- On or after

e. To add a searchable request attribute to the Track Requests page, click **Add Fields**, and select the attribute from the list of attributes.

For example, if you want to track all requests by a requester, then you can add the Requester attribute as a searchable field and specify a search condition.

f. Optionally, click **Reset** to reset the search conditions that you specified. Typically, you perform this step to remove the specified search conditions and specify a new search condition.

g. Click **Search**. The search results is displayed in a tabular format.

4. If the request search you performed displays a large number of records, then you can filter the request search result. To do so:

a. From the Show list, select any of the following:

- **Requests Raised By Me:** This is selected by default. Returns requests created by logged-in user.
- **Requests Raised For Me:** Returns requests where login user exists as beneficiary or target user.
- **For Reportee:** This option is available if the logged-in user is a manager of a user.
- **For User:** This option is available if the logged-in user has been granted the User Administrator or the HelpDesk admin role.
- **All:** Returns all requests in the search result. This option is available if the logged-in user has been granted the System Administrator role.

b. To sort the requests in the search result by any of the columns such as Request ID or Status, click the **Sort Ascending** or **Sort Descending** arrows in the column. The requests in the search result are sorted by the selected column.

5. In the request search result, click a request to view the details of the request. The details of the request is shown in a page with the following information:

- Summary information: This section shows general request details, such as request ID, request status, and effective date.
- Target Users: This section lists the beneficiaries or target users for the request.

- Related Requests: This section lists requests that are related to the open request, if any.
- Request Details: This tab lists the requested catalog items. You can select an item to display a summary information of the item.
- Approval Details: This tab displays the status of request approval by each approver to whom the request has been assigned.

> **Note:**
>
> HelpDesk users and beneficiaries can view request approval details. However, they cannot add comments or attachments on the request summary page.

6.6.2 Tracking a Draft Request

A requester can save a request for modifying, submitting, or deleting it later. This is useful if the requester is awaiting additional information before submitting the request.

Only the requester can modify, submit, or delete the draft request. Users such as system administrators and beneficiaries cannot view draft requests saved by others.

To track a draft request:

1. In the **Self Service** tab, click the icon in the **Track Requests** box. The Track Requests page is displayed.
2. From the Status list, select the **Equals** search operator, and then select **Request Draft Created** from the adjacent list.
3. In the Search Results region, from the Show list, select the **Requests Raised by Me** filter.
4. (Optional) Use any other search criteria as described in Tracking a Request.
5. Click **Search**. The search results is displayed in a tabular format.

   The draft request cannot be withdrawn or closed. To delete a draft request, select a request and click **Delete Request.**

   To open a draft request to modify or submit it, click the link in the Request ID column. In the Edit Draft Request page, you can click **Submit** to submit the draft request. If the **Submit** button is not active, select and edit each cart item in the Cart Items region, and then click **Ready to Submit.** To modify and save the request data, click **Update Draft Request**.

> **Note:**
>
> The request data saved in draft mode does not include sensitive information such as passwords, even if they were entered before saving the request as draft.

6.7 Deleting a Request

Delete the requests that are not required.

To delete a request:

1. In the **Self Service** tab, click the icon in the **Track Requests** box. The Track Requests page is displayed.
2. Search and select the request that you want to delete.
3. From the Actions menu, select **Delete Request**. Alternatively, you can click **Close Request** on the toolbar.
4. Click **Yes** in the confirmation message box. The request is deleted and a notification is sent to the beneficiary and requester of the request.

> **Note:**
>
> - Configuration of notification can be done in the human task of a SOA composite.
> - For more information about request-related tasks, such as approving a request, reassigning a task, and rejecting a task, see Using the Unified Inbox.

6.8 Withdrawing a Request

A request can be withdrawn by the requester, and only the requests that have not started the execution phase can be withdrawn. Also, beneficiaries cannot withdraw requests.

Requests having the following stages can be withdrawn:

- Obtaining Approval
- Approved

> **Note:**
>
> – Approved requests cannot be closed unless the request has the Request Awaiting Completion status.
> – Draft requests, which are in Request Draft Created status, cannot be withdrawn.
> – If a request is closed while the request is in the Obtaining Approval stage, then all the approvals that are still pending in the approver task list are removed.

To withdraw a request:

1. In the Self Service tab, click the icon in the **Track Requests** box. The Track Requests page is displayed.
2. Search for the requests that you want to withdraw. The search results display a list of requests that match your search criteria with a Withdraw Request button for each request.
3. For a request that you want to withdraw, click **Withdraw Request**. Alternatively, you can open the details of a request by clicking the request ID, and subsequently clicking **Withdraw Request** on the request details page.
4. Click **Yes** in the confirmation message box. The request is withdrawn and a notification is sent to the beneficiary and requester of the request. If the withdrawal is successful, then request moves to the Request Withdrawn stage. Any pending approval tasks associated with the request are canceled.

6.9 Closing a Request

Administrators can prematurely close any request that has not started the execution phase. This includes all requests waiting for approvals or has completed approvals but no operation has been started.

Requests with the following state can be closed:

- Obtaining Approval
- Approved

> **Note:**
>
> - Approved requests cannot be closed unless the request has the Request Awaiting Completion status.
> - Draft requests, which are in Request Draft Created status, cannot be closed.
> - If a request is closed while the request is in the Obtaining Approval stage, then all the approvals that are still pending in the approver task list are removed.

To close a request:

1. In the **Self Service** tab, click the icon in the **Track Requests** box. The Track Request page is displayed.
2. Search for the requests that you want to close. The requests that match the search condition are displayed in a tabular format.
3. Select the request that you want to close.
4. From the Actions menu, select **Close Request.** Alternatively, you can click the **Close Request** icon on the toolbar.
5. Click **Yes** in the confirmation message box. The request is closed and a notification is sent to the requester and target user of this request. When a request is closed successfully, the request moves to the Request Closed stage.

Note:

- Configuration of notification can be done in the human task of a SOA composite.
- For more information about request-related tasks, such as approving a request, reassigning a task, and rejecting a task, see Managing Pending Approvals .

6.10 Requesting Access With Policy Violations

You can submit request with known access violations.

The following sections describe requesting access with policy violations:

- About Requesting Access With Policy Violations
- Migrating the Policy Violations and Submitting the Requesting
- Predictive Policy Validation for In-Flight Requests

6.10.1 About Requesting Access With Policy Violations

When a request for access is submitted and the Identity Audit feature is enabled, the information in the request data is scanned to detect any possible access violations.

A violation occurs if the combination of the access currently assigned to a user along with the access being requested, matches an audit policy.

For example, consider an Identity Audit policy consisting of the following rule:

```
role[*].Role Name EQUAL AP Expense Approver
AND
role[*].Role Name EQUAL AP Merchandise Vendor Approver
```

The rule specifies that a user cannot have both the AP Expense Approver and the AP Merchandise Approver roles at the same time. If this situation occurs, then it is a policy violation.

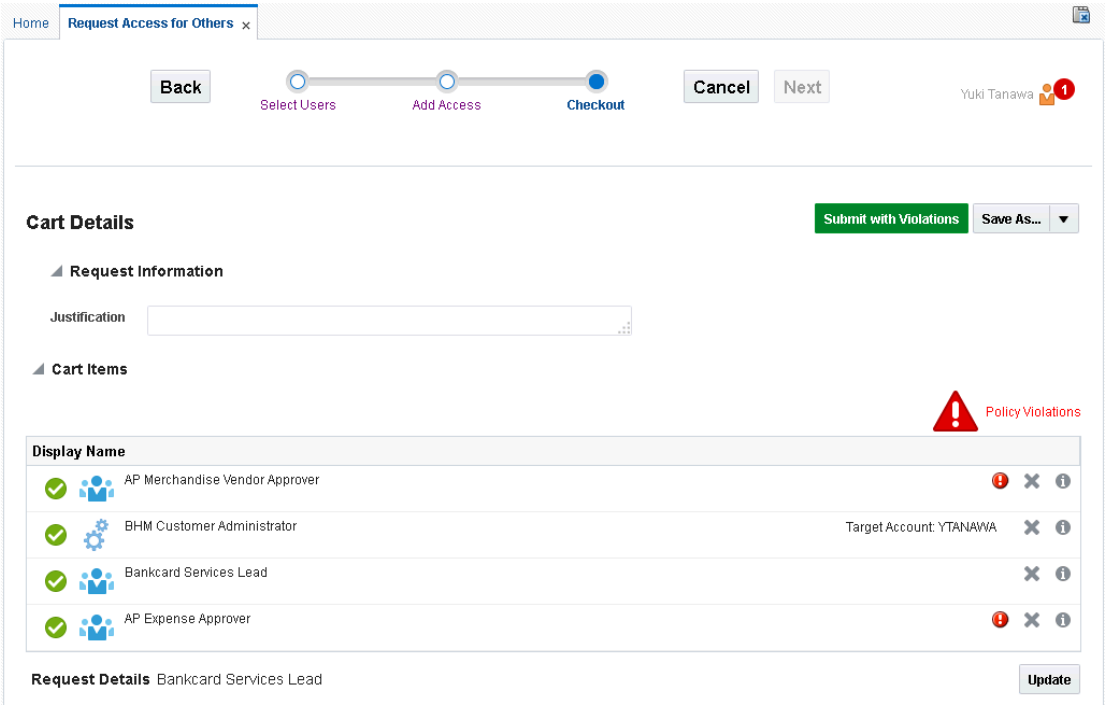
If a violation is detected, the initial request is returned to the requestor, and the page is refreshed to indicate the violations.

Each cart item that is causing the violation is indicated with the icon, and an overall warning message is displayed. Clicking the message displays an overall view of all the violations detected.

It is still possible to submit the request with the known violations by clicking the **Submit with Violations** button.

Figure 6-1 shows the Checkout page that is indicating policy violations.

Figure 6-1 Policy Violation



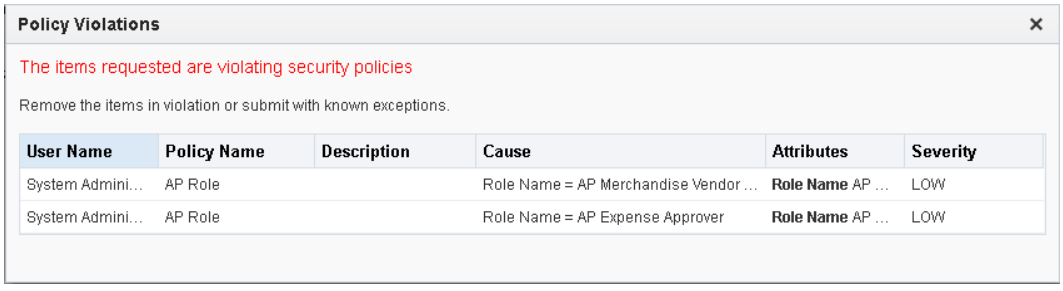
6.10.2 Migrating the Policy Violations and Submitting the Requesting

You can take corrective steps to mitigate the requests with policy violations and submit the request.

Perform the following steps to mitigate the policy violations and submit the request:

1. In the Checkout page of the access catalog, click **Policy Violations**. The Policy Violations dialog box is displayed with the cart items that are causing the policy violation. It displays the policy name that is violated, the cause of the violation, the attributes that cause the violation, and the severity of the violation, as shown in Figure 6-2.

Figure 6-2 The Policy Violations Dialog Box



2. Close the Policy Violations dialog box.
3. Click the cross icon with the cart items to remove the items causing the policy violation. In the example in this section, removing any one of the AP Expense Approver or AP Merchandise Vendor Approver roles will remove the policy violation.

The policy violation icons and the policy violation warning are no longer displayed, and the **Submit with Violations** button changes to **Submit**.

4. Click **Submit** to submit the request.

   Alternatively, to submit the request with policy violations, click **Submit with Violations**.

6.10.3 Predictive Policy Validation for In-Flight Requests

Identity audit policy validation takes place for in-flight requests.

By default, identity audit policies validate entitlements that are being requested for the accounts in provisioned, enabled, or disabled states. This validation does not apply when the requests for applications and entitlements are pending for approval. For example, the target user already has associated application instance and some or no entitlements on the account, and identity audit policy rule states that Entitlement A and Entitlement B cannot be provisioned together. When the request for Entitlement A is submitted, the request is pending for approval. At the same time, Oracle Identity Governance allows to submit another request for Entitlement B.

After you apply Oracle Identity Governance Bundle Patch 12.2.1.4.210428, the identity audit policy validation takes place for in-flight requests, in other words, for application and entitlement requests that are pending for approval. Therefore, for the above example, submitting the request for Entitlement B results in policy violation.

7

Using the Unified Inbox

In Oracle Identity Self Service, Unified Inbox allows you to view approval, provisioning, certification tasks, and audit violation tasks.
This chapter describes the unified inbox and some common tasks that you perform in the following sections:

- Understanding the Task Types in Oracle Identity Governance
- About the Unified Inbox
- Creating a View Definition
- Editing the Task Chart
- Editing Inbox Settings

7.1 Understanding the Task Types in Oracle Identity Governance

In Oracle Identity Self Service, you can view task instances of specific types. These types are associated with specific Oracle Identity Governance components.

The task types are approval, provisioning, certification tasks, and audit violation tasks.

- About Pending Approval Tasks
- About Provisioning Tasks (or Manual Provisioning)
- About Certification Tasks (or Pending Certifications)
- About Audit Violation Tasks (or Pending Violations)

7.1.1 About Pending Approval Tasks

The approval tasks can be viewed and managed from the Inbox as well as from the Pending Approvals page of Identity Self Service. These tasks are instantiated by request service and correspond to associated requests that are in the user or administrator's queue to be approved. For more information, see "Managing Pending Approvals ".

7.1.2 About Provisioning Tasks (or Manual Provisioning)

Provisioning Tasks are not displayed in the Inbox. The provisioning tasks can be viewed and managed from the Provisioning Tasks section of Identity Self Service. These tasks correspond to tasks instantiated by requests, or pending manual provisioning tasks, or failed automatic provisioning tasks in the user or administrator's queue. For more information, see Managing Pending Provisioning Tasks.

Pending manual provisioning tasks can be viewed from the Manual Fulfillment section of Identity Self Service. These tasks are related to provisioning of disconnected application instances. For more information, see Managing Manual Fulfillment Tasks.

The approval and provisioning tasks can be used by both administrators and end-users. For example, an IT department personnel responsible for delivering a laptop to an employee may not be an Oracle Identity Manager administrator, but needs to view and change provisioning tasks.

7.1.3 About Certification Tasks (or Pending Certifications)

The certification review tasks can be viewed and managed from the Inbox as well as from the Pending Certifications page of Identity Self Service. These tasks correspond to the certification process in the reviewer's queue. For more information, see Managing Certification Review Tasks .

7.1.4 About Audit Violation Tasks (or Pending Violations)

The audit violation tasks can be viewed and managed from the Inbox as well as from the Pending Violations page of Identity Self Service. As a remediator of policy violations that are assigned to you, you can access the pending violations and take action on them. For more information, see Managing Pending Violations .

> **Note:**
>
> Certification and audit violation tasks are displayed only when the Identity Audit feature is enabled. See Enabling Identity Audit for information about enabling the Identity Audit feature.

7.2 About the Unified Inbox

The Inbox lists all the approval and certification-review tasks assigned to the logged-in user in a single screen.

It enables the logged-in user to filter task views into user preferences, such as assigned tasks, completed tasks, and tasks for which information has been requested. The user can select a task to open it in a new tab and then perform necessary actions on the task. This allows you to work on multiple tasks at a time by opening them in different tabs.

To access the Inbox, login to Oracle Identity Self Service, click the down arrow displayed with the logged-in user name, and click **Inbox**.

The Inbox also allows the user to search tasks, organize them in views, and create shared views. The Views pane of the Inbox lists the available views. You can click a view to display its contents, which are filtered representations of tasks that match the view definition.

7.3 Creating a View Definition

The Inbox page allows you to search tasks, organize them in views, and create shared views or view definitions.

To create a view definition in the Inbox:

1. On the toolbar in the Inbox, enter a search criteria in the Search field. You can click the search icon adjacent to the Search field to display the search results. You can also choose to perform an advanced search. To do so, click the down arrow adjacent to the search icon, and click **Advanced**. The Advanced Search dialog box is displayed.
2. In the Definition tab, select the **Save Search as View** option. Selecting this option saves the search conditions as a view definition.
3. In the Name box, enter a name for the view. Alternatively, to create a copy of a publicly shared view, click the lookup icon to open the Select Public View dialog box, select a public view name, and click **OK**.

> **Note:**
>
> If you log in as a domain admin user, then you can create the view as public so that all users can see the view. When you create a public view, it is displayed under the Standard Views section. For more information, refer to SOA documentation.

4. From the Assignee list, select the assignee for the tasks that are to be listed in the view. You can filter the options by selecting the options, such as Me, Admin, and Creator.
5. In the Assignee, Task Type, and Add Condition fields, specify a search condition based on which certifications will be displayed in the view. For more information, see Searching Certifications in the Pending Certifications Page.
6. In the Share View section, select any one of the following:
   - **Definition only:** Select this option to share the view definition with other users and groups.
   - **Data:** Select this option to share the data or search result in your view.
7. Click the lookup icon adjacent to the Users and Groups fields to select users and groups respectively with whom you want to share the view.
8. Click **Save as View**. The view is added in the Views pane of the Inbox under My Views.

7.4 Editing the Task Chart

You can use the Inbox page to show or hide the task status information and to update the task status.

To do so:

1. On the toolbar on top of the Inbox, click the **Task Status** icon adjacent to the Status list.

> **Tip:**
>
> If the Task Status section is not displayed by default, then click the arrow next to Task Status to expand the Task Status. To collapse the Task Status, you can click the arrow again.

2. Click the **Edit Task Chart** icon. The Chart Display States dialog box is displayed.

3. Select the task status options that you want to display in the Task Status section of the Inbox. To hide the task status, deselect the task status options.
4. Click **OK**.

7.5 Editing Inbox Settings

You can modify the way data is displayed in the Inbox by changing the Inbox Settings.

To update Inbox settings:

1. Click the Edit Inbox Settings icon on the toolbar of the Inbox. The Edit Inbox Settings dialog box is displayed.
2. In the Show Columns section, move the column names to and from the Selected Columns list by using the right and left arrows. Only the columns in the Selected Columns list is displayed in the Inbox.

   You can also change the order in which the columns are displayed in the Inbox by using the up and down arrows. However, the Title column is always displayed as the first column irrespective of its position.
3. Specify the order in which tasks will be displayed in the Inbox by selecting the column names in the Sort by and Then by lists. Also specify the ascending or descending sort order in the Sort Order list.
4. From the Number of tasks per fetch list, select the number of tasks that will be displayed at a time in the Inbox.
5. Select Hide Task Details Panel if you do not want to display the task details page.
6. From the Default View list, select the default view that will be selected when you navigate to the Inbox.
7. Click **OK**.

8
Managing Pending Approvals

The Oracle Identity Manager allows you to view and update the tasks waiting for your approval. You can do this from the Inbox or the Pending Approvals page of Oracle Identity Self Service.
This chapter describes some of the task actions in the following sections:

> **Note:**
>
> The features related to performing task actions in the Inbox section are provided by Oracle SOA. Refer to SOA documentation for detailed information about the task actions.

- About Pending Approvals
- Viewing Pending Approval Tasks
- Adding Comments and Attachments
- Approving a Task
- Rejecting a Task
- Reassigning a Task
- Suspending a Task
- Withdrawing a Task
- Skipping Current Assignment
- Claiming a Task
- Modifying Grant Duration

8.1 About Pending Approvals

When a request is submitted, the request service initiates the approval as a task in Oracle SOA Server. This task is assigned to the approver.

Oracle Identity Manager request service interacts with SOA Server to handle various aspects of human interaction in Oracle Identity Manager workflows. This request service is used to assign tasks to roles and users. You can perform various operations upon tasks assigned to you. For example, you can approve, reject, or claim a task, or request for more information. The process flow in corresponding Oracle Identity Manager workflow is dependent on the outcome of given tasks.

> **See Also:**
>
> Developing Workflows in the *Developing and Customizing Applications for Oracle Identity Governance* for information about approval workflows

Further processing of the request by request service remains pending, which is subject to the outcome of the corresponding task. The approver can access either the Inbox section or the Pending Approvals page of the Identity Self Service that lists all the tasks assigned to the approver. The approver can now act upon this task and set its outcome, for example, approve or reject. After the task outcome has been set, the request service resumes the processing of the request that is based on the task outcome.

On successful submission of requests, the request service creates Human Tasks in SOA and assigns them to users or roles in Oracle Identity Manager. Authenticated users can view the tasks waiting for action in the Inbox or in the Pending Approvals page.

8.2 Viewing Pending Approval Tasks

You can view the pending approval tasks from the Inbox or the Pending Approvals.

To view for approval details:

1. Log in to Identity Self Service.
2. Click **Self Service**. Self service Home page is displayed.
3. Click the **Pending Approval**s box. The Pending Approvals page is displayed.

   The Pending Approvals page displays the details of your tasks in columns described in Table 8-1:

Table 8-1 Columns in the My Tasks Page

Column	Description
Title	The title of the task.
Assignees	The assignee of the task.
State	The current state of the task.
Created	The date and time on which the task is created.
Expires	The expire date of the task.

4. Click the task you would like to view details for.

   The task details page displays a detailed view of the request in the Details section, Summary Information section, the Request Details tab, the Approvals tab, and the Cart Items section. It allows complete management of the listed task.

   In the Cart Items section, the approver can provide data, without which (if the field is marked as mandatory) the approver will not be allowed to approve a request. For example, when an approver opens a task related to self-registration request, the organization field is marked as mandatory, but no value is specified for this

field by the requester. Therefore, the approver must specify a value for this mandatory field.

In addition, the following tabs display details associated to the request:

- **Request Details:** This tab displays the target users or beneficiary information, and related requests, if any.
- **Approvals:** This tab displays the complete approval flow with all approvers. You can select the **Future participants** option to display the next level approvers. You can select the **Full task actions** option to display all the approvals for the task.

8.3 Adding Comments and Attachments

You can add comments and attachments prior to performing any operation on the task such as approving, rejecting, or reassigning the request.

An attachment can either be a hyperlink or an actual file. It is recommended that the size of the file attachment that you upload be less than 2 MB. If you want to upload file attachments of size greater than 2 MB, then you must change the ADF configuration and increase the size limit.

To add comments and attachments:

1. Log in to Identity Self Service.
2. Click **Self Service**. Self service Home page is displayed.
3. Click **Pending Approval**s box. The Pending Approvals page is displayed.

   Click the task for which you want to add comments or attachments. The details of the task are displayed in a new tab.
4. To add a comment:
   a. Click the **Approvals** tab.
   b. In the Comments section, click the Create icon. The Create Comment dialog box is displayed.
   c. In the Comment field, enter the comments related to the task, and then click **OK.**
   d. Select **Task Actions**, **Save** to save the comment.
5. To add an attachment:
   a. Expand the Attachments section if it not already expanded.
   b. In the Attachments section, click the Add icon. The Add Attachment dialog box is displayed.
   c. Select one of the following options as the attachment type:
      - **URL:** Specify the URL to an attachment.
      - **Desktop File:** Allows you to select and upload a file from the desktop.

> **Note:**
>
> By default, uploading of all file types are supported. However, the file types that will be allowed for upload can be configured, as follows:
>
> i. Login to Oracle BPM Worklist by navigating to the following URL and providing the WebLogic admin credentials:
>
> `http://SOA_HOST:SOA_PORT/integration/worklistapp/faces/login.jspx`
>
> See Using Oracle BPM Worklist for information about Oracle BPM Worklist and the configurations you can do by using it.
>
> ii. Click **WebLogic User** at the top-right corner of the screen, and select **Administration**. The Application References page is displayed.
>
> iii. Click the **Administration** tab if it is not active.
>
> iv. In the File Types Allowed for Upload field, specify the comma-separated list of file type extensions that you want to allow for uploading, for example, `txt,png,pdf`.
>
> v. Click **Save**.
>
> vi. Restart Oracle Identity Manager server and SOA server.

d. Click **OK.**

6. Select **Task Actions**, **Save** to save the attachment.

8.4 Approving a Task

You can check details of the task, provide comments if required and approve the task from the Pending Approvals page.

To approve a task that is assigned to you:

1. Log in to Identity Self Service.
2. Click **Self Service**. Self service Home page is displayed.
3. Click **Pending Approval**s box. The Pending Approvals page is displayed.
4. Select the task that you want to approve.
5. Click the task to view its details in a new tab, and then click **Approve.**

> **Note:**
>
> If the request is to modify a parent or child form, then a bubble icon is displayed adjacent to the modified fields in the approval form. This bubble icon indicates that the particular field value has been modified to a newer value.

The task is approved and is no longer displayed in the tasks table.

> **Note:**
>
> A self-registration request is assigned to the System Administrator role by default. Before you can approve a self-registration request, as a member of the System Administrator role, you must claim a self-registration task and update the request if required and then approve it.

8.5 Rejecting a Task

You can check details of the task, provide comments if required and reject the task from the Pending Approvals page.

To reject a request that is assigned to you:

1. Log in to Identity Self Service.
2. Click **Self Service**. Self service Home page is displayed.
3. Click **Pending Approval**s box. The Pending Approvals page is displayed.
4. Select the task that you want to reject.
5. Click the task to view its details in a new tab and provide any comments. Then, click **Reject.** The task is rejected and is no longer displayed in the tasks table of the Approval Details page.

8.6 Reassigning a Task

You can check details of the task, and reassign or delegate the task to another user from the Pending Approvals page.

To reassign a request that is assigned to you:

1. Log in to Identity Self Service.
2. Click **Self Service**. Self service Home page is displayed.
3. Click **Pending Approval**s box. The Pending Approvals page is displayed.
4. Select the task that you want to reassign.
5. Click the task to view its details in a new tab. Then, from the Task Actions menu, select **Reassign**.

   The Reassign Task dialog box is displayed.
6. Select any one of the following options:
   - **Reassign (transfer task to another user or group):** To reassign the task to another user, group, or application role. On selecting this option, you can search and select users, groups, or application roles for reassigning.
   - **Delegate (allow specified user to act on my behalf):** To delegate the task to a user that you can search and select. The delegated user will take actions on the task on your behalf. The privileges of the delegatee are based on the delegator's privileges.
7. Search for user or groups to which you want to reassign the task, and select the users or group. Otherwise, click **Select All** to select all searched users or groups.

8. Click **OK**. The task is assigned.

8.7 Suspending a Task

You can suspend a task from the Pending Approvals page.

To suspend a task:

1. In the Approval Details page, search and select the request that you want to suspend.
2. Click the task to view its details in a new tab. Then, from the Task Actions menu, select **Suspend**.

   A message is displayed stating that your request has been processed successfully.

8.8 Withdrawing a Task

You can withdraw a task from the Pending Approvals page.

To withdraw a task:

1. In the Approval Details page, search for the request that you want to withdraw.
2. Click the task to view its details in a new tab. Then, from the Task Actions menu, select **Withdraw**.

   A message is displayed stating that your request has been processed successfully.

8.9 Skipping Current Assignment

In the Pending Approvals page, the Skip Current Assignment option in the Actions menu or Task Actions menu is displayed only to users with the System Administrators role. This option is not displayed for end users.

Skipping the current assignment is not a valid action for an approver. If an approver chooses this action, then the corresponding request fails. Therefore, this option can be hidden for system administrators also. See Hiding the Skip Current Assignment Option in the *Developing and Customizing Applications for Oracle Identity Governance* for information about hiding the Skip Current Assignment option.

8.10 Claiming a Task

You can claim a task that is not assigned to you from the Pending Approvals page.

To claim a task that is not assigned to you:

1. In the Approval Details page, search and select the request that you want to claim.
2. From the Actions menu, select **claim**.

   A message is displayed stating that the request has been assigned to you.

8.11 Modifying Grant Duration

You can modify the grant duration of the role, account, or entitlement which are pending for approval from the Pending Approvals page.

To modify the grant duration of the role, account, or entitlement to the user:

1. In the Approval Details page, search and select the request for which you want to modify the grant duration.
2. Open the request details.
3. Click **Claim** in the request details page.
4. In the Request Details tab, click the Grant Duration icon.
5. Modify the values in the following fields:
   - **Start Date:** The start date when the role, account, or entitlement will be provisioned. This must be a future date. This field is not available for modification if the role, account, or entitlement is already assigned to the user.
   - **End Date:** The end date when the role, account, or entitlement will be revoked.

   For detailed information about grant duration, see Adding and Removing Grant Duration.
6. Click **Update** in the Request Details tab.

9 Managing Provisioning Tasks

The Oracle Identity Manager allows you to view and manage the provisioning tasks assigned to you. The provisioning tasks feature is used by administrators as well as users.
This chapter describes working with provisioning tasks in the following sections:

- About Provisioning Tasks
- Managing Pending Provisioning Tasks
- Managing Manual Fulfillment Tasks

9.1 About Provisioning Tasks

The provisioning tasks feature is used by administrators as well as users. For example, the person in IT administration who is responsible for delivering a laptop computer to an employee may not be an administrator in Oracle Identity Manager, but must view and change provisioning tasks.

The Provisioning Tasks page of the Identity Self Service displays the provisioning tasks assigned to you. In addition, failed automatic provisioning tasks that you must review to take corrective action are displayed, and you must take corrective action on those tasks, such as retry and manually complete.

A provisioning operation such as creating or updating an account, or granting or revoking an entitlement can fail due to one of the following reasons:

- Mandatory information in the process form associated with the provisioning task is missing.
- Password specified for the account does not comply with the password policies configured on the target application.
- Target system is unavailable.
- Connectivity information specified in the ITResource parameter are incorrect, or password is no longer valid.

When a provisioning operation fails, you can configure the provisioning workflow to assign the failed task to an administrator or resource owner for taking an action. These tasks are visible in the Provisioning Tasks page. In this page, all tasks assigned to you for remediation are displayed, and you can perform actions, such as viewing the details of a rejected task and retrying it. If the task is no longer valid, then you can manually complete it. For more information, see Managing Pending Provisioning Tasks.

> **Note:**
>
> A user with System Administrator admin role can retry provisioning task.

The manual provisioning tasks for disconnected application instances are displayed in the Manual Fulfillment page of the Identity Self Service, where you can take actions on the tasks. For more information, see Managing Manual Fulfillment Tasks.

9.2 Managing Pending Provisioning Tasks

The Provisioning page allows you to search for the provisioning tasks assigned to you, view details, set response, add notes, reassign, view task assignment history, view and manage form details, and manually complete a task.

You can perform the following tasks in the Provisioning Tasks page:

- Searching Provisioning Tasks
- Viewing Provisioning Task Details
- Setting Response for a Task
- Adding Notes to a Task
- Reassigning a Task
- Viewing Task Assignment History
- Viewing Form Details
- Modifying Form Details
- Retrying a Task
- Manually Completing a Task

9.2.1 Searching Provisioning Tasks

The Provisioning page allows you to search for the provisioning tasks assigned to you or on which your action is pending.

To search for provisioning tasks you can use:

- Basic Search for Provisioning Tasks
- Advanced Search for Provisioning Tasks

9.2.1.1 Basic Search for Provisioning Tasks

To perform basic search:

1. Log in to Identity Self Service.
2. Click the **Self Service** tab.
3. Click the **Provisioning Tasks** box, and select **Open Tasks**. The Provisioning page is displayed.

> **Note:**
>
> The Provisioning Tasks tile is a combination of open tasks and manual fulfillment tasks. As a result, the open task count is not displayed.

4. To perform basic search, select any one of the following search options from the Search drop-down:
   - Task Name
   - Beneficiary
   - Task Status
   - Application Instance
5. Enter value for the search option selected and, click the search icon.
6. The provisioning tasks that match the selected search criteria are displayed in a tabular format.

9.2.1.2 Advanced Search for Provisioning Tasks

To perform advanced search:

1. Log in to Identity Self Service.
2. Click the **Self Service** tab.
3. Click the **Provisioning Tasks** box, and select **Open Tasks**. The Provisioning page is displayed.
4. Click the **Advanced** link. The fields for advanced search page is displayed.
5. Specify values in one or more of the following fields:
   - **Match:** The **All** and **Any** options are read-only.
   - **Task Name:** Specify a task name that you want to search.
   - **Beneficiary**: Specify the beneficiary of the task.
   - **Task Status:** Select **Pending** or **Rejected** to search for tasks that are pending or rejected respectively.
   - **Application Instance:** Specify the name of the application instance associated with the provisioning task.

   After specifying the search criteria, when you click **Search,** the search results table is displayed.
6. Click **Search**. The provisioning tasks that match your search criteria are displayed in a tabular format.

Table 9-1 lists the fields in the search results table.

Table 9-1 Fields in the Provisioning Tasks Search Results Table

Field	Description
Task Name	The name of the task
Task Status	The status of the task, which is Pending or Rejected
Application Instance	The name of the application instance, which is affected by this task
Beneficiary	The user whose provisioned application instance will get affected because of this task
Date Assigned	The date and time when the Provisioning task has been assigned to the Assignee

Table 9-1 (Cont.) Fields in the Provisioning Tasks Search Results Table

Field	Description
Assignee	The user to whom the task is assigned
Request ID	The ID of the provisioning request task
Account Name	The name of the account being provisioned

9.2.2 Viewing Provisioning Task Details

The Task Details page allows you to view the task details.

To view provisioning task details:

1. Login to Identity Self Service.
2. Click the **Self Service** tab.

   Click the **Provisioning Tasks** box, and select **Open Tasks**. The Provisioning page is displayed.
3. Search and select the task whose detail you want to view.
4. From the Actions menu, select **Open.** Alternatively, you can click **Open** on the toolbar. The Task Details page in displayed in a new window.

Table 9-2 lists the fields in the Task Details window:

Table 9-2 Fields in the Task Details Window

Field	Description
Task Name	The following fields are displayed in this section: • **Resource Name**: The name of the resource, which is affected by this task • **User**: The beneficiary user name • **Assigned to User**: The user to whom or role to which the task is assigned. **Note**: If the task is assigned to a role, this property will come as "Assigned to Role" with the role details • **Status**: The status of the task, Pending or Rejected • **Task Description**: A description of the task
Response and Error Details	The following fields are displayed in this section: • **Response**: The response set by the user on the Set Response page. **Note:** For information about setting response, see Setting Response for a Task. • **Response Description**: The description of the response that is defined in the Response tab of the Task Definition section in Oracle Identity Manager Design Console.
Error Details	The error, if any, while setting the response. The following fields are displayed in this section: • **Notes**: The additional comments entered by the approver.

Table 9-2 (Cont.) Fields in the Task Details Window

Field	Description
Schedule Detail	The following fields are displayed in this section: • **Projected Start**: The date when the task is scheduled to start • **Projected End**: The date when the task is suppose to end • **Actual Start**: The date when the task was started • **Actual End**: The date when the task was ended • **Last Update**: The date when the task was last updated
Add Notes	You can provide additional comments. For more information, see Adding Notes to a Task.
Reassign	You can reassign a task to another user or role. For more information, see Reassigning a Task.
Set Response	You can set a response for the task while taking an action on the task. For more information, see Setting Response for a Task.
Task Assignment History	You can view the task assignment history for a task. For more information, see Viewing Task Assignment History.

9.2.3 Setting Response for a Task

As an approver, you can set a response for the task while taking an action on the task.

To set a response for a task:

> **Note:**
>
> Response cannot be set if there are no response codes defined for the corresponding tasks. Response codes are defined by using Oracle Identity Manager Design Console, as described in Responses Tab in *Developing and Customizing Applications for Oracle Identity Governance*.

1. In the Self Service tab, click the **Provisioning Tasks** box, and select **Open Tasks**. The Provisioning page is displayed.
2. Search and select a task for which you want to set a response.
3. From the Actions menu, select **Set Response**. Alternatively, click **Set Response** on the toolbar. The Specify Task Responses page is displayed.
4. Select one of the multiple responses defined, and click **Set Response.** The response is set.

9.2.4 Adding Notes to a Task

Notes are additional comments provided by the approver. These comments are optional.

To add notes to a task:

1. In the Provisioning page, search and select a task for which you want to add notes.
2. From the Actions menu, select **Open.** Alternatively, you can click **Open** on the toolbar. The Task Details window is displayed.
3. In the Task Details window, click **Add Notes**. The Add Additional Notes dialog box is displayed.
4. In the Notes field, enter the note that you want to add to the task.
5. Click **Save Notes**.

9.2.5 Reassigning a Task

As the approver, you can reassign a task to another user or role for taking appropriate action on the task. When the task is reassigned to another user, the assignee becomes the approver. When the task is reassigned to a role, any one member of that role can approve or reject the task.

To reassign a task to another user or role:

1. In the Provisioning page, search and select the task that you want to reassign.
2. From the Actions menu, select **Open.** Alternatively, you can click **Open** on the toolbar. The Task Details window is displayed.
3. In the Task Details window, click **Reassign**. The Reassign Open Task dialog box is displayed.
4. Select **User** or **Role** depending on what you want to search for. In the Search section, search for a user or role. A list of users or roles is displayed, depending on your search.
5. In the Reassign column, select a user or role to whom you want to assign the task.
6. Click **Reassign.**
7. Check whether the value in the Assigned to User field in the Task Details window is properly updated according to the reassignment action.

9.2.6 Viewing Task Assignment History

You can view the task assignment history for a task in the Task History window.

To view the assignment history of a task:

1. In the Provisioning page, search and select a task for which you want to view the task assignment history.
2. From the Actions menu, select **Open.** Alternatively, you can click **Open** on the toolbar. The Task Details window is displayed.
3. In the Task Details window, click **Task Assignment History**. The Task Assignment History window is displayed. Table 9-3 lists the columns of the task assignment history.

Table 9-3 Fields in the Task History Window

Field	Description
Task Status	The status of the task, Pending or Rejected
Task Action	The source details of the task, for example, when the task is first created it will be "Engine". If the user reassigns the task, it will be "User".
Assign Type	The type of the assignee of the task, for example, when the task is assigned for the first time, it is "Default Task Assignment". If the task is reassigned, then its value is either user or role.
Assigned to User	The user to whom the task is assigned
Assigned to Role	The role to which the task is assigned
Assigned By	The user who assigned the task
Assigned Date	The date when the task was assigned

9.2.7 Viewing Form Details

You can view the process form or account details attached with a task. These are process forms associated with the underlying process definition. A task is embedded in the process definition.

To view the process form attached with a task:

1. In the Provisioning Tasks page, search and select a task whose process form you want to view.
2. From the Actions menu, select **View Form.** Alternatively, you can click **View Form** on the toolbar. The Edit Form page for the selected task is displayed.

9.2.8 Modifying Form Details

You can edit the process form associated with a provisioning workflow to provide missing information, if any.

To modify the process form details:

1. In the Provisioning Tasks page, search and select a task whose process form you want to modify.
2. From the Actions menu, select **Edit Form.** Alternatively, you can click **Edit Form** on the toolbar.
3. In the Edit Form page, modify the required details, and click **Save**.

9.2.9 Retrying a Task

As the approver, you can retry a task when an error is generated while setting the response in the first attempt.

To retry a task:

> **Note:**
>
> Only automated tasks can be retried, and an adapter must be attached to the task. Manual tasks cannot be retried.

1. In the Provisioning Tasks page, search and select a task that you want to retry.
2. From the Actions menu, select **Retry.** Alternatively, you can click **Retry** on the toolbar.
3. A warning message is displayed prompting you to confirm whether you want to retry the task.
4. Click **Retry.**

9.2.10 Manually Completing a Task

A manual fulfillment task is created if you want to introduce manual steps to mandate an administrator to take some action either before or after the provisioning operation. You can manually complete a task from the Provisioning page.

This section describes the different types of provisioning operations and how to complete manual fulfillment task in the following sections:

- Different Types of Provisioning Operations
- Completing Manual Fulfillment Task

9.2.10.1 Different Types of Provisioning Operations

There are two types of provisioning operations:

- **Automated:** These are provisioning operations that take place in an automated manner by using an Oracle Identity Manager connector for a particular target application.
- **Manual:** These are provisioning operations that are manually performed with human intervention.

A manual fulfillment task is created during manual provisioning operations. In addition, a manual fulfillment task is created during automated provisioning operation if you want to introduce manual steps to mandate an administrator to take some action either before or after the provisioning operation. For example, if the task requires creation of an account in the EBusiness or AD target, then you must manually fulfill the task after manually creating the account.

9.2.10.2 Completing Manual Fulfillment Task

To complete a manual fulfillment task:

1. In the Provisioning page, search and select the task that you want to manually complete.
2. From the Actions menu, select Manual Complete. Alternatively, click Manual Complete on the toolbar.

   A warning is displayed asking for confirmation.

3. Click **Manually Complete**.

9.3 Managing Manual Fulfillment Tasks

The Manual Fulfillment page in the Identity Self Service lists all tasks for provisioning of disconnected application instances.

You can perform the following tasks in the Manual Fulfillment page:

- About Manual Fulfillment Task
- Viewing and Editing Task Details
- Completing a Task
- Rejecting a Task
- Adding Comments and Attachments
- Requesting for Information
- Reassigning a Task
- Modifying Grant Duration

9.3.1 About Manual Fulfillment Task

As a part of provisioning to disconnected application instance, a task is generated. The task is assigned to a user based on the assignment rules specified in the Manual Provisioning Workflow. See "Disconnected Application Instances" in the *Administering Oracle Identity Governance* for information about disconnected application instances.

When the manual action is done, the administrator or the assignee logs into Identity Self Service and completes the manual provisioning task.

9.3.2 Viewing and Editing Task Details

You can view and modify manual fulfillment task details from the Manual Fulfillment page.

To view and edit the details of a manual fulfillment task:

1. Login to Oracle Identity Self Service.
2. Click the **Self Service** tab.
3. Click the **Provisioning Tasks** box, and select **Manual Fulfillment**. The Manual Fulfillment page is displayed.
4. Search for the task for which you want to view or modify the details. To do so, enter a task title in the search field, and click the search icon.
5. Click the task that you want to open. The details of the task is displayed in a separate tab. The task details page consists of the following sections:
    - **Details:** Displays information about the assignee of the task.
    - **Contents:** Displays the details of the task, such as application instance name and beneficiary details.
    - **Cart Details:** Lists the cart items that will be provisioned when the task is completed.
    - **Request Details:** Displays the details of the selected cart item. This consists of:

  - **Details:** Enables you to modify the account information before fulfilling the task.
  - **Grant Duration:** Enables you to modify the duration for which the disconnected application will be provisioned. For more information, see Adding and Removing Grant Duration.
- **History:** Displays all actions taken on the task. You can filter the task history by clicking Options and selecting one or more of the following options:
  - **Show all:** To show all actions in the task
  - **Exclude system approvals:** To exclude the approvals by Oracle Identity Manager
  - **Combine Repeated Approvals:** To combine the approvals that have been done repeatedly
  - **Include Future approvals:** To show the approvals required in future dates
- **Comments:** Displays the comment associated to the task, and allows to add a comment to the task.
- **Attachments:** Displays any attachments with the task, and allows to add or modify the attachments.

6. In the Request Details section, modify the attribute values, and click **Fulfill**.

9.3.3 Completing a Task

You can check details of the task, provide comments if required and complete the task.

To complete a task:

1. In the Manual Fulfillment page, search and select the task that you want to complete.
2. From the Actions menu, select **Complete**. Alternatively, you can open the task details, and click **Complete**.

> **Note:**
>
> If the request is to modify a parent form, then a bubble icon is displayed adjacent to the modified fields in the manual fulfillment form. This bubble icon indicates that the particular field value has been modified to a newer value.

9.3.4 Rejecting a Task

You can check details of the task, provide comments if required and reject the task.

To reject a task:

1. In the Manual Fulfillment page, search and select the task that you want to reject.
2. From the Actions menu, select **Reject**. Alternatively, you can open the task details, and click **Reject**.

9.3.5 Adding Comments and Attachments

After you view the task details, you can add comments and attachments prior to performing any operation on the task such as approving, rejecting, or reassigning the request.

An attachment can either be a hyperlink or an actual file. It is recommended that the size of the file attachment that you upload be less than 2 MB. If you want to upload file attachments of size greater than 2 MB, then you must change the ADF configuration and increase the size limit.

To add comments and attachments to a task:

1. In the Manual Fulfillment page, search the task to which you want to. add a comment or attachment.
2. Click the task to open the task details.
3. To add a comment:
   a. In the Comments section, click the Create icon. The Create Comment dialog box is displayed.
   b. In the comment field, enter a comment for the task.
   c. Click **OK**.
4. To add an attachment:
   a. In the Attachments section, click the Add icon. The Add Attachment dialog box is displayed.
   b. Select one of the following options as the attachment type:
      - **URL:** Select to specify the URL to an attachment. Enter the attachment name in the Name field, and enter the URL to the attachment in the URL field.
      - **Desktop File:** Select to upload a file from the desktop. Click Browse, and select the attachment.
   c. Click **OK**.
5. Click **Task**, **Save**.

9.3.6 Requesting for Information

You can request for additional information from the user before taking appropriate action on the task.

To request for information about a task:

1. In the Manual Fulfillment page, search for the task for which you want to request for information.
2. Open the task details.
3. Select **Actions**, **Request Information**. The Request More Information dialog box is displayed.
4. Select any one of the following options:
   - **Participant:** To select a participant from the list. Also, select a return option to specify whether the task will return to the current assignee or will go to subsequent participants for further action.

- **Other users:** To select a user from whom information is requested. Click the lookup icon, and search and select a user.

5. Click **OK**.

9.3.7 Reassigning a Task

As the approver, you can reassign a task to another user or role for taking appropriate action on the task. When the task is reassigned to another user, the assignee becomes the approver. When the task is reassigned to a role, any one member of that role can approve or reject the task.

To reassign a task that is assigned to you:

1. In the Manual Fulfillment page, search for the task that you want to reassign.
2. Select the task. From the Actions menu, select **Reassign**.

   Alternatively, open the task details, and select **Actions**, **Reassign**.

   The Reassign Task dialog box is displayed.
3. Select any one of the following options:
   - **Reassign (transfer task to another user or group):** To reassign the task to another user, group, or application role. On selecting this option, you can search and select users, groups, or application roles for reassigning.
   - **Delegate (allow specified user to act on my behalf):** To delegate the task to a user that you can search and select. The delegated user will take actions on the task on your behalf. The privileges of the delegatee are based on the delegator's privileges.
4. Click **OK**.

9.3.8 Modifying Grant Duration

You can modify the grant duration of the account or entitlement which are pending for approval from the Request Details tab.

To modify the grant duration of the account or entitlement to the user:

1. In the Manual Fulfillment page, search for the task for which you want to modify the grant duration of the account or entitlement.
2. Open the request details.
3. In the Request Details tab, click the Grant Duration icon.
4. Modify the values in the following fields:
   - Start Date: The start date when the account or entitlement will be provisioned. This must be a future date. This field is not available for modification if the account or entitlement is already assigned to the user.
   - End Date: The end date when the account or entitlement will be revoked.

   For detailed information about grant duration, see Adding and Removing Grant Duration.
5. Save the task.

10

Managing Certification Review Tasks

The Oracle Identity Manager allows you to view and make decisions on certifications. You can do this from the Inbox or the Pending Certifications page of Oracle Identity Self Service. This section describes working with certifications in the following topics:

- Searching and Viewing Certifications
- Completing Certifications
- Claiming and Releasing Group Certifier Assignments

> **Note:**
>
> This document describes the actions you can perform in the Pending Certifications page. For certification and identity audit tasks, use the Certifications and Pending Violations tiles respectively. If you are using the Inbox Generic view, then do not use the Actions menu because the actions are not supported for certification and identity audit.
>
> For an overview of identity certification and information about operations you can perform by using the Dashboard, see Using Identity Certification.

10.1 Searching and Viewing Certifications

You can search and filter certifications in the Pending Certifications page and view the certification details.

This section contains the following topics:

- Searching Certifications in the Pending Certifications Page
- Accessing Certification Tasks From the Pending Certifications Page

10.1.1 Searching Certifications in the Pending Certifications Page

You can search for the certification review tasks assigned to you.

To perform simple search for certifications:

1. Login to Oracle Identity Self Service.
2. Click the **Self Service** tab.
3. Click the **Certifications** box. The Pending Certifications page is displayed with a list of certification review tasks assigned to you.
4. From the Status list, select the certification status that you want to search for, for example, **Assigned**. Select **Any** to search for any certification irrespective of the status.

> **Note:**
>
> By default, completed certifications are not shown in the Pending Certifications page. If you want to display the completed certifications in the Pending Certifications page, perform the steps described in the Tech Note *Pending Certifications Not Displaying Completed Certifications (Doc ID 2400640.1)* at My Oracle Support web site at the following URL: https://support.oracle.com

5. In the Search box, specify a search criterion, for example, the certification name.
6. Click the Search icon. The certifications that match your search criteria are listed in the search results table.

> **Tip:**
>
> - To sort the data in the search results table, place the mouse pointer on a column name. Up and down arrows are displayed on the column names. Click the up arrow to sort in ascending order. Click the down arrow to sort in descending order.
> - In this release of Oracle Identity Manager, you can sort the certifications by their percent completion. If you place your mouse pointer on the Percent Complete column, the up and down arrow keys are displayed. Click the up arrow to sort by ascending order of percent completion, and click the down arrow to sort by descending order of percent completion.

10.1.2 Accessing Certification Tasks From the Pending Certifications Page

You can view details of different types of certification tasks like User Certification, Role Certification, Application Instance Certification, and Entitlement Certification.

This section describes how to access certification tasks for each type of certification:

- Viewing User Certification Details
- Viewing Role Certification Details
- Viewing Application Instance Certification Details
- Viewing Entitlement Certification Details

> **Note:**
>
> The pages that display certification details and the details for user access rights, role content and membership, account details for application instances and entitlements enable you to personalize the contents of the pages. For example, you can use saved search, show/hide columns, and sort the data in columns. These personalization features are similar in all pages in Oracle Identity Self Service. See Personalizing Self Service for information about personalizing pages in Oracle Identity Self Service.

10.1.2.1 Viewing User Certification Details

To view user certification details:

1. In the Self Service tab of Oracle Identity Self Service, click the **Certifications** box. The Pending Certifications page is displayed with a list of certification tasks assigned to you, and for which you are the primary reviewer or delegated reviewer.
2. Click a certification task name to open it in a new page. The user certification summary of the certification task opens in a new page.
3. Review the following sections of the user details:
   - The user certification name and certification creation date appears at the top of the page. Clicking the information icon adjacent to the certification name displays a Certification Details pop-up with detailed statistics of the current certification being reviewed. The details include information about Overview, Progress Details, and History.
   - In the table that lists the users, the user name is a hyperlink. Clicking this hyperlink opens the access details of the user.

     > **Note:**
     >
     > Access details of the user are described in steps 4 through 6 in this procedure.

   - The Detailed Information section consists of the following tabs:
     - **User Information:** This tab displays user attributes that are included in the certification snapshot during certification generation. The user name is a hyperlink. Click the user name to display the user details in a new tab.
     - **Risk Summary:** This tab identifies why a user's Risk Summary is High/ Medium/Low based on various factors. The pie chart in this tab displays the overall breakdown of a user's risk. Click any area of the chart to open the detail screen of the user certification. To view the risk items in a tooltip, place your mouse pointer over the charts.

       This tab also displays a graph that breaks down the risk levels based on the roles, accounts, and entitlements the user has, as well as their associated risk levels. Click any area of the graph to open the detail screen of the user certification. To view the risk items in a tooltip, place your mouse pointer over the graph.

  - **Action History:** This tab displays the various delegation paths available on the user details page, and a trail of the actions taken by the reviewers as well as by Oracle Identity Manager. Possible details displayed include all the actions that are available in the Actions menu, as well as proxy, escalate, expire, and route. The route action indicates that certification oversight is active.

4. Review the following sections of the role details displayed when you click the user name to view the user details:

> **Note:**
>
> Depending on the entities assigned to the user, such as roles, accounts, and entitlements, the information is displayed, as described in steps 4 through 6.

- The User Detail section displays the user attributes that are included in the certification snapshot during certification generation.
- The table lists the roles with Display Name, Action, and Risk Summary.
- The Detailed Information section consists of the following tabs:
  - **Catalog Information:** This tab displays the default catalog attributes that are included as part of the default snapshot creation. The Name and Owner fields are hyper-linked. Clicking these hyperlinks opens the role detail and user details pages in new tabs.
  - **Risk Summary:** This tab identifies why the Risk Summary is High, Medium, or Low based on various factors, such as Item Risk, Last Certification Decision, Provisioning Method, and Audit Violations. If there are no audit violations associated with the item, then the Audit Violations entry is not displayed. The Provisioning Method field is hyper-linked. Clicking this hyperlink opens the appropriate access policy or access request details in a new tab.
  - **Certification History:** This tab displays the various certification decisions made by reviewers in the past on the given line-item.
  - **Action History:** This tab displays the phase in which the reviewer made a given decision. Possible values include all the actions that are available in the Actions menu, as well as proxy, escalate, and expire.
  - **Audit Violations:** This tab displays a list of audit violations associated with the selected item. Information includes the policy name, status, remediator, and severity for each audit violation. If there are no audit violations, then the list is empty.

5. Review the following sections of the account details:

- The account name and the application instance name are displayed in the table, along with the underlying entitlements associated to the account. Accounts and entitlements are indicated by different icons.
- The Detailed Information section consists of the following tabs:
  - **Catalog Information:** This tab displays the account details that are the default catalog attributes. These attributes must be included as part of the default snapshot creation. The Name and Certifier fields are hyper-linked.

Clicking these hyperlinks opens the account detail and user details pages in new tabs.

- **Risk Summary:** This tab identifies why the Risk Summary is High, Medium, or Low based on various factors, such as Item Risk, Last Certification Decision, Provisioning Method, and Audit Violations. If there are no audit violations associated with the item, then the Audit Violations entry is not displayed. The Provisioning Method field is hyper-linked for an access request. Clicking this hyperlink opens the appropriate access policy or access request details in a new tab.
- **Certification History:** This tab displays the various certification decisions made by reviewers in the past on the given line-item.
- **Action History:** This tab displays the phase in which the reviewer made a given decision. Possible values include all the actions that are available in the Actions menu, as well as proxy, escalate, and expire.
- **Audit Violations:** This tab displays a list of audit violations associated with the selected item. Information includes the policy name, status, remediator, and severity for each audit violation. If there are no audit violations, then the list is empty.

6. Review the following sections of the entitlement details:
   - The account name and the application instance name are displayed in the table, along with the underlying entitlements associated to the account. Accounts and entitlements are indicated by different icons.
   - The Detailed Information section consists of the following tabs:
     - **Catalog Information:** This tab displays the entitlement details that are the default catalog attributes. These attributes must be included as part of the default snapshot creation. The Display Name and Certifier fields are hyper-linked. When you click the Display Name of the entitlement, the granular entitlement hierarchy, if it is being captured in the catalog for a given entitlement, is displayed in a new tab. Clicking the Certifier name opens the user details page in a new tabs.
     - **Risk Summary:** This tab identifies why the Risk Summary is High, Medium, or Low based on various factors, such as Item Risk, Last Certification Decision, Provisioning Method, and Audit Violations. If there are no audit violations associated with the item, then the Audit Violations entry is not displayed. The Provisioning Method field is hyper-linked. Clicking this hyperlink opens the appropriate access policy or access request details in a new tab.
     - **Certification History:** This tab displays the various certification decisions made by reviewers in the past on the given line-item.
     - **Action History:** This tab displays the phase in which the reviewer made a given decision. Possible values include all the actions that are available in the Actions menu, as well as proxy, escalate, and expire.
     - **Audit Violations:** This tab displays a list of audit violations associated with the selected item. Information includes the policy name, status, remediator, and severity for each audit violation. If there are no audit violations, then the list is empty.
7. To display the details of the access rights for the next user in the certification task, click **Next** at the top of the page. You can click First, Previous, Next, and Last buttons to navigate between the pages for the access rights of each user. You can click **Back to Summary** to go back to the user certification detail page.

10.1.2.2 Viewing Role Certification Details

To view role certification details:

1. In the Self Service tab of Oracle Identity Self Service, click the **Certifications** box. The Pending Certifications page is displayed with a list of certification tasks assigned to you, and for which you are the primary reviewer or delegated reviewer.
2. Click a certification task name to open it in a new page. Page 1 or the role certification summary page of the certification task opens.
3. Review the following sections of the role certification details page:
   - The role certification name and certification creation date appears at the top of the page. Clicking the information icon adjacent to the certification name displays a pop-up with detailed statistics of the current certification being reviewed.
   - In the table that lists the roles, the user name is a hyperlink. Clicking this hyperlink opens the role details. The table also displays the Members and Policies columns.
   - Select a role in the certification table. The Detailed Information section displays the following tabs:
     - **Catalog Information:** This tab displays all catalog attributes of the selected role. The Role Name and Certifier fields are hyperlinked. Clicking these hyperlinks opens the role details and user details in new tabs.
     - **Action History:** This tab displays the various delegation paths available on the role details page, and a trail of the actions taken by the reviewers as well as by Oracle Identity Manager. Possible actions include delegate, re-assign, escalate, proxy, or route. The route action indicates that certification oversight is active.
4. In the certification table, click a role name to open the role detail. The role detail page consists of the following tabs:
   - **Members:** This tab lists the role membership of the open role. Select a row in the members table to display the Detailed Information section, which consists of the User Information, Risk Summary, Certification History, Action History, and Audit Violations tabs.
   - **Policies:** This tab lists the policies associated with the open role. Select a row in the policies table to display the Detailed Information section, which consists of the Policy Information, Certification History, and Action History tabs.
5. In the Policies tab, expand a policy by clicking the icon adjacent to the policy. The entitlements associated with the policy are listed in the table. Select the entitlement to display the entitlement details in the Detailed Information section. The entitlement details are displayed in the Catalog Information, Certification History, and Action History tabs.
6. To display the role contents and role members for the next role in the certification task, click **Next** at the top of the page. You can click First, Previous, Next, and Last buttons to navigate between the pages for the role contents and role member details of each role. You can click **Back to Summary** to go back to the role certification detail page.

10.1.2.3 Viewing Application Instance Certification Details

To view application instance certification details:

1. In the Self Service tab of the Oracle Identity Self Service, click the **Certifications** box. The Pending Certifications page is displayed with a list of certification tasks assigned to you, and for which you are the primary reviewer or delegated reviewer.
2. Click a certification task name to open it in a new page. Page 1 or the application instance certification summary page of the certification task opens.
3. Review the following sections of the application instance certification details page:
   - The application instance certification name and certification creation date appears at the top of the page. Clicking the information icon adjacent to the certification name displays a pop-up with detailed statistics of the current certification being reviewed.
   - In the table that lists the application instances, the application instance name is a hyperlink. Clicking this hyperlink lists the accounts belonging to the selected application instance.
   - Select an application instance in the certification table. The Detailed Information section displays the following tabs:
     - **Catalog Information:** This tab displays all catalog attributes of the selected application instance. The Certifier field is hyperlinked. Clicking this hyperlink opens the user details in a new tab.
     - **Action History:** This tab displays the various delegation paths available on the application instance details page, and a trail of the actions taken by the reviewers as well as by Oracle Identity Manager. Possible values include all the actions that are available in the Actions menu, and delegate, re-assign, escalate, proxy, or route. The route action indicates that certification oversight is active.
4. In the certification table, click an application instance name to open the application instance detail. This page lists the application instance names and account names along with the underlying entitlements associated to the account.
5. Click an account to display the account details in the Detailed Information section. This section displays the account details in the Catalog Information, Risk Summary, Certification History, and Action History tabs.
6. Click an entitlement to display the entitlement details in the Detailed Information section. This section displays the entitlement details in the Catalog Information, Risk Summary, Certification History, Action History, and Audit Violations tabs.
7. To display the set of users who have accounts for the next the application instance in the certification task, click **Next** at the top of the page. You can click First, Previous, Next, and Last buttons to navigate between the pages for the account details of each application instance. You can click **Back to Summary** to go back to the application instance certification detail page.

10.1.2.4 Viewing Entitlement Certification Details

To view entitlement certification details:

1. In the Self Service tab of Oracle Identity Self Service, click the **Certifications** box. The Pending Certifications page is displayed with a list of certification tasks assigned to you, and for which you are the primary reviewer or delegated reviewer.

2. Click a certification task name to open it in a new page. Page 1 or the entitlement certification detail page of the certification task opens.
3. Review the following sections of the entitlement certification details page:
   - The entitlement certification name and certification creation date appears at the top of the page. Clicking the information icon adjacent to the certification name displays a pop-up with detailed statistics of the current certification being reviewed.
   - In the table that lists the entitlements, the entitlement name is a hyperlink. Clicking this hyperlink displays the entitlement assignment details of the selected entitlement.
   - Select an entitlement in the certification table. The Detailed Information section displays the following tabs:
     - **Catalog Information:** This tab displays all catalog attributes of the selected application instance. The Display Name and Certifier fields are hyperlinked. Clicking these hyperlinks opens the entitlement details and user details in new tabs.
     - **Action History:** This tab displays the various delegation paths available on the entitlement details page, and a trail of the actions taken by the reviewers as well as by Oracle Identity Manager. Possible values include all the actions in the Actions menu, and delegate, re-assign, escalate, proxy, or route. The route action indicates that certification oversight is active.
4. In the certification table, click an entitlement name to open the entitlement assignment detail. This page lists the account names of the selected entitlement.
5. Click an account to display the account details in the Detailed Information section. This section displays the account details in the Account-Owner Information, Risk Summary, Certification History, and Action History tabs.
6. Click an entitlement to display the entitlement details in the Detailed Information section. This section displays the entitlement details in the Catalog Information, Risk Summary, Certification History, Action History, and Audit Violations tabs.
7. To display the set of users who have accounts for the next entitlement in the certification task, click **Next** at the top of the page. You can click First, Previous, Next, and Last buttons to navigate between the pages for the account details of each entitlement. You can click **Back to Summary** to go back to the entitlement certification detail page.

10.2 Completing Certifications

You can set any missing decisions on user, role-assignments, accounts, or entitlement-assignments to Certify.

Completing certifications is described in the following sections:

- Completing User Certifications
- Completing Role Certifications
- Completing Application Instance Certifications
- Completing Entitlement Certifications

10.2.1 Completing User Certifications

User certification enables managers to verify their employees and the role assignments, accounts and entitlement assignments for each.

Completing a user certification involves the following steps:

- Making Certification Decision on the Users
- Reviewing Roles and Entitlements
- Finishing the User Certification

10.2.1.1 Making Certification Decision on the Users

When a certification task is opened, you may be required to verify the access of each user. This verification step is optional based on the configuration settings set in the certification definition. If verification is not required, then the initial summary view of users are skipped and you are presented with the user detail view.

If verification is required, then a decision must be made on each of the users that you have been asked to review. To do so:

1. In the Pending Certifications page, open the new or in progress certification review task. Page 1 of the certification task is displayed with a list of users.

> **Note:**
>
> Page 1 of the certification task provides the following capabilities:
>
> - Sort by percentage completion: In this release of Oracle Identity Manager, you can sort the certifications by their percent completion. If you place your mouse pointer on the Percent Complete column, the up and down arrow keys are displayed. Click the up arrow to sort by ascending order of percent completion, and click the down arrow to sort by descending order of percent completion.
> - Query By Example: You can filter the certification tasks by using Query By Example. For more information about using Query By Example, see Using Query By Example.

2. Review the list of users and verify that each employee works for you, and that you are responsible for verifying their access.
3. From the Actions menu, select any one of the following for each user:
   - **Claim:** Select to restore a user to your verification queue for certification. This might happen automatically, depending on the values in certification configuration. See Configuring Certification Options for information about the certification configuration options. However, even if each user is claimed automatically, you are free to choose another action.
   - **Revoke:** Select if the user is no longer part of the organization. This action removes the user from the certification process, and you will not approve or revoke roles and entitlements for this user. To return a user to your verification queue, select the user name, and select **Claim** from the Actions menu.

- **Revoke Access:** Select to revoke the roles, entitlements, and applications of the active user. After access is revoked by clicking this menu option, the action and comment for the user in the user certification page are not displayed. The action and comment for the revoke access operation is displayed in the user details page.

  > **Note:**
  >
  > This option is available after you apply Oracle Identity Governance Bundle Patch 12.2.1.4.210428.

- **Re-assign:** Select if the user works for someone else who should now be responsible for verifying the user's assigned roles and entitlements. This action removes the selected user(s) from the current certification, creates a new certification with the selected user(s), and assigns the person you specify as the primary reviewer for that new certification.
- **Abstain:** Select if the employee does not work for you and you do not know who should be responsible for verifying the user's assigned roles and entitlements. This action on the user records on each role and entitlement assigns to the user your decision to abstain, that is, to leave each assignment as it is. If you know who should be responsible, then you can reassign the user instead.

After you have taken a verification action on each user, you must make certification decisions on each role and entitlement assigned to the users you have claimed. You do not need to make any further certification decisions on a user that you have revoked or reassigned or abstained. Normally, this means that you will open each user and then review its roles and entitlements, as described in Reviewing Roles and Entitlements. However, you may also choose to delegate one or more users to another person, which allows that person to make certification decisions on the roles and entitlements assigned to that user. The following actions are available from the Actions menu:

- **Open:** Select this action to review the details of each user and to make certification decisions on the roles and entitlements assigned to the user. See Reviewing Roles and Entitlements.
- **Delegate:** Select this action to allow another person to make decisions on the access privileges of each selected user. This action will create a new delegated-review task that contains the selected user(s) and will assign the task to the person you specify as delegate. Responsibility still remains with you, the primary reviewer.
- **Un-delegate:** This action applies only to delegated users. This action removes each selected user from the delegated-review task and returns decision-making rights to you, the primary reviewer.

The Actions menu offers two additional convenience actions that are useful after you have made some certification decisions on the details of a user. These actions affect the decisions on multiple details, that is, accesses of each selected user:

- **Complete:** Sets any missing decisions on role-assignments, accounts, or entitlement-assignments to Certify.
- **Reset Status:** Clears all decisions made on the user including decisions on the user's access.

- **Edit Comment:** Allows you to edit the comment associated with the certification task.
- **Sign-off:** Allows you to complete the certification by signing off.

10.2.1.2 Reviewing Roles and Entitlements

Use the details view of the certification to review a user's role assignments, accounts, and entitlement assignments. The details view can be accessed by selecting a user in the summary view, and clicking **Open** from the Actions menu, or by clicking the user name.

After your selections are made, you can use the Actions menu to select the appropriate action. The Actions menu contains the following options:

- **Certify:** You approve each selected assignment.
- **Revoke:** You disapprove each selected assignment. This decision indicates that the user no longer needs the privilege and the assignment should be removed. When you select this option, a dialog box might be displayed that asks for comments. Type a note in the Comments pop-up, and click **OK**.
- **Certify Conditionally:** You approve each selected assignment, but only temporarily. This action also requires you to specify an end date on which your approval expires.
- **Abstain:** You take no position on each selected assignment. This records your decision to leave the assignment as it is.
- **Reset:** Use this to clear any decision you have made on the selected assignment.

For each action, optional comments can be added. By default, every decision other than to certify, such as Revoke, Certify Conditionally, and Abstain, allow optional comments.

10.2.1.3 Finishing the User Certification

The final step in the certification cycle is the sign-off action. Signing off can only be done when every access privilege has a decision assigned to it. When this state is reached, Oracle Identity Manager automatically prompts you to sign-off on all the decisions taken. If you choose not to sign-off at that time, then you can manually invoke the sign-off dialog box later assuming that all access privileges are still completed. The process for signing off is the same whether automatically prompted by the system or manually activated.

To manually sign-off:

1. From the Actions menu, select **Sign-off**. The Sign-off dialog box is displayed asking to complete the certification.
2. To complete the certification, select **Yes**, and enter a password in the Password Required field. The password option is configurable and set in the certification definition. If disabled, the password field is not displayed in the Sign-off dialog box.

   Alternatively, to complete the certification later, select **No**.
3. Click **OK**.

Upon successful sign-off, the tab displaying the certification is closed automatically and a confirmation message is displayed.

If the `FlexibleCertificationProcess` composite is selected in the Certification Configuration page of Oracle Identity System Administration or while creating the certification definition, then the certification tasks are assigned to the user's manager by default. Here, the user's manager is the overseer. The certification is not complete until the overseer signs off. The certification will go to the completed stage only after sign-off by the overseer.

10.2.2 Completing Role Certifications

Role certification enables role owners to certify roles and role content.

Completing a role certification involves the following steps:

- Making Certification Decisions on the Roles
- Reviewing the Contents of the Roles
- Finishing the Role Certification

10.2.2.1 Making Certification Decisions on the Roles

When a certification task is opened, you may be required to verify the access of each role. This verification step is optional based on the configuration settings set in the certification definition. If verification is not required, then the initial summary view of role will be skipped, and you will be presented with the role detail view.

If verification is required, then a decision must be made on each of the roles for which you are the role owner. To do so:

1. In the Pending Certifications page, open the new or in progress certification review task. Page 1 of the certification task is displayed with a list of roles.

> **Note:**
>
> Page 1 of the certification task provides the following capabilities:
>
> - Sort by percentage completion: In this release of Oracle Identity Manager, you can sort the certifications by their percent completion. If you place your mouse pointer on the Percent Complete column, the up and down arrow keys are displayed. Click the up arrow to sort by ascending order of percent completion, and click the down arrow to sort by descending order of percent completion.
> - Query By Example: You can filter the certification tasks by using Query By Example. For more information about using Query By Example, see Using Query By Example.

2. From the Actions menu, select any one of the following for each role:
   - **Claim:** Select to restore a role to your verification queue for certification. This might happen automatically, depending on the values in certification configuration. See Configuring Certification Options for information about the certification configuration options. However, even if each role is claimed automatically, you are free to choose another action.
   - **Revoke:** Select if the role is no longer appropriate. This action removes the role from the certification process, and you will not approve or revoke assignments for this role. To return a role to your verification queue, select the role name, and select **Claim** from the Actions menu.
   - **Re-assign:** Select to remove the role from the current certification and create a new one with the selected role. This action removes the selected role(s) from the current certification, creates a new certification with the selected

role(s), and assigns the person you specify as the primary reviewer for that new certification.

- **Abstain:** Select if the role is not appropriate and you do not know who should be responsible for verifying the role's assigned accounts, memberships, and entitlements. This action on the role records on each account and entitlement assigns to the role your decision to abstain, that is, to leave each assignment as it is. If you know who should be responsible, then you can reassign the role instead.

After you have taken a verification action on each role, you must make certification decisions on each policy and entitlement assigned to the roles you have claimed. You do not need to make any further certification decisions on a role that you have revoked or reassigned or abstained. Normally, this means that you will open each role and then review its policies and entitlements, as described in Reviewing the Contents of the Roles. However, you may also choose to delegate one or more roles to another person, which allows that person to make certification decisions on the policies and entitlements assigned to that role. The following actions are available from the Actions menu:

- **Open:** Select this action to review the details of each role and to make certification decisions on the policies and entitlements assigned to the role. See Reviewing the Contents of the Roles.
- **Delegate:** Select this action to allow another person to make decisions on the access privileges of each selected role. This action will create a new delegated-review task that contains the selected role(s) and will assign the task to the person you specify as delegate. Responsibility still remains with you, the primary reviewer.
- **Un-delegate:** This action applies only to delegated roles. This action removes each selected role from the delegated-review task and returns decision-making rights to you, the primary reviewer.

The Actions menu offers two additional convenience actions that are useful after you have made some certification decisions on the details of a role. These actions affect the decisions on multiple details, that is, accesses of each selected role:

- **Complete:** Sets any missing decisions on account or entitlement assignments to Certify.
- **Reset:** Clears all decisions made on the role including decisions on the role's access.

10.2.2.2 Reviewing the Contents of the Roles

Use the details view of the certification to review a role's policies, memberships, and entitlements. The details view can be accessed by selecting a role in the summary view and clicking the **Open** button from the Actions menu, or by clicking the role name.

After your selections are made, you can use the Actions menu to select the appropriate action. The Actions menu contains the following options:

- **Certify:** You approve each selected assignment.
- **Revoke:** You disapprove each selected assignment. This decision indicates that the role no longer needs the privilege and the assignment should be removed. When you select this option, a dialog box might be displayed that asks for comments. Type a note in the Comments pop-up, and click **OK**.
- **Certify Conditionally:** You approve each selected assignment, but only temporarily. This action also requires you to specify an end date on which your approval expires.
- **Abstain:** You take no position on each selected assignment. This records your decision to leave the assignment as it is.

- **Reset:** Use this to clear any decision you have made on the selected assignment.

For each action, optional comments can be added. By default, every decision other than to certify, such as Revoke, Certify Conditionally, and Abstain, allow optional comments.

Click the **Members** tab to review the users who have this role assigned. Revoke, Certify Conditionally, Certify, and/or Abstain the role's members as required. In this tab, an additional **Approve** option is available for two-phased user certification. Selecting this option copies the decision from Phase 1 to Phase 2. See Understanding Multi-Phased Review in User Certification for information about two-phased review.

10.2.2.3 Finishing the Role Certification

The final step in the certification cycle is the sign-off action. Signing off can only be done when every access privilege has a decision assigned to it. When this state is reached, Oracle Identity Manager automatically prompts you to sign-off on all the decisions taken. If you choose not to sign-off at that time, then you can manually invoke the sign-off dialog box later assuming that all access privileges are still completed. The process for signing off is the same whether automatically prompted by the system or manually activated.

To manually sign-off:

1. From the Actions menu, select **Sign-off**. The Sign-off dialog box is displayed asking to complete the certification.
2. To complete the certification, Select **Yes**, and enter a password in the Password Required field. The password option is configurable and set in the certification definition. If disabled, the password field is not displayed in the Sign-off dialog box.

   Alternatively, to complete the certification later, select **No**.
3. Click **OK**.

Upon successful sign-off, the tab displaying the certification is closed automatically and a confirmation message is displayed.

10.2.3 Completing Application Instance Certifications

Application instance certification involves certifying or revoking employee entitlements on one or more application instances. These entitlements are assigned directly to an employee and are not assigned as part of a role.

Completing an application instance certification involves the following steps:

- Making Certification Decisions on the Application Instances
- Reviewing Account and Entitlement Assignments
- Finishing the Application Instance Certification

10.2.3.1 Making Certification Decisions on the Application Instances

When a certification task is opened, you may be required to verify the access of each application instance. This verification step is optional based on the configuration settings set in the certification definition. If verification is not required, then the initial summary view of application instances is skipped, and you are presented with the

application instance detail view.If verification is required, then a decision must be made on each of the application instances. To do so:

1. In the Pending Certifications page, open the new or in-progress certification review task. Page 1 of the certification task is displayed with a list of review tasks.

> **Note:**
>
> Page 1 of the certification task provides the following capabilities:
>
> - Sort by percentage completion: In this release of Oracle Identity Manager, you can sort the certifications by their percent completion. If you place your mouse pointer on the Percent Complete column, the up and down arrow keys are displayed. Click the up arrow to sort by ascending order of percent completion, and click the down arrow to sort by descending order of percent completion.
> - Query By Example: You can filter the certification tasks by using Query By Example. For more information about using Query By Example, see Using Query By Example.

2. From the Actions menu, select any one of the following for each application instance:

   - **Claim:** Select to restore an application instance to your verification queue for certification. This might happen automatically, depending on the values in certification configuration. See Configuring Certification Options for information about the certification configuration options. However, even if each application instance is claimed automatically, you are free to choose another action.
   - **Revoke:** Select if the application instance is no longer appropriate. This action removes the application instance from the certification process, and you will not approve or revoke assignments for this application instance. To return an application instance to your verification queue, select the application instance name, and select **Claim** from the Actions menu.
   - **Re-assign:** Select to remove the application instance from the current certification and create a new one with the selected application instance. This action removes the selected application instance(s) from the current certification, creates a new certification with the selected application instance(s), and assigns the person you specify as the primary reviewer for that new certification.
   - **Abstain:** Select if the application instance is not appropriate and you do not know who should be responsible for verifying the application instance's assigned accounts and entitlements. This action on the application instance records on each account and entitlement assigns to the application instance your decision to abstain, that is, to leave each assignment as it is. If you know who should be responsible, then you can reassign the application instance instead.

   After you have taken a verification action on each application instance, you must make certification decisions on each account and entitlement assigned to the application instances you have claimed. You do not need to make any further certification decisions on an application instance that you have revoked or reassigned or abstained. Normally, this means that you will open each application instance and then review its accounts and entitlements, as described in Reviewing Account and Entitlement Assignments. However, you may also choose to delegate one or more application instances to another person, which allows that person to make certification decisions on the accounts and entitlements

assigned to that application instance. The following actions are available from the Actions menu:

- **Open:** Select this action to review the details of each application instance and to make certification decisions on the accounts and entitlements assigned to the application instance. See Reviewing Account and Entitlement Assignments.
- **Delegate:** Select this action to allow another person to make decisions on the access privileges of each selected application instance. This action will create a new delegated-review task that contains the selected application instance(s) and will assign the task to the person you specify as delegate. Responsibility still remains with you, the primary reviewer.
- **Un-delegate:** This action applies only to delegated application instances. This action removes each selected application instance from the delegated-review task and returns decision-making rights to you, the primary reviewer.

The Actions menu offers two additional convenience actions that are useful after you have made some certification decisions on the details of an application instance. These actions affect the decisions on multiple details, that is, accesses of each selected application instance:

- **Complete:** Sets any missing decisions on account or entitlement assignments to Certify.
- **Reset:** Clears all decisions made on the role including decisions on the application instance's access.

10.2.3.2 Reviewing Account and Entitlement Assignments

Use the details view of the certification to review an application instance's accounts and entitlements. The details view can be accessed by selecting an application instance in the summary view and clicking the **Open** button from the Actions menu, or by clicking the application instance name.

After your selections are made, you can use the Actions menu to select the appropriate action. The Actions menu contains the following options:

- **Certify:** You approve each selected assignment.
- **Revoke:** You disapprove each selected assignment. This decision indicates that the application instance no longer needs the privilege and the assignment should be removed. When you select this option, a dialog box might be displayed that asks for comments. Type a note in the Comments pop-up, and click **OK**.
- **Certify Conditionally:** You approve each selected assignment, but only temporarily. This action also requires you to specify an end date on which your approval expires.
- **Abstain:** You take no position on each selected assignment. This records your decision to leave the assignment as it is.
- **Reset:** Use this to clear any decision you have made on the selected assignment.

For each action, optional comments can be added. By default, every decision other than to certify, such as Revoke, Certify Conditionally, and Abstain, allow optional comments.

An additional **Approve** option is available for two-phased user certification. Selecting this option copies the decision from Phase 1 to Phase 2. See Understanding Multi-Phased Review in User Certification for information about two-phased review.

10.2.3.3 Finishing the Application Instance Certification

The final step in the certification cycle is the sign-off action. Signing off can only be done when every access privilege has a decision assigned to it. When this state is reached, Oracle Identity Manager automatically prompts you to sign-off on all the decisions taken. If you choose not to sign-off at that time, then you can manually invoke the sign-off dialog box later assuming that all access privileges are still completed. The process for signing off is the same whether automatically prompted by the system or manually activated.

To manually sign-off:

1. From the Actions menu, select **Sign-off**. The Sign-off dialog box is displayed asking to complete the certification.
2. To complete the certification, Select **Yes**, and enter a password in the Password Required field. The password option is configurable and set in the certification definition. If disabled, the password field is not displayed in the Sign-off dialog box.

   Alternatively, to complete the certification later, select **No**.
3. Click **OK**.

Upon successful sign-off, the tab displaying the certification is closed automatically and a confirmation message is displayed.

10.2.4 Completing Entitlement Certifications

Entitlement certifications enable you to certify whether employees should be able to access entitlements.

Completing an entitlement certification involves the following steps:

- Making Certification Decisions on the Entitlements
- Reviewing the Entitlement Assignments
- Finishing the Entitlement Certification

10.2.4.1 Making Certification Decisions on the Entitlements

When a certification task is opened, you may be required to verify the access of each entitlement. This verification step is optional based on the configuration settings set in the certification definition. If verification is not required, then the initial summary view of the entitlements is skipped, and you are presented with the entitlement detail view.If verification is required, then a decision must be made on each of the entitlements. To do so:

1. In the Pending Certifications page, open the new or in-progress certification review task. Page 1 of the certification task is displayed with a list of review tasks.

> **Note:**
>
> Page 1 of the certification task provides the following capabilities:
>
> - Sort by percentage completion: In this release of Oracle Identity Manager, you can sort the certifications by their percent completion. If you place your mouse pointer on the Percent Complete column, the up and down arrow keys are displayed. Click the up arrow to sort by ascending order of percent completion, and click the down arrow to sort by descending order of percent completion.
> - Query By Example: You can filter the certification tasks by using Query By Example. For more information about using Query By Example, see Using Query By Example.

2. From the Actions menu, select any one of the following for each entitlement:

   - **Claim:** Select to restore an entitlement to your verification queue for certification. This might happen automatically, depending on the values in certification configuration. See Configuring Certification Options for information about the certification configuration options. However, even if each entitlement is claimed automatically, you are free to choose another action.
   - **Revoke:** Select if the entitlement is no longer appropriate. This action removes the entitlement from the certification process, and you will not approve or revoke assignments for this entitlement. To return an entitlement to your verification queue, select the entitlement name, and select **Claim** from the Actions menu.
   - **Re-assign:** Select to remove the entitlement from the current certification and create a new one with the selected entitlement. This action removes the selected entitlement(s) from the current certification, creates a new certification with the selected entitlement(s), and assigns the person you specify as the primary reviewer for that new certification.
   - **Abstain:** Select if the entitlement is not appropriate and you do not know who should be responsible for verifying the entitlement's assigned accounts. This action on the entitlement records on each account assigns to the entitlement your decision to abstain, that is, to leave each assignment as it is. If you know who should be responsible, then you can reassign the entitlement instead.

   After you have taken a verification action on each entitlement, you must make certification decisions on each user account assigned to the entitlements you have claimed. You do not need to make any further certification decisions on an entitlement that you have revoked or reassigned or abstained. Normally, this means that you will open each entitlement and then review its user accounts, as described in Reviewing the Entitlement Assignments. However, you may also choose to delegate one or more entitlements to another person, which allows that person to make certification decisions on the user accounts assigned to that entitlement. The following actions are available from the Actions menu:

   - **Open:** Select this action to review the details of each entitlement and to make certification decisions on the user accounts assigned to the entitlement. See Reviewing the Entitlement Assignments.
   - **Delegate:** Select this action to allow another person to make decisions on the access privileges of each selected entitlement. This action will create a new delegated-review task that contains the selected entitlement(s) and will assign

the task to the person you specify as delegate. Responsibility still remains with you, the primary reviewer.

- **Un-delegate:** This action applies only to delegated entitlements. This action removes each selected entitlement from the delegated-review task and returns decision-making rights to you, the primary reviewer.

The Actions menu offers two additional convenience actions that are useful after you have made some certification decisions on the details of an entitlement. These actions affect the decisions on multiple details, that is, accesses of each selected entitlement:

- **Complete:** Sets any missing decisions on account assignments to Certify.
- **Reset:** Clears all decisions made on the entitlement including decisions on the entitlement's access.

10.2.4.2 Reviewing the Entitlement Assignments

Use the details view of the certification to review an entitlement's user accounts. The details view can be accessed by selecting an entitlement in the summary view and clicking **Open** from the Actions menu, or by clicking the entitlement name.

After your selections are made, you can use the Actions menu to select the appropriate action. The Actions menu contains the following options:

- **Certify:** You approve each selected assignment.
- **Revoke:** You disapprove each selected assignment. This decision indicates that the entitlement no longer needs the privilege and the assignment should be removed. When you select this option, a dialog box might be displayed that asks for comments. Type a note in the Comments pop-up, and click **OK**.
- **Certify Conditionally:** You approve each selected assignment, but only temporarily. This action also requires you to specify an end date on which your approval expires.
- **Abstain:** You take no position on each selected assignment. This records your decision to leave the assignment as it is.
- **Reset:** Use this to clear any decision you have made on the selected assignment.

For each action, optional comments can be added. By default, every decision other than to certify, such as Revoke, Certify Conditionally, and Abstain, allow optional comments.

An additional **Approve** option is available for two-phased user certification. Selecting this option copies the decision from Phase 1 to Phase 2. See Understanding Multi-Phased Review in User Certification for information about two-phased review.

10.2.4.3 Finishing the Entitlement Certification

The final step in the certification cycle is the sign-off action. Signing off can only be done when every access privilege has a decision assigned to it. When this state is reached, Oracle Identity Manager automatically prompts you to sign-off on all the decisions taken. If you choose not to sign-off at that time, then you can manually invoke the sign-off dialog box later assuming that all access privileges are still completed. The process for signing off is the same whether automatically prompted by the system or manually activated.

To manually sign-off:

1. From the Actions menu, select **Sign-off**. The Sign-off dialog box is displayed asking to complete the certification.

2. To complete the certification, Select **Yes**, and enter a password in the Password Required field. The password option is configurable and set in the certification definition. If disabled, the password field is not displayed in the Sign-off dialog box.

   Alternatively, to complete the certification later, select **No**.

3. Click **OK**.

Upon successful sign-off, the tab displaying the certification is closed automatically and a confirmation message is displayed.

10.3 Claiming and Releasing Group Certifier Assignments

Group or certifier assignments must be claimed by a user to take actions on it and released by the user for other users in the group to view the actions taken.

You can have a predefined role with potential certifiers as members. Each time a certification is created with certifier as the role, each member of the role can take action on the certification by claiming the task. The member who claims the task first is the primary reviewer for that certification. Rest of the members will not be able to view or work on the same certification. Similarly, the member can release the certification task back to the group if the user has claimed it before.

This section contains the following topics:

- Claiming Group Certifier Assignments
- Releasing Group Certifier Assignments

10.3.1 Claiming Group Certifier Assignments

Group certifier review tasks can be claimed by clicking the Claim Task button.

To claim a group certifier review task as the user member of a role that has been selected as the primary reviewer of the certification task:

1. Search and open the group certifier review task, as described in Searching and Viewing Certifications.

   If a role has been selected as the reviewer of the certification task in the Reviewers page of the Certification Definition wizard, as described in Creating Certification Definitions, then all members of the role can see the certification task in the Inbox, and a **Claim Task** button is displayed at the top right corner of Page 1 of the certification review task. This button is displayed only if the certification task is not already claimed by another member of the group.

2. Click the **Claim Task** button.

   When the task is claimed by a user member of the role, the task is not displayed in the Inbox of the other members of the role. The user who claimed the task can take action on the task.

10.3.2 Releasing Group Certifier Assignments

Group certifier assignments can be released by clicking the Release Task button.

To release a group certifier review task that you have claimed:

1. Search and open the group certifier review task, as described in Searching and Viewing Certifications.

For a certification review task for which a role has been selected as the primary reviewer, as described in Creating Certification Definitions, and if you have claimed the task as a member of the role, then a **Release Task** button is displayed at the top right corner of Page 1 of the review task.

2. Click the **Release Task** button.

   The task is release back to the role. Other members of the role can view the task, and any one of them can take action on it by claiming it.

When a task is released back to the group/role, all actions on the task taken by a member are can be viewed by other members in the Action History tab of the certification details.

11
Managing Pending Violations

The Oracle Identity Manager allows you to view the policy violations assigned to you and take action on them.
This chapter describes how to manage the pending violations assigned to you. It contains the following sections:

- Viewing Policy Violations
- Searching Pending Violations
- Completing Policy Violations
- Reassigning or Delegating Policy Violations

11.1 Viewing Policy Violations

You can view the policy violations assigned to you from the Inbox or the Pending Violations page of Oracle Identity Self Service.

You can navigate and view the policy violations assigned to you in any one of the following ways:

1. In Oracle Identity Self Service, click the **Self Service** tab. Click the icon in the **Pending Violations** tile.

   > **Note:**
   >
   > - When policy violation tasks are generated, the notification icon in the Pending Violations tile displays the number of pending violations.
   > - For certification and identity audit tasks, use the Certifications and Pending Violations tiles respectively. If you are using the Inbox Generic view, then do not use the Actions menu because the actions are not supported for certification and identity audit.

2. In Oracle Identity Self Service, click the down arrow at the top, and select **Inbox**. Under Views, click the **Pending Violations** view.

11.2 Searching Pending Violations

You can search for policy violations if you are aware of the policy violation name that is system-generated.

To search for pending violations:

1. Login to Oracle Identity Self Service.
2. Click the **Self Service** tab.

3. Click the icon in the **Pending Violations** box. The Pending Violations page is displayed.

   Alternatively, you can open the Inbox and click the Pending Violations view, as described in Viewing Policy Violations.

4. In the Search field, enter a search criterion, such as the policy violation name.
5. Click the Search icon. The pending violations that match the search criteria are displayed in a tabular format.

11.3 Completing Policy Violations

You can take corrective action on the policy violations assigned to you based on the cause of the violation and request for remediation.

To request for remediation for a policy violation assigned to you:

1. Navigate to the Pending Violation page or Inbox, as described in Viewing Policy Violations.
2. Click the policy violation to open the Violation details page. This page consists of the following tabs:
   - **Details:** This tab has the following sections:
     - **Violation Details:** Displays the details of the policy violation, such as the policy attributes, status, detection count, and the details of the user for which the violation is generated.
     - **Access Details:** Displays the cause of the violation, the rules within the policy that have been violated, the status and attributes of the violation, and comments, if any. In addition, the Attributes column displays details of the cause of the violation.

       You can place your mouse pointer on the information icon in the Rules Violated column to display a popup with details of the violated rule, such as rule name, description, and rule condition.
   - **Action History:** This tab displays all actions taken by the remediator of the policy till the current state.
3. For each item in the Access Details section of the Details tab, you can perform the following actions:
   - **Close as Fixed:** This action is to indicate that the cause has been fixed manually, either because it has been taken care of outside the system or the remediator has manually taken action to ensure that this access no longer exists for the user.

     To close the policy violation cause by accepting the violation risk:

     a. Select **Close as Fixed**. Alternatively, click **Close** on the toolbar, and then select **Close as Fixed**. The Provide Comments dialog box is displayed.

     b. Enter a comment, and click **Submit**.
   - **Close as Risk Accepted:** This action is to indicate that the access is required by the user for a particular time period, and the user can have the access until that date.

     To close the policy violation cause by accepting the violation risk:

a. From the Actions menu, select **Close as Risk Accepted**. Alternatively, click **Close** on the toolbar, and then select **Close as Risk Accepted**. The Provide Comments dialog box is displayed.

b. In the Expiration Date field, specify a date after which the violation will be re-opened if it still exists.

   The default value of the Expiration Date field is 30 days. It can be increased to more than 30 by setting the value of the `Maximum Risk Acceptance period for Policy Violation Causes` field. For information about setting the value of this field, see Setting Identity Audit Options.

c. In the Comments field, enter a comment, and click **Submit**.

- **Request for Remediation:** This action is to indicate that you want to revoke the access of the user because it is not required by the user, in order to mitigate the violation.

> **Note:**
>
> This action is not available for any user attribute that is causing violations, for example user title.

To request for remediation of the policy violation cause:

a. From the Actions menu, select **Request for Remediation**. Alternatively, click **Remediate** on the toolbar. The Provide Comments dialog box is displayed.

b. Enter a comment, and click **Submit**.

4. After you have taken actions on some or all or the access details, click **Complete** on the top-right corner of the screen.

   Based on the actions taken and the conditions of the rules, the policy violation will either be closed (if there are no more violations) or re-opened (if some of the actions were left open or the risk accepted date has passed and the user still has the access) during subsequent identity audit scans.

11.4 Reassigning or Delegating Policy Violations

You can reassign or delegate a policy violation task to other user/users. The ownership of the task is transferred to the user (assignee), and the task is removed from your view.

To reassign or delegate policy violations to other users:

1. Navigate to the Pending Violation page or Inbox, as described in Viewing Policy Violations.
2. Search and select the policy violation that you want to reassign or delegate.
3. From the Actions menu, select **Reassign**. The Reassign Task dialog box is displayed.
4. Select any one of the following options:
   - **Reassign (transfer task to another user or group):** Select this option if you want to move the pending violation task to other users or roles that you specify.

- **Delegate (allow specified user to act on my behalf):** Select this option if you want to allow the specified user to take action on the pending violation task on behalf of the logged-in user.

5. Search for the users (assignees) by specifying a search criterion in the search field.
6. Select the checkbox for each user that you want to select.

   You can click **Select All** to select all the users in the search result, or you can click **Select None** to reset your selection.
7. Click **OK**. The pending violation task is reassigned/delegated to the selected users. The task is no longer displayed in the task view of the logged-in user.

Part III
Working with Compliance

Audit and compliance features in the Identity Self Service are identity certification and identity audit.

This part describes the audit and compliance features of Identity Self Service.

It contains the following chapters:

- Using Identity Certification
- Managing Identity Certification
- Managing Identity Audit

12

Using Identity Certification

Identity certification concepts include certification types, reviewer types, certification name formats, and the Certification Dashboard. Using the Dashboard, you can search, filter, and view certifications from the Dashboard, complete user certifications in offline mode, and generate certification reports.
This chapter provides an overview of identity certification, describes the identity certification user interface, and includes information about how to complete identity certifications. It contains the following topics:

- Identity Certification Overview
- Certification UI
- Certification Name Formats
- Searching and Viewing Certifications
- Completing User Certifications in Offline Mode
- Generating Certification Reports

12.1 Identity Certification Overview

Understand identity certification and certification types, the various types of reviewers, and the certification types that can be accessed by each reviewer.

This section describes what, why, and how identity certifications are conducted. It also discusses who is typically involved in the identity certification process.

- What Is Identity Certification?
- Who Is Involved in Completing Identity Certifications?

12.1.1 What Is Identity Certification?

Identity certification is the process of reviewing user entitlements and access-privileges within an enterprise to ensure that users have not acquired entitlements that they are not authorized to have. It also involves either approving (certifying) or rejecting (revoking) each access-privilege. Identity certification can be for the user, role, organization, and entitlement entities.

Certifications can be scheduled to run on a regular basis to meet compliance requirements. Managers use the identity certification feature to review their employees' entitlements to access applications and data. Based on changes reported by the identity certification module, managers can authorize or revoke employee access as needed.

You can create four types of certifications. Each type of certification addresses a particular use-case—a specific type of review that enterprises commonly perform. Each type of reviewer reviews a different subset of access-related data from a specific point of view.

Table 12-1 lists the four types of identity certification that are possible in Oracle Identity Manager.

Table 12-1 The Four Types of Identity Certification

Identity Certification Type	Description
User Certification	Allows managers to certify employee access to roles, accounts, and entitlements. Typically, each manager in an organization reviews the access-privileges of the people who report directly to that manager. Each reviewer in a certification of this type is focused on his or her direct-reports, but is expected to review all of the access-privileges for each direct report. User certification optimizes review from the perspective of the line-of-business (LOB) manager, who must review all access-privileges for each user who reports to the LOB manager. User certification also supports a two-phased review, in which user access rights can be reviewed by managers first, and subsequently by any of the other IT owners, such as role owner, application instance owner, or entitlement owner, all within a single certification campaign.
Role Certification	Allows role owners to certify role content and/or role members. This certification is used in organizations that have implemented role-based access control (RBAC). Typically, the owner of a role is the person responsible for reviewing its definition (that is, the set of access-privileges that it conveys) as well as its membership (the set of users to whom the role has been assigned). Each reviewer in a certification of this type is focused on a particular enterprise role. Role certification optimizes review from the perspective of the role authorizer or role administrator, who must review the definition and the membership of each role that are owned by the role authorizer or role administrator.
Application Instance Certification	This certification allows the person who is responsible for a particular system or application to review the set of users who have accounts on that system or application. The reviewer can drill down and view the details of the access-privileges of each account. Each reviewer in a certification of this type is focused on one specific system or application. Application instance certification optimizes review from the perspective of the Application Instance Authorizer or Application Instance Administrator, who must review the membership (accounts) and the set of privileges (entitlement-assignments) for each application that are owned by the Application Instance Authorizer or Application Instance Administrator.
Entitlement Certification	Allows entitlement owners to certify user accounts that have a particular privilege. This certification is used if a specific person is responsible for a particular entitlement (that is, an Attribute Value or a group membership that confers a specific access-privilege). The entitlement owner can review the set of user accounts that have that particular entitlement. Each reviewer in a certification of this type is focused on one specific privilege within one specific resource. Entitlement certification optimizes review from the perspective of the Entitlement Authorizer or Entitlement Administrator, who must review the definition and the membership (entitlement-assignments) for each privilege (entitlement-definition) that are owned by the Entitlement Authorizer or Entitlement Administrator.

A scheduled job generates certifications based on a specified certification definition. Oracle Identity Manager applies the selection criteria within the certification definition to select the privilege assignments (and/or privilege definitions) that will be reviewed and by whom. Oracle Identity Manager generates a separate certification for each primary reviewer. Oracle Identity Manager also generates a review task for each primary reviewer. Oracle Identity Manager creates a new review task whenever a primary reviewer delegates or reassigns line-items to another reviewer. As each reviewer acts on the review task assigned to that reviewer, this updates the overall certification. Overall progress for each certification is visible from the Dashboard.

12.1.2 Who Is Involved in Completing Identity Certifications?

Identity certification allows personnel in an organization to review and certify user entitlement data, role content data, application instance data, and entitlement data.

This section provides descriptions of the types of users that are typically involved in the identity certification process, as well as the certifications that each user type can authorize or revoke. In Oracle Identity Manager, personnel who participate in the identity certification process are called *reviewers*.

Table 12-2 lists the reviewers involved in identity certification.

Table 12-2 Identity Certification Reviewers

Reviewer Name	Description	Certification Types That Can Be Accessed
Certifier	A generic term that signifies a person who is responsible for reviewing and completing any kind of certification.	• User certification • Role certification • Application instance certification • Entitlement certification
User manager	A manager with direct reports. Users report to a user manager.	• User entitlement
Business reviewer	A user within an enterprise who reviews the access-privileges of other users from a business-oriented perspective. Typically, this is a Line-Of-Business (LOB) manager who is responsible for the access-privileges of users who report to him/her. **Note:** LOB is a category of industry or business function. For example, an LOB manager is oriented to a business function within an enterprise, such as Sales.	• User certification • Role certification • Application instance certification • Entitlement certification

Table 12-2 (Cont.) Identity Certification Reviewers

Reviewer Name	Description	Certification Types That Can Be Accessed
Primary Reviewer	The person who is primarily responsible for making certification decisions on a particular set of line-items. The primary reviewer can reassign a line-item to another user, in which case that user becomes the new primary reviewer for that line-item, and the original primary reviewer never sees that line-item again. The primary reviewer can also delegate any of his line-items to another person, in which case that user becomes the delegated reviewer for that line-item, but the primary reviewer still retains responsibility for that line-item. **Note:** For information about line-item, see Line of Business and Line Item.	• User certification • Role certification • Application instance certification • Entitlement certification
Technical Reviewer	A user within an enterprise who reviews the access-privileges of others from a technically-oriented perspective. Typically, this is an IT expert or an application-owner who is responsible for access-privileges being specified correctly, or for limiting access within the enterprise to a specific access-privilege.	• User certification
Delegated Reviewer	A person who is assigned to help with the certification work. The delegated reviewer is secondarily responsible for making certification-decisions on a particular set of line-items, but the primary reviewer remains ultimately responsible. Any decision made by the delegated reviewer eventually returns to the primary reviewer, who can override that decision.	• User certification • Role certification • Application instance certification • Entitlement certification
Final Reviewer	The person who has the final say over the certification-decisions. The final reviewer can review and override the certification decisions of other reviewers. Final Review is performed only after a two-phased review (and only when an administrator has configured the certification-definition to enable this). The primary reviewer from the first phase can then make a final review of the certification actions made by all the reviewers in the first two phases.	• User Certification

12.2 Certification UI

You can view and work with certification objects by using the Pending Certifications page and the Certification Dashboard in the Identity Self Service.

You can view and work with certification objects by using the following in Oracle Identity Self Service:

- **Pending Certifications page:** The Pending Certifications page lists all the tasks assigned to the logged-in user in a single screen. It enables the logged-in user to filter task views into user preferences, such as assigned tasks, completed tasks, and tasks for which information has been requested. The user can select a task to open it in a new tab and then perform necessary actions on the task. This allows the user to work on multiple tasks at a time by opening them in different tabs.

  To access the Pending Certifications page, login to Oracle Identity Self Service, and in the Self Service tab, click the **Certification** box.

  > **See Also:**
  >
  > Managing Certification Review Tasks for detailed information about the Pending Certifications page and the operations you can perform by using the Pending Certifications page

- **Dashboard:** The Identity Certification Dashboard provides an overview of in-progress and completed certifications in the system. The certifications displayed in the dashboard depends on your role. A user with either the Certification Administrator or Certification Viewer admin role can see all certifications in the system. A non-administrative user, for example, a manager, can see any certification for which that user is assigned as a primary reviewer. A primary reviewer or user with the Certification Viewer admin role can view the certification information. A user assigned the Certification Administrator admin role can view any certification, and take basic actions on in-progress certifications. The primary reviewer cannot take actions on the certifications in the Dashboard.

  To access the Dashboard, login to Oracle Identity Self Service, click the Compliance tab, click the Identity Certification box, and select **Dashboard**.

12.3 Certification Name Formats

The certification task names are displayed is different formats depending on the review phase and reviewer.

Table 12-3 lists the certification task names in various review phases.

> **See Also:**
>
> - "Certification Task" for information about certification tasks
> - Understanding Multi-Phased Review in User Certification for information about the review phases in multi-phased review for user certification

Table 12-3 Certification Name Formats

Review Phase	Name Format	Example
Phase 1 (P1)	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]	Q1 Access 2012[Robert Klein]
Phase 1 Reassign	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Reassigned[*NEW_PRIMARY_REVIEWER*]	Q1 Access 2012[Robert Klein]Reassigned[Jane Doe]
Phase 1 Delegate	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Delegated[*P1_DELEGATED_REVIEWER*]	Q1 Access 2012[Robert Klein]Delegated[Jane Doe]
Phase 1 Verification	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Verification	Q1 Access 2012[Robert Klein]Verification
Phase 2 (P2)	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Roles[*P2_TECHNICAL_REVIEWER*]	Q1 Access 2012[Robert Klein]Roles[Terence Hill]
Phase 2 (P2)	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Application Instances[*P2_TECHNICAL_REVIEWER*]	Q1 Access 2012[Robert Klein]Application Instances[Martha Smith]
Phase 2 (P2)	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Entitlements[*P2_TECHNICAL_REVIEWER*]	Q1 Access 2012[Robert Klein]Entitlements[Hattori Hanzo]
Phase 2 Reassign	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Roles[*P2_TECHNICAL_REVIEWER*]Reassigned[*NEW_P2_TECHNICAL_REVIEWER*]	Q1 Access 2012[Robert Klein]Roles[Terrence Hill]Reassigned[Jane Doe]
Phase 2 Reassign	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Application Instances[*P2_TECHNICAL_REVIEWER*]Reassigned[*NEW_P2_TECHNICAL_REVIEWER*]	Q1 Access 2012[Robert Klein]Application Instances[Martha Smith]Reassigned[Jane Doe]
Phase 2 Reassign	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Entitlements[*P2_TECHNICAL_REVIEWER*]Reassigned[*NEW_P2_TECHNICAL_REVIEWER*]	Q1 Access 2012[Robert Klein]Entitlements[Hattori Hanzo]Reassigned[Jane Doe]
Phase 2 Delegate	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Roles[*P2_TECHNICAL_REVIEWER*]Delegated[*NEW_P2_TECHNICAL_REVIEWER*]	Q1 Access 2012[Robert Klein]Roles[Terrence Hill]Delegated[Jane Doe]
Phase 2 Delegate	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Application Instances[*P2_TECHNICAL_REVIEWER*]Delegated[*NEW_P2_TECHNICAL_REVIEWER*]	Q1 Access 2012[Robert Klein]Application Instances[Martha Smith]Delegated[Jane Doe]
Phase 2 Delegate	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Entitlements[*P2_TECHNICAL_REVIEWER*]Delegated[*NEW_P2_TECHNICAL_REVIEWER*]	Q1 Access 2012[Robert Klein]Entitlements[Hattori Hanzo]Delegated[Jane Doe]
Phase 2 Verification	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Roles[*P2_TECHNICAL_REVIEWER*]Verification	Q1 Access 2012[Robert Klein]Roles[Terence Hill]Verification

Table 12-3 (Cont.) Certification Name Formats

Review Phase	Name Format	Example
Phase 2 Verification	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Application Instances[*P2_TECHNICAL_REVIEWER*]Verification	Q1 Access 2012[Robert Klein]Application Instances[Martha Smith]Verification
Phase 2 Verification	*CERT_DEFINITION*[*P1_PRIMARY_REVIEWER*]Entitlements[*P2_TECHNICAL_REVIEWER*]Verification	Q1 Access 2012[Robert Klein]Entitlements[Hattori Hanzo]Verification
Final review	CERT_DEFINITION[P1_PRIMARY_REVIEWER]Final Review	Q1 Access 2012[Robert Klein]Final Review

12.4 Searching and Viewing Certifications

You can search, sort, and view certifications, and access pre-upgrade certifications by using the Dashboard.

This section describes how to search and filter certifications in the Certification Dashboard, and how to view the details of certifications. It contains the following topics:

- Searching Certifications in the Dashboard
- Sorting Certification Search Results
- Viewing Certifications From the Dashboard
- Accessing Pre-Upgrade Certifications in the Dashboard

12.4.1 Searching Certifications in the Dashboard

The Dashboard enables you to perform basic search and advanced search for certifications.

This section contains the following topics:

- Performing Basic Search for Certification
- Performing Advanced Search for Certification

12.4.1.1 Performing Basic Search for Certification

To perform a basic search for certifications:

1. Login to Oracle Identity Self Service.
2. Click the **Compliance** tab.
3. Click the **Identity Certification** box, and select **Dashboard**. The Dashboard page is displayed.
4. From the Search list, select any one of the following, and enter a search criterion in the box adjacent to the list:
   - **Certification Name:** To search the certifications by certification name.
   - **Organization Name:** To search the certifications by the organization name selected for the certification.

- **Type:** To search the certifications by the certification type.
- **Create Date:** To search the certifications by certification creation date.

5. Click the search icon. The certifications that match your search criteria are displayed in the search results table.

> **Tip:**
>
> To sort the data in the search results table, place the mouse pointer on a column name. Up and down arrows are displayed on the column names. Click the up arrow to sort in ascending order. Click the down arrow to sort in descending order.

12.4.1.2 Performing Advanced Search for Certification

To perform an advanced search for certifications:

1. Login to Oracle Identity Self Service.
2. Click the **Compliance** tab.
3. Click the **Identity Certification** box, and select **Dashboard**. The Dashboard is displayed with a list of certifications in a table. The table consists of columns, such as Name, Percent Complete, and Organization.

   You can personalize the table to display or hide certification attributes that are displayed as columns in the table. You can also change the order in which the columns are displayed in the table.
4. To show or hide columns and change the order of the columns, follow the instructions in Personalizing the Search Result.
5. In the Search Certifications section, click **Advanced**.
6. Select any one of the following options:
   - **All:** To specify that the search result must match all the specified search criteria.
   - **Any:** To specify that the search result must match any one of the specified search criteria.
7. Enter values in the certification search attributes.
8. Click the Search icon. The certifications that match your search criteria are displayed in the table.

> **Tip:**
>
> To sort the data in the search results table, place the mouse pointer on a column name. Up and down arrows are displayed on the column names. Click the up arrow to sort in ascending order. Click the down arrow to sort in descending order.

9. (Optional) You can refine the certification search result. To do so, from the Show list, select any one of the following to filter the list of certifications displayed in the Dashboard:

- **New and In Progress:** Lists the certifications that are assigned to you and the certifications in progress.
- **New:** Lists only the new certifications that are assigned to you.
- **In Progress:** Lists only the certifications in progress.
- **Completed:** Lists the certifications that are in the completed state.
- **Expired:** Lists the certifications whose end date has passed.
- **All:** Lists all types of certifications including new, in progress, and expired certifications.

12.4.2 Sorting Certification Search Results

Certification search results can be sorted in ascending and descending orders.

You can sort the certification search results in ascending and descending orders. To do so, see Sorting Data in Search Results.

In this release of Oracle Identity Manager, you can sort and list the certifications by the percentage completion of the certifications. In the certification search results in the Dashboard, you can place the mouse pointer on the Percent Complete column to display the up and down arrow keys. Clicking the up arrow key sorts the certifications in ascending order of percentage completion, and clicking the down arrow key sorts the certifications in descending order or percentage completion.

12.4.3 Viewing Certifications From the Dashboard

Only the primary reviewers, who have been selected as certifiers during the certification creation process, can see the certifications in the Dashboard.

You can open and view certification details from the Pending Certifications page or the Dashboard. However, all users cannot see the certifications in the Dashboard. Only the primary reviewers, who have been selected as certifiers during the certification creation process, can see the certifications in the Dashboard. All other users can access certification tasks only from the Pending Certifications page. For example, the delegated reviewers cannot see the particular certification in the Dashboard, but can see a certification task in the Pending Certifications page. Similarly, phase 2 reviewers for user certification cannot see any certification in the Dashboard. For non-admin users, the Dashboard provides a read-only access to certifications for the purpose of monitoring.

> **See Also:**
>
> Understanding Multi-Phased Review in User Certification for information about the phases of reviews in multi-phased review for user certification.

To open and view certification details from the Dashboard:

1. In the **Compliance** tab of Oracle Identity Self Service, click the **Identity Certification** box, and select **Dashboard**. The Dashboard page is displayed.
2. Select the certification for which you want to display the details. A summary of the selected certification is displayed in the Detail Information section, which consists of the following tabs:

- **Certification Details:** Displays the certification attributes such as name, percentage complete, and number of roles, accounts, entitlements, or users for the selected certification. A link to the requests page is also displayed if closed-loop remediation has been activated for the certification.

  For information about closed-loop remediation and remediation tracking, see About Closed-Loop Remediation and Remediation Tracking. For information about the Track Requests page, see Tracking a Request.

- **Certification Tasks:** Displays a list of certification tasks that are part of the selected certification. This is a read-only view, and the user cannot take any action on the certification tasks.

- **Reports:** Enables you to generate certification reports. This tab is displayed only if the report option is configured in Oracle Identity Manager. See Generating Certification Reports for details.

3. From the Actions menu, select **Open**. Alternatively, you can click **Open** on the toolbar, or click the certification name to open it. The details of the selected certification are displayed in the certification details page.

   In both Pending Certifications page and the Dashboard, you can also click the certification name to open the details of the certification.

   The certification details is displayed in a tabular format. You can hide, unhide, and re-order columns in the table. For details, see Personalizing the Search Result. In addition, you can use the saved search feature in this page to search for the details. For information about creating and using saved search, see Using Saved Search.

> **Note:**
>
> If a user is deleted from Oracle Identity Governance through Deleted User Account Clean Up job, then you might see empty details or an x character in the user information field in the User Details page.

12.4.4 Accessing Pre-Upgrade Certifications in the Dashboard

Run the Certification Maintenance Job scheduled job to populate pre-upgrade certifications in the Dashboard.

If you have upgraded Oracle Identity Manager from an earlier release, then no certifications are available in the Certification Dashboard. To populate the Dashboard with the pre-upgrade certifications, run the Certification Maintenance Job scheduled job. For information about this scheduled job and its parameters, see Predefined Scheduled Tasks in *Administering Oracle Identity Governance*.

Time required to complete the execution of the Certification Maintenance Job scheduled job depends on the number of pre-upgrade certifications and their content. If the upgraded system has large number of pre-upgrade certification, then this job execution might take a long time to finish. This job processes few certifications (depending on Batch Size parameter) at a time.

If the job execution is interrupted before the job is finished, then the Certification Dashboard will only display the certifications that have been successfully processed by the job. This job is re-entrant and can be run multiple times if required. It will process each pre-upgrade certification once and populate the relevant data. Certification

Maintenance Job execution does not impact other features or functionality. Run this job if any pre-upgrade certifications are found to be missing from the dashboard.

12.5 Completing User Certifications in Offline Mode

The Dashboard allows working on user certifications in offline mode. Offline certification is not allowed for other entities, such as role, organization, and entitlement.

This section describes user certification in offline mode. It contains the following topics:

- Understanding User Certifications in Offline Mode
- Working on a User Certification in Offline Mode

12.5.1 Understanding User Certifications in Offline Mode

The availability of offline user certification is controlled by enabling or disabling the **Enable Interactive Excel** option in the Certification Configuration page in the Identity Self Service.

You have the option to download user certification data to your local computer and work on it in an offline mode by using Microsoft Excel without having an active session with Oracle Identity Manager. After making decisions on the certifications, you can connect to Oracle Identity Manager and upload your decisions. The availability of this option can be controlled by enabling or disabling the **Enable Interactive Excel** option in the Certification Configuration page in Oracle Identity Self Service. For information about this option, see Configuring Certification Options.

Note:

- The option to download user certification data to your local computer and work on it in an offline mode is available for user certifications only. This functionality is not available for role, application instance, and entitlement certifications.
- For this functionality to work, you must have Microsoft Excel 2016 or Excel for Microsoft Office 365. To configure Microsoft Excel for this functionality:
  1. Ensure that the prerequisites described in "Configuring Excel to work with ADF Desktop Integration" in the *Desktop Integration Developer's Guide for Oracle Application Development* are met.
  2. Perform the one-time configuration, as described in "How to Install Runtime Edition of ADF Desktop Integration" in the *Desktop Integration Developer's Guide for Oracle Application Development*.
- For applications running in an environment using Oracle Access Manager, ensure that the URL for the ADF Desktop Integration Remote servlet is configured as a protected resource for Oracle Access Manager. The ADF Desktop Integration Remote servlet is:

  `http://IDM_HOST.IDM_DOMAIN.com:OIG_PORT/identity/adfdiRemoteServlet`

When the **Enable Interactive Excel** option is enabled, the **Download to Editable Excel** menu option is available in the Actions menu in the certification detail and certification summary pages of the user certification.

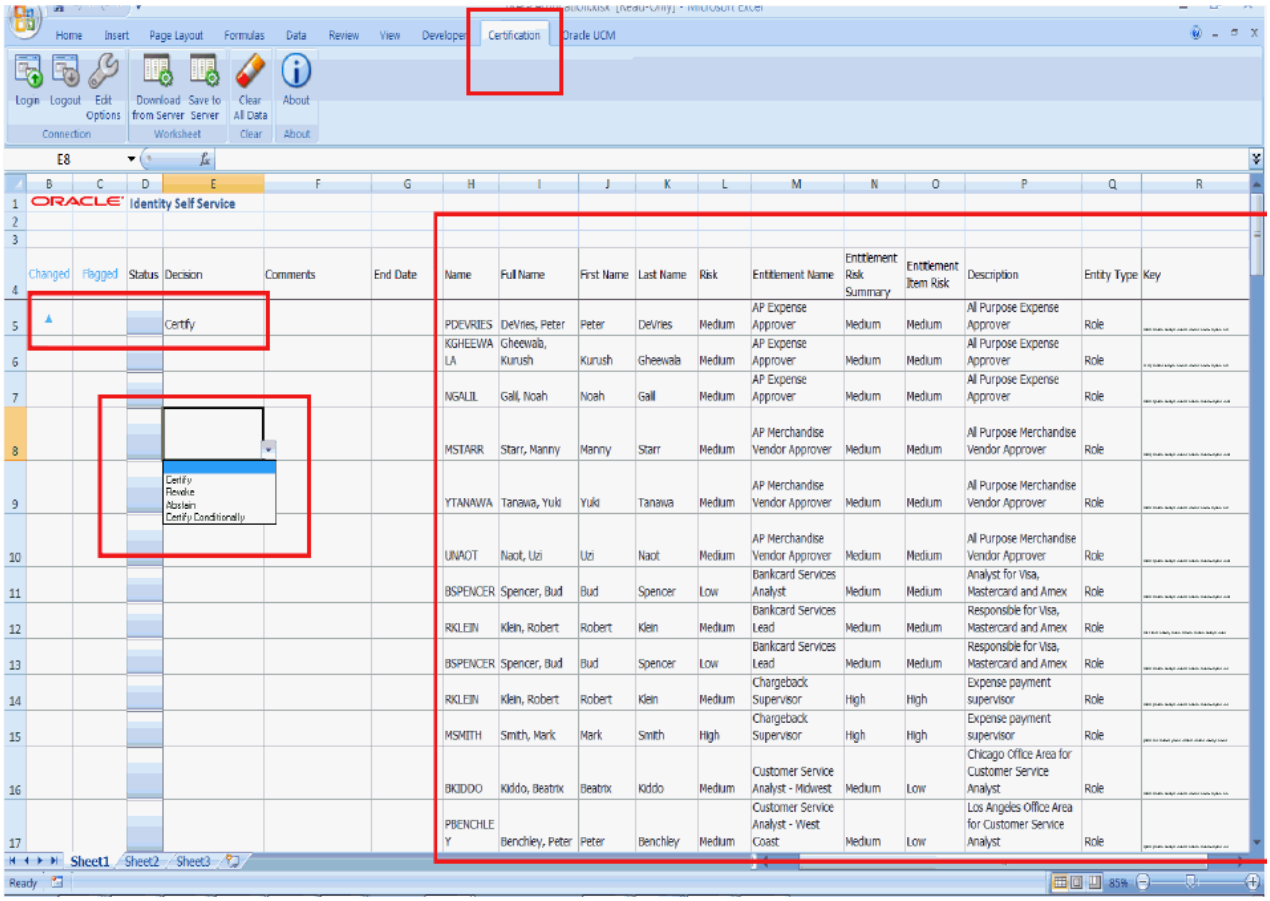
12.5.2 Working on a User Certification in Offline Mode

You have the option to download user certification data to your local computer and work on it in an offline mode by using Microsoft Excel without having an active session with Oracle Identity Manager. After making decisions on the certifications, you can connect to Oracle Identity Manager and upload your decisions.

To work on a user certification in offline mode:

1. Open a user certification from the Dashboard or Pending Certifications page.
2. From the Actions menu, select **Download to Editable Excel**. A message box is displayed with the options to open or save the file.
3. Select **Open with**.
4. Make sure that **Microsoft Office Excel** is selected instead of Microsoft Office Excel (Default). Microsoft Office Excel (Default) is the version of Excel for which the plugin for this functionality is not enabled.
5. Click **OK**. A message box is displayed asking whether you want to connect to the corresponding server where the application is running and from where the spreadsheet was downloaded.
6. Click **Yes**. The page to login to Oracle Identity Self Service is displayed. This provides an extra layer of security before you can download the data to work on.
7. Login to Oracle Identity Self Service by providing the credentials. The user certification data is downloaded into a spreadsheet.
8. Click the **Certification** tab. This displays the list of options available when you work on a record. Figure 12-1 shows the Certification tab.

Figure 12-1 The Certification Tab



9. Select the decisions from the drop-down for each user. When a decision is selected, the Changed column displays a flag that indicates the change. The area highlighted in grey color is a read-only area and no changes can be made there.

   Decisions other than Certify cannot be updated unless certain conditions are met, and as a result, the data upload will fail. To view these errors, double-click the error field under the status column. Then, you can perform the necessary action to fix it before trying to upload again. The actions can be:

   - Revoke: Comments are required.
   - Abstain: Comments are required.
   - Certify Conditionally: Comments and an end date are required.

   > **Note:**
   >
   > User-defined field (UDF) data for both user and catalog will show up in the spreadsheet as read-only columns.

10. When you finish selecting the decisions, you can upload the data back to the server by clicking the **Save to Server**. The user data is updated on the user certification screens.

> **Note:**
>
> When you upload the spreadsheet data, if the application instance and entitlement decisions are different, the decisions for entitlements maybe be over-ridden on the server side depending on which data gets uploaded to the server first. In other words, data downloaded in a particular order is uploaded in that particular order.
>
> For example, if you revoke an entitlement and certify the account as Certify Conditionally, the entitlement could also be certified as Certify Conditionally if the account is updated last in the server, after the entitlement has been updated.
>
> As a work around, you can download the Excel file again to verify the final value updated on the server.

If you try to download the spreadsheet for a certification that has already been completed, then a different version of the spreadsheet is downloaded, in which all the columns are marked as read-only and the **Save to Server** button is not available.

12.6 Generating Certification Reports

You can generate certification reports from the Dashboard or from the Pending Certifications page.

This section describes generating certification reports in the following topics:

- About Generating Certification
- Generating Certification Reports From the Dashboard
- Generating Exported Certification Reports From the Certification Pages

12.6.1 About Generating Certification

Oracle BI Publisher reports are used for identity certification. These reports select data from the certification tables of the Oracle Identity Manager database.

There are specific templates to control the format and content of reports. For example, many of the certification reports have a template that includes details from action history for each line-item and detail, and another template that does not.

There are a list of predefined or default certification reports in Oracle Identity Manager. For more information about the default certification reports, see "Certification Reports" in the *Administering Oracle Identity Governance*.

12.6.2 Generating Certification Reports From the Dashboard

Use the Reports tab of the Dashboard to generate certification reports in HTM or PDF formats.

To generate certification reports by using the Dashboard:

1. In Oracle Identity Self Service, click the **Compliance** tab. Click the **Identity Certification** box, and select **Dashboard**.

2. Search and select the certification for which you want to generate the report. The Detailed Information section is displayed for the selected certification.
3. Click the **Reports** tab.
4. Select Report Type as Complete Certification, Certified, Revoked, Abstained, or Certified Conditionally.
5. From the Report Format Output list, select the format in which you want to generate the report, such as HTML or PDF.
6. Select the **Display Action History** option to include in the report the action history or trail of actions taken by all reviewers on the certification. Deselecting this option does not show the action history in the certification report.
7. Click **Generate Report**. The certification information is exported to the selected option, such as HTML or PDF.

> **Tip:**
>
> On selecting Excel as the report format in step 5, an error message is displayed on opening the report. This is a security alert from Microsoft and can be ignored. However, if you want to avoid the message, then perform the following steps:
>
> a. Go to Windows registry.
> b. Search and navigate to the `HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Security` key.
> c. Set the following value:
>
> ```
> (DWORD)"ExtensionHardening" = 0
> ```

12.6.3 Generating Exported Certification Reports From the Certification Pages

Use the Pending Certifications page to export certification tasks to PDF or Excel.

To generate certification reports by using the Pending Certifications page:

1. In Oracle Identity Self Service, click the **Self Service** tab. Click the **Certifications** box. The Pending Certifications page is displayed.
2. Click an in-progress certification task name to open Page 1 of the certification task.
3. From the Actions menu, select Export to PDF or Excel.

   The exported certification tasks in PDF or Excel is equivalent to Complete Certification Report.

13

Managing Identity Certification

Managing identity certification involves understanding certification concepts, configuring and scheduling certification, managing certification definitions, managing event listeners, configuring certification reports, and troubleshooting certification.
This chapter describes the concepts related to identity certification and the configuration tasks required for identity certification. It contains the following topics:

- Certification Concepts
- Configuring Certifications
- Managing Certification Definitions
- Scheduling Certifications
- About How Risk Summaries are Calculated
- About Closed-Loop Remediation and Remediation Tracking
- Configuring Challenge Workflows
- About Event Listeners
- Configuring Event Listeners and Certification Event Trigger Jobs
- Configuring Certification Reports
- Understanding Multi-Phased Review in User Certification
- About Certification Oversight
- Troubleshooting Identity Certification

13.1 Certification Concepts

Key concepts related to identity certification are lines of business and line items, certification tasks, objects, definitions, and jobs, closed-loop remediation, remediation tracking, event listeners, certification authorization, and custom reviewer for user certification.

The concepts related to identity certification are described in the following sections.

- Line of Business and Line Item
- Certification Task
- Certification Object
- Certification Definition
- Certification Jobs
- Closed-Loop Remediation
- Remediation Tracking
- Event Listener
- Certification Authorization

- Custom Reviewer for User Certifications

13.1.1 Line of Business and Line Item

Line of Business (LOB) is a category of industry or business function. A line item is a row of data that appears on Page One of a certification.

LOB is a category of industry or business function. For example, an LOB manager is oriented to a business function within an enterprise, such as Sales.

A line item is a row of data that appears on Page One of a certification. Each line item collects or groups together according to the type of certification the set of privilege-assignments related to a particular identity or privilege. A reviewer can open any line-item to see its line item details. For example, within phase one of a user certification, each line item represents a user. Opening the user details displays the access-privileges of that user.

13.1.2 Certification Task

Certification task consists of a set of work to be done within a certification process.

Each set of line-items that is assigned to a particular reviewer initiates a Service-Oriented Architecture (SOA) task that contains that particular set of line items and that is routed to SOA Inbox of that particular reviewer. The SOA component also notifies the reviewer that a certification task has been assigned to the reviewer.

13.1.3 Certification Object

Certification object consists of a certification ID and a set of line items.

Certification object is a generated certification that is assigned to a particular certifier or primary reviewer. Each certification object consists of:

- A unique certification ID
- A set of line-items, each of which contains a set of details

13.1.4 Certification Definition

Certification definition is a named set of parameters that is used as input to a certification job to generate certification objects.

A certification definition specifies the following:

- The type of certification to generate, such as user certification, role certification, application instance certification, or entitlement certification
- Selection criteria that describe which line items, for example users, to select
- Content-restriction criteria that describe which details to select for each line item
- Other parameters that control the generation of certification objects or the behavior of review tasks

13.1.5 Certification Jobs

Certification jobs are used to create certifications as requested or as scheduled.

A certification job is a background execution-task that generates certification objects based on a specified certification definition. Certification jobs can be:

- Scheduled to run at regular intervals, such as weekly, monthly, or quarterly, as required
- Run immediately from the Scheduler section of Oracle Identity System Administration
- Triggered from an event-listener action

You can create and run certification-generation jobs to create certifications as requested or as scheduled. You can enable and run the risk-aggregation job to calculate the risk-values of entities, such as users, accounts, role-assignments, and entitlement-assignments.

13.1.6 Closed-Loop Remediation

Closed-loop remediation is used to revoke access privileges as an outcome of the certification process.

Closed-loop remediation is a feature that utilizes the provisioning system of Oracle Identity Manager to automatically revoke accounts, roles, and entitlements based on the results of the Oracle Identity Manager certification process.

13.1.7 Remediation Tracking

The access request catalog is used for remediation tracking.

You can use the request catalog to track the remediation status of revoked accounts, access within accounts, or roles. This records whether and when each revocation request is fulfilled.

13.1.8 Event Listener

Event listener is a service that responds to changes in users. Event listeners are supported for all certification types.

Each event listener for certification contains:

- The selection-criteria specified by an administrator
- The certification definition to use in response

13.1.9 Certification Authorization

Certification authorization is controlled by assigning or revoking the Certification Administrator and Certification Viewer administrative roles.

The following Oracle Identity Manager admin roles grant the assignee privileges required to administer the certification feature and monitor the progress of certification instances:

- **Certification Administrator:** The Certification Administrator admin role grants the assignee super-user privileges for the certification feature. In particular, this admin role grants access to the certification configuration and scheduler in the Oracle Identity Manager System Administration. This role also grants full access to certification where you can view or take action on any certifications.
- **Certification Viewer:** The Certification Viewer is a read-only role, allowing a compliance administrator to view new, in progress, and completed certifications.

13.1.10 Custom Reviewer for User Certifications

Custom reviewer for user certifications can be specified by defining certification rules in the CERT_CUSTOM_ACCESS_REVIEWERS table.

Oracle Identity Manager enables you to define your own custom reviewer for user certifications. This section contains the following topics:

- About Custom Access Reviewer
- Conditions for Using Custom Access Reviewer
- Sample CERT_CUSTOM_ACCESS_REVIEWERS Table
- Custom Access Reviewer Scenarios

13.1.10.1 About Custom Access Reviewer

You can define your own custom access reviewer for user certifications by specifying certification rules for specific user accounts, roles, entitlements, or application instances, or a combination of these entities, with a particular reviewer. In addition, you can group the certification rules and assign a map name to the certification rule to specify a reviewer for that map name.

These rules can be defined in the CERT_CUSTOM_ACCESS_REVIEWERS table in Oracle Identity Manager database.Table 13-1describes the columns of the CERT_CUSTOM_ACCESS_REVIEWERS table.

> **Note:**
>
> The CERT_CUSTOM_ACCESS_REVIEWERS table must be populated before running the intended certification jobs. The data in the table is to be maintained by Oracle Identity Manager administrators.

Table 13-1 CERT_CUSTOM_ACCESS_REVIEWERS Table Definition

Column	Data Type	Description
reviewer_login	varchar2(256)	OIM login ID for the reviewer user. This field can have the following special values: • <USER_MANAGER>: Specifies the default reviewer to be the user's manager for any user in the mapping • <ORGANIZATION_MANAGER>: Specifies the default reviewer to be the organization manager for any user in the mapping

Table 13-1 (Cont.) CERT_CUSTOM_ACCESS_REVIEWERS Table Definition

Column	Data Type	Description
user_login	varchar2(256)	OIM user login for the user whose access needs to be filtered. This field can have the following special value: <ANY>: Specifies special reviewer mapping to be applied for any user
access_type	number(2)	Access type has numeric value and the possible value is one of the following: 1 for User 2 for Role 3 for Account 4 for Entitlement 5 for Default Reviewer 6 for Alternate Reviewer
app_instance_name	varchar2(4000)	Name of the application instance.
account_name	varchar2(300)	Name of the specific account on the application instance.
entitlement_name	varchar2(4000)	Name of the entitlement.
role_name	varchar2(4000)	Name of the role.
map_name	varchar2(4000)	The map name that can be used to tag mappings and used in certification definitions.

13.1.10.2 Conditions for Using Custom Access Reviewer

Certain conditions must be met for using the custom access reviewer for user certifications.

The following conditions must be met for using the custom access reviewer for user certification feature:

- Reviewer table does not support any wildcards for any of the fields/columns.
- Reviewer table has mappings defined for each and every user to be included in certification.
- Application instance information is required for all account and entitlement mappings.
- Only one instance of default reviewer and alternate reviewer mapping is allowed per map name.

13.1.10.3 Sample CERT_CUSTOM_ACCESS_REVIEWERS Table

Table 13-2shows a sample CERT_CUSTOM_ACCESS_REVIEWERS table with custom reviewers defined for certification rules.

Table 13-2 Sample CERT_CUSTOM_ACCESS_REVIEWERS Table

Row #	REVIEWER_LOGIN	USER_LOGIN	ACCESS_TYPE	Application Instance Name	Account name	Entitlement Name	Map Name
1	ACERTUSER2	VCERTUSER2	3	VISDU1	VCERTUSER2SERVICE		2015 Review
2	ACERTUSER1	VCERTUSER3	4	VISDU1	VCERTUSER3	EntTestDB~CN=VISDU11,DC=abc,DC=com	2015 Review
3	ACERTUSER3	VCERTUSER2	4	VISDU1	VCERTUSER2	EntTestDB~CN=VISDU11,DC=abc,DC=com	2015 Review
4	VCERTUSER10	VCERTUSER2	1	NA	NA	NA	<GLOBAL>

The rows in the sample table represent the following certification rules:

- Row #1 has a mapping defined for the specific application instance VISDU1 owned by the user account VCERTUSER2SERVICE of user VCERTUSER2 with a particular reviewer ACERTUSER2.
- Row #2 has a mapping defined for the specific entitlement EntTestDB~CN=VISDU11,DC=abc,DC=com with an application instance VISDU1 owned by the user account VCERTUSER3 of user VCERTUSER3 with a particular reviewer ACERTUSER1.
- Row #3 has a mapping defined for the specific entitlement EntTestDB~CN=VISDU11,DC=abc,DC=com with an application instance VISDU1 owned by the user account VCERTUSER2 of user VCERTUSER2 with a particular reviewer ACERTUSER3.

13.1.10.4 Custom Access Reviewer Scenarios

The following is a list of supported custom access reviewer configuration scenarios.

Custom reviewer for specific user

Reviewer table has mapping defined for a specific user U1 with a particular reviewer R1.

This mapping is treated as whole access responsibility mapping. Reviewer R1 will review the entire access for user U1, and user U1 will be included in a certification for reviewer R1. Any access for user U1 will be excluded for which R1 is not a reviewer in reviewer table.

Custom reviewer for account owned by specific user

Reviewer table has mapping defined for a specific user account U1A1 of user U1 with a particular reviewer R2.

This mapping is treated as limited access responsibility mapping. Reviewer R2 will only review account U1A1 for user U1, and user U1 will be included in a certification

for reviewer R2. Oracle Identity Manager will include U1A1 account along with all the entitlements that are part of U1A1 for reviewer R2.

Custom reviewer for entitlement owned by specific user account

Reviewer table has mapping defined for a specific entitlement U1A1E1 owned by a specific account U1A1 with a particular reviewer R3.

This mapping is treated as limited access responsibility mapping. Reviewer R3 will only review entitlement U1A1E1 for user U1, and user U1 will be included in a certification for reviewer R3. Oracle Identity Manager will include account U1A1 and only entitlement U1A1E1 for reviewer R3.

Custom reviewer for entitlement within an application instance (without any account name)

Reviewer table has mapping defined for a specific entitlement E3 with an application instance name APP2 with a particular reviewer R5. Account name is not defined for this mapping.

This mapping is treated as limited responsibility mapping. Reviewer R5 will review all the entitlements with name E3 from all the user accounts available in the application instance APP2. Certifications will be generated for all users who have entitlement E3 in the application instance APP2 and assigned to reviewer R5. Oracle Identity Manager will include accounts with only entitlement E3 in the certification for reviewer R5.

Custom reviewer for role owned by specific user

Reviewer table has mapping defined for a specific user role U1R1 of user U1 with a particular reviewer R4.

This mapping is treated as limited access responsibility mapping. Reviewer R4 will only review role U1R1 for user U1, and user U1 will be included in a certification for reviewer R4. Oracle Identity Manager will include only role U1R1 for reviewer R4.

Custom reviewers for different access types specified in the reviewer table

Certifications are created for each of the reviewers defined in the table. Each reviewer will only see the access elements for which mappings are defined. Each reviewer will have only one certification created in one certification job run.

Custom reviewer table with tag/map name defined in reviewer table

The reviewer table is scoped per the tag/map name defined in the certification definition. If the certification definition does not have a tag/map name specified, then the reviewer table is scoped for the <GLOBAL> tag/map name.

Default reviewer mapping for a specific map name

Reviewer table has mapping defined in default reviewer row as <Default Reviewer> - <USER_MANAGER> - <ANY> for map name MAP1.

This mapping is treated as default user reviewer mapping and will default the reviewer for any user to be the user's manager. All user's managers are included as reviewers. Oracle Identity Manager will NOT include a user in the certification for user's manager if there is another User access type mapping defined in the reviewer table. This mapping will NOT affect other mappings in any way.

Reviewer table with user-level mappings as subset of base selection in certification definition

Base selection consists of users U1, U2, U3 and reviewer table with mapping for U1::U1A1-> R1 (account type), U2::U2A1E1-> R2 (entitlement type). Default reviewer mapping is <USER_MANAGER>-<ANY>. Managers are available as U1->M1, U2->M2, and U3->M3.

Certifications are generated for all users U1, U2 and U3. Each user's manager will review each user's access. Reviewer M3 will review all access for U3. Reviewer M2 will review all access for U2 except entitlement U2A1E1. Reviewer R2 will review only U2A1E1 for user U2. Reviewer M1 will review all access for U1 except account U1A1. Reviewer R1 will review only U1A1 for user U1.

Reviewer table with default reviewer mapping and overriding user-level mapping

Reviewer table has default reviewer mapping as <Default Reviewer> - <USER_MANAGER> - <ANY> for <GLOBAL> map name. Reviewer table also has user type mapping for U1 -> R1. User U1 has manager M1 defined in system. One certification is generated for reviewer R1, and no certification is generated for manager M1.

Reviewer table with default reviewer mapping and alternate reviewer mapping

Reviewer table has default reviewer mapping as <Default Reviewer> -< USER_MANAGER> - <ANY> for <GLOBAL> map name. Reviewer table has alternate reviewer mapping as <Alternate Reviewer> - <AR1> - <ANY> for <GLOBAL> map name. User U1 has manager M1 defined in system. Reviewer M1 is an inactive user in system.

Any certification will not be generated for manager M1 because the user is inactive. One certification will be generated for reviewer AR1 with user U1.

13.2 Configuring Certifications

After certain prerequisites for certification configuration are met, you can set the certification configuration properties in the Certification Configuration page of the Identity Self Service.

This section describes how to configuring certifications in the following topics:

- Prerequisites for Configuring Certifications
- Configuring Certification Options

13.2.1 Prerequisites for Configuring Certifications

Prerequisites for configuring certifications include marking a catalog item as certifiable, setting the certifier, user manager, organization certifier, user attributes for certification snapshot, and risk levels for individual entities, tagging attributes, and configuring the availability of identity certification, reminders, notifications, escalations, and expiry for certifications.

Configuring certifications has the following prerequisite steps:

- Marking a Catalog Item as Certifiable

- Setting the Certifier in the Request Catalog
- Setting User Manager and Organization Certifier
- Setting User Attributes for Certification Snapshot
- Setting Risk Levels for Individual Entities
- Tagging Attributes
- Configuring the Availability of Identity Certification
- Configuring Reminders, Notifications, Escalations, and Expiry for Certifications (Optional)

> **Note:**
>
> Some of the preconfiguration steps require you to use the request catalog. For detailed information about the request catalog, see the following sections:
>
> - Requesting Access
> - Managing the Access Request Catalog in the *Administering Oracle Identity Governance*

13.2.1.1 Marking a Catalog Item as Certifiable

A requestable entity, such as role assignment, role membership, application instance, or entitlement, is available for certification only after it is marked as certifiable in the request catalog. Any entity that is not marked as certifiable does not appear in the certification.

By default, all items in the catalog are marked as certifiable. You can deselect the **Certifiable** option if you do not want a certification task to be generated for that entity.

To mark an entity as certifiable:

1. Login to Oracle Identity Self Service.
2. Navigate to the request catalog page.
3. Search and select the application instance or entitlement that you want to set as certifiable.

   To modify the Certifiable option for roles, open the role details page, and then set the Certifiable option in the Catalog Attributes section.
4. Click the info (i) icon to open the Detailed Information tab for the selected catalog item.
5. Under Detailed Information, select the **Certifiable** option.
6. Click **Apply**.

13.2.1.2 Setting the Certifier in the Request Catalog

When you set a user as the certifier for an entity and select some of the options for selecting reviewers, such as Role Certifier or Application Instance Certifier, the user is automatically set as the certifier or primary reviewer for certifying that entity. For example, if user John Doe is selected as the certifier for the Vision Developers role, then John Doe is automatically set as the primary reviewer for certifying the Vision Developers role depending on the selection in the Reviewers screen of creating certifications. In this example, after the user is set as the

certifier for the Vision Developers role and you are creating a Role Certification, selecting the Role Certifier option will pick up this field.

> **Note:**
>
> Setting the certifier in the request catalog is required if you want to use some of the options for selecting reviewers in the certification creation screen, such as Role Certifier or Application Instance Certifier.

To set the certifier in the catalog:

1. In Oracle Identity Self Service, navigate to the Catalog page.
2. Search and select the role, application instance, or entitlement for which you want to set the certifier.
3. For the Certifier User field, click the lookup icon. From the lookup, search and select a user that you want to set as certifier for the selected entity.
4. Click **Apply**.

13.2.1.3 Setting User Manager and Organization Certifier

The user manager and organization certifier are available for selection as the primary reviewer in the certification creation process.

User manager is the user selected in the Manager field in the Attributes tab of the User Details page in Oracle Identity Self Service. If Jane Doe is specified as the manager for Terence Hill, then while creating a user certification definition, as described in Creating Certification Definitions, when you select user manager as the primary reviewer, Jane Doe is automatically set as the primary reviewer for the certification tasks generated for Terence Hill.

The organization certifier is the user selected in the Certifier User Login field in the Attributes tab of the Organization Details page in Oracle Identity Self Service. If Robert Klein is specified as the organization certifier for the Vision North organization, then while creating the certification definition, when you select organization certifier as the primary reviewer, Robert Klein is automatically set as the primary reviewers for the certifications tasks generated for Vision North.

> **Note:**
>
> - Setting the user manager or organization certifier is required if you want to use the Reviewer option of User Manager or Organization Certifier. Otherwise, this is not required.
> - Role organization certifier does not support the Hierarchy aware option. For the organization certifier, the role must be available in the organization. In other words, the specific organization must be specified for the role. Otherwise, certification will not be generated. Make sure that the role and organization are linked and organization has the certifier user assigned.

13.2.1.4 Setting User Attributes for Certification Snapshot

Certification snapshots the following user attributes in Oracle Identity Manager:

```
UserManagerConstants.AttributeName.USER_KEY.getId());
UserManagerConstants.AttributeName.USER_ORGANIZATION.getId());
UserManagerConstants.AttributeName.USER_LOGIN.getId());
UserManagerConstants.AttributeName.MANAGER_KEY.getId());
UserManagerConstants.AttributeName.STATUS.getId());
UserManagerConstants.AttributeName.EMAIL.getId());
UserManagerConstants.AttributeName.FIRSTNAME.getId());
UserManagerConstants.AttributeName.LASTNAME.getId());
UserManagerConstants.AttributeName.DISPLAYNAME.getId());
UserManagerConstants.AttributeName.EMPTYPE.getId());
UserManagerConstants.AttributeName.PHONE_NUMBER.getId());
UserManagerConstants.AttributeName.EMPLOYEE_NUMBER.getId());
UserManagerConstants.AttributeName.USER_UPDATE.getId());
UserManagerConstants.AttributeName.USER_CREATEBY.getId());
UserManagerConstants.AttributeName.USER_UPDATEBY.getId());
UserManagerConstants.AttributeName.USER_CREATED.getId());
UserManagerConstants.AttributeName.DEPARTMENT_NUMBER.getId());
UserManagerConstants.AttributeName.LOCALITY_NAME.getId());
UserManagerConstants.AttributeName.POSTAL_CODE.getId());
UserManagerConstants.AttributeName.STATE.getId());
UserManagerConstants.AttributeName.STREET.getId());
UserManagerConstants.AttributeName.USER_COUNTRY.getId());
UserManagerConstants.AttributeName.LOCALE.getId());
UserManagerConstants.AttributeName.TITLE.getId());
UserManagerConstants.AttributeName.GENERATION_QUALIFIER.getId())
UserManagerConstants.AttributeName.COMMONNAME.getId());
UserManagerConstants.AttributeName.HIRE_DATE.getId());
UserManagerConstants.AttributeName.ACCOUNT_STATUS.getId());
UserManagerConstants.AttributeName.MIDDLENAME.getId());
```

All other user attributes can be added to the certification snapshots if the attributes are marked as certifiable . These attributes are stored along with the other user defined attributes. Note that marking an attribute as certifiable can impact performance, and therefore, it is recommended to mark the attributes as certifiable only if required.

13.2.1.5 Setting Risk Levels for Individual Entities

To set the risk levels for individual entities:

> **Note:**
>
> See About How Risk Summaries are Calculated for information about the impact of setting risk levels and how Oracle Identity Manager processes risk levels to arrive at risk summaries.

1. In Oracle Identity Self Service, navigate to the Catalog page.
2. Search and select the role, application instance, or entitlement for which you want to set the risk level.

3. Under Detailed Information, from the Risk Level list, select **High Risk**, **Medium Risk**, or **Low Risk**.
4. Click **Apply**.

After setting the risk level for an individual entity, you must run the Risk Aggregation scheduled job so that the new risk level is correctly picked up when new certifications are created. Note that existing certification objects do not reflect the new risk level.

13.2.1.6 Tagging Attributes

Accounts, IT resources, and entitlements must be tagged for certification in the Design Console. Without tagging, certification for the entities are not generated.

You can check if the accounts, IT resources, and entitlements are already tagged by following the navigation in the Design Console as described in this section. If the entities are already tagged, then you can skip this section. Otherwise, configure account and IT resource tagging by performing the steps in this section.

> **Note:**
>
> For the certification creation to work, the value of the following properties must be set to `true`, as described in the procedure in this section.
>
> - `Entitlement`
> - `ITResource`
> - `AccountName`

To configure account and IT resource tagging:

1. Login to the Design Console.
2. Under Development Tools, click **Form Designer**.
3. Click the search icon on the top. The Form Designer Table is displayed with a list of all available forms.
4. Open the child process form, and click **Create New Version**.
5. Click the **Properties** tab.
6. Locate only one entitlement field per form, click **Add Property**, and add the `Entitlement = true` property setting.

   If there are multiple entitlement child forms, then add one `Entitlement = true` property setting per entitlement form.
7. Save the child form, and click **Make Version Active**.

> **Note:**
>
> If there are multiple child forms, update all of them by repeating steps 4 through 7 before going to the next step.

8. Select the parent forms for each connector that is installed. The parent form has the User ID fields to store the account name in the target system, for example, UD_ADUSER and UD_EBS_USER.
9. Select a form. A new Form Designer tab opens.
10. Click **Create New Version**. In the popup, enter a name, for example, `v2`. Click the save icon. Close the popup.
11. In the Current version list, make sure that the newly created version v2 is selected.
12. Click the **Properties** tab.
13. Locate the field that uniquely identifies the account in the target system, such as UserID, UserName, and AccountName, which are typical fields in the default connectors. Click **Add Property**, and add the `AccountName = true` property setting.
14. Locate the IT resource field. For most connectors, this is identified by the text ITResourceLookupField as a property for the target system. Click **Add Property**, and add the `ITResource = true` property setting.
15. Save the parent form. Click **Make Version Active**.
16. Repeat steps 3 through 11 for each IT resource.

13.2.1.7 Configuring the Availability of Identity Certification

The certification feature is part of Compliance in Oracle Identity Manager. Therefore, the certification feature is available when the value of the `Identity Auditor Feature Set Availability` system property is set to `TRUE`. When the value of this property is `TRUE`, role lifecycle management, Segregation of Duties (SoD), and identity certification are enabled.

If you change the value of this property, then you must restart Oracle Identity Manager server.

> **Note:**
>
> For information about system properties and setting the values of system properties, see “Managing System Properties” in the *Administering Oracle Identity Governance*.

13.2.1.8 Configuring Reminders, Notifications, Escalations, and Expiry for Certifications (Optional)

If email notifications is configured in SOA, as described in "Configuring SOA Email Notification" in *Administering Oracle Identity Governance*, then email notifications are sent by default in the following scenarios:

- When a task is assigned to a user
- When a task is completed

By default, two reminders are sent one day after and two days after the certification has been created. There is no escalation or expiry set for the certifications by default.

To change the default configuration for certification:

1. Login to Oracle SOA Composer with Admin credentials, such as weblogic, by navigating to the following URL:

   http://*HOST_NAME*:*PORT_NUMBER*/soa/composer

2. Click **Open**, and select **Open Tasks**. The Select a Task to open dialog box is displayed.
3. Select CertificationProcess_rev1.0, and click **Open**. The CertificationTask : Event Driven Configuration page is displayed.
4. In the Notification Settings section, perform the following:
   a. The assignees of the task are selected as recipients of the notification for Assign and Complete tasks. To change the default setting, you can select the task status in the Task Status column, and select the notification recipient in the Recipient column. You can click the pencil icon for each task to edit the default notification message, and click **OK**.
   b. In the drop-down below, change the default setting for reminders.
5. In the Expiry and Escalation Policy section, you can change the default value for escalation and expiry.
6. Click **OK**.
7. Click **Save**, and then click **Commit**.

13.2.2 Configuring Certification Options

You can set default options in Oracle Identity Self Service that are used during certification creation based on the type of certification. These options can be changed during the certification creation process for each certification definition.

To configure certification options:

1. Login to Oracle Identity Self Service.
2. Click the **Compliance** tab.
3. Click the **Identity Certification** box, and select **Certification Configuration**. The Certification Configuration page is displayed.
4. Set the configuration properties, as listed in Table 13-3.

> **Note:**
>
> All the options listed in Table 13-3 set the default configuration that is picked up during certification creation based on the type of certification. These can be changed during the certification creation process for each certification definition.

Table 13-3 Configuration Properties

Property	Description
Password required on sign-off	Select to require users to sign off in order to complete a certification.

Table 13-3 (Cont.) Configuration Properties

Property	Description
Allow comments on certify operations	Select to allow the user to add a comment if a certify action is selected.
Mandatory comments on certify operations	Select to make comments mandatory for certify action. This element is only available if **Allow comments on certify operations** is selected.
Pre-populate comments on certify operations	Select to pre-populate comments for certify operations. This element is only available if the option **Allow comments on certify operations** is selected. For more information, see About Pre-populate Certification Comments. **Note:**When this property is selected, the comments will populate for all the line items during campaign run itself, so the run might take some additional time to complete.
Allow comments on all non-certify operations	Select to allow the user to add a comment if a revoke action is selected.
Mandatory comments on all non-certify operations	Select to make comments mandatory for all non-certify action. This element is only available if the option **Allow comments on all non-certify operations** is selected.
Verify employee access	Select to control if you want to view Page 1 in the user certification view. By default, this option is selected. This option is used in user certification.
Prevent self certification	Select to prevent reviewers from being able to certify their own access. Enabling this option allows the certification creator to assign the certification to an alternate reviewer. When the Prevent self certification option is enabled, the **User Manager** option is selected by default, which means that the assignee is the user's manager. To select any other user, select **Select User**. Click the Search icon to search and select an alternate reviewer. Here, the following reviewers and not available for selection for particular certification types because they are not supported for those certification types: • For user certification: Search for a Role • For role certification: Role - Certifier User, Role - Certifier Role • For application instance certification: Application Instance (Certifier Role), Search for a Role • For entitlement certification: Entitlement - Certifier Role
User and Account Selections	Select any one of the following: • Include only active users and active accounts • Include any user with active accounts • Include all users and all accounts
Allow advanced delegation	Select to enable the ability to delegate a line item to others. This option is not selected by default. When delegation is enabled, there is a verification stage, in which the certification is routed to the primary reviewer with all the decisions of the delegates as well as the primary reviewer's own decisions for final sign off.

Table 13-3 (Cont.) Configuration Properties

Property	Description
Allow multi-phased review	Select to enable collaborative certification, for which in phase 1 the business review is completed and that is followed by a phase 2 for the technical review followed by an optional final review, which is completed by the business reviewer again. This is used in user certification only.
Allow reassignment	Select to enable the ability to reassign the line items in page 1 of certifications to other users. When line items are reassigned, the items are removed from the certification task and are no longer visible within the review cycle for the original certification object. A new certification object is created containing the reassigned line items. The new assignee is the primary reviewer for the new certification object.
Allow auto-claim	Select to mark all the items in page 1 as claimed by default. By default, auto claim is enabled. If you deselect this option, then users have to manually claim each item before they can view the item details.
Perform closed loop remediation	Select to specify closed-loop remediation when certification is completed.
Disable Account for Revoke action	Select this option to disable an account instead of revoke on closed loop remediation when certification is completed. By default, this option is not selected, users have to manually select this option for disabling accounts in the OIG setup.
Enable Interactive Excel	Select to enable ADF DeskTop Integration (DI) for user certification that provides the user the option to download certification data to Microsoft Excel worksheet and work on it in offline mode. For information about working on certifications in an offline mode, see Completing User Certifications in Offline Mode
Enable Certification Reports	Select to enable the creation of certification reports and display the Reports tab in the Detailed Information section of the Certification Dashboard.
Composite Name	Select the SOA composite for the certification workflow. The default composite is default/CertificationProcess. You can select another version of the composite to enable certification oversight in the certification workflow. To do so, select the CertificationOverseerProcess composite. This composite specifies that the reviewer's manager is the overseer for the certification process.

> **Note:**
>
> From Oct 21 Bundle Patch and later releases, the Certification UI is enhanced. For more details about the new UI features, see Certification UI New Features.

5. Click **Save**.

13.3 Managing Certification Definitions

Managing certification definitions include creating, modifying, and deleting the definitions for user, role, application instance, and entitlement certification.

This section describes about certification definitions in the following topics:

- Creating Certification Definitions
- Modifying Certification Definitions
- Deleting Certification Definitions

13.3.1 Creating Certification Definitions

You can create user, role, application instance, and entitlement certification definitions by launching the New Certification wizard from the Certification Definitions page.

Creating certification definitions is described in the following sections:

- Creating a User Certification Definition
- Creating a Role Certification Definition
- Creating an Application Instance Certification Definition
- Creating an Entitlement Certification Definition

13.3.1.1 Creating a User Certification Definition

To create a user certification definition:

1. Log in to Oracle Identity Self Service.
2. Click the **Compliance** tab.
3. Click the **Identity Certification** box, and select **Definitions**. The Certification Definitions page is displayed.
4. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The General Details page of the New Certification wizard is displayed.
5. Enter values as follows:
   - **Certification Name:** Enter a name for the certification.
   - **Type:** Select **User** to create a user certification.
   - **Description:** Optionally enter a description for the new user certification.
6. Click **Next**. The Base Selection page of the New Certification wizard is displayed.
7. Select a user-selection strategy in the Base Selection section, as follows:
   - **Users from All Organizations:** Selects users from all organizations in Oracle Identity Manager.
   - **Only Users from Selected Organizations:** Allows you to manually select specific organizations. You can select the organizations by clicking Add. To remove a selected organization, click Remove.

> **Note:**
>
> When completing a certification, a certifier cannot see the organization name or any other details about the organization unless that person is also the organization administrator for that organization. If the certifier is not the organization administrator, only the users in the organization are displayed.

- **All users:** Selects all the users in Oracle Identity Manager.
- **Users criteria:** Selects all the users that meet the given search condition. You can filter the criteria based on various user attributes and user-defined fields (UDFs). To do so, select the **Apply further criteria** option in the Selection Constraints section, and then select the attributes and UDFs.
- **Selected users:** Allows you to select specific users from a list of users in the system. To select users, click **Add**. To remove selected users, click **Remove**.

> **Note:**
>
> You can save the search and use it for specifying user criteria while creating another user certification definition. The saved search is not mapped to a specific certification. To use the user criteria saved search for another user certification definition:
>
> a. During certification creation, after selecting the **Users criteria** option and specifying the search condition, you must click **Update and Preview Results**. This associates the selected criteria with the definition.
>
> b. If you want to save this search criteria as a template, then click **Save**. You are prompted to enter a name for the template that you are saving. You can then save this template and reuse it.
> The saved template is not specific to a certification. While creating another certification, this template is displayed by default. If you create another new template, then that template is displayed. In other words, the latest template is displayed for all criteria screens associated with a type of certification.
>
> c. If you do not want to use the generated template, then change the value in the Saved Search list to something else that you want to use.

8. Select any one of the following options to specify constraints to the base selection:
   - Users with Any Level of Risk
   - Only Users with High Risk Summaries
   - Only Users with High Risk Roles
   - Only Users with High Risk Application Instances
   - Only User with High Risk Entitlements
9. Click **Next**. The Content Selection page is displayed.
10. In the Content Selection section, select the following:

a. Select the **Include Users with no accounts** option to include users who have no access within the certification.

b. In the Roles section, select any one of the following options to limit the role assignments to certify for each user:

> **Note:**
>
> The list of roles per user can be restricted to the selected option. For example, if you select selected roles or selected criteria and add one role, then that role only will show up in the certification if it is marked as certifiable in the catalog even if the user has other roles.

- **All Roles:** Select to show all roles.
- **Only High Risk Roles:** Select to show only the roles with high risk level, and exclude the roles with medium and low risk levels.
- **Selected Roles Only:** Select this option to manually select the roles.
- **Selected Roles Criteria:** Select to show the roles based on a filter criteria.
- **Roles Outside Rules:** Select to exclude the roles that have been granted to users through membership rules.
- **High Risk Roles Outside Rules:** Select to exclude the roles with high risk level that have been granted to users through membership rules, and include only the high risk roles that have not been granted through membership rules.

> **Note:**
>
> The **Roles Outside Rules** and **High Risk Roles Outside Rules** options are available after you apply Oracle Identity Governance Bundle Patch 12.2.1.4.210428.

- **None:** Select to exclude all roles from the certification.

c. In the Application Instances section, select the following:

i. Selct the **Include accounts with no certification attributes** option to include the accounts in the selected application instances even if there are no certifiable entitlements (access) within the target system. If you deselect this option, then accounts in the target system that do not have any entitlements do not appear in the certification.

ii. Select any one of the following options to limit the application instance assignments to certify for each user:

> **Note:**
>
> Similar to roles, you can restrict the application instances you want to see within the certification.

- **All Application Instances:** Select to include all application instances.
- **Only High Risk Application Instances:** Select to include only the application instances with high risk level, and exclude the application instances with medium and low risk levels.
- **Selected Application Instances Only:** Select this option to manually select the application instances.
- **Selected Application Instances Criteria:** Select to show the application instances based on a filter criteria.

d. Select any one of the following options to limit the entitlements that you can see within the certification:

- **All Entitlements:** Select to show all entitlements.
- **Entitlements Outside Roles:** Select to show only the entitlements that are not provisioned by roles/access policies, and exclude access granted via roles/access policies.
- **Accounts with High-Risk Entitlements:** Select to show account information for high-risk entitlements only.
- **Only High-Risk Entitlements:** Select to show only the high-risk entitlements, and exclude the entitlements with medium and low risk levels.
- **Only High-Risk Entitlements Outside Roles:** Select to show only high-risk entitlements, exclude the entitlements with medium and low risk levels, and exclude all entitlements (with any risk) granted via roles/access policies.
- **Selected Entitlements Criteria:** Select to show entitlements based on a filter criteria.

11. Click **Next**. The Configuration page is displayed.
12. Select the options, as described in Table 13-3, and click **Next**. The Reviewers page is displayed.

    If you want to enable multi-phased review with advanced delegation, then select the **Allow advanced delegation** and **Allow multi-phased review** options.

    If you want to enable certification oversight in the certification workflow, then click the search icon, search for the available composites, select the **CertificationOverseerProcess** composite, and click **Add**.

> **Note:**
>
> In the Configuration page, if you select the **Prevent self certification** option and choose an alternate reviewer, then the **Search for a Role** reviewer option is not available for selection.

13. From the Reviewer list, select a primary reviewer. The primary reviewer can be user manager, organization certifier, any other user that you select, or any other role that you select. The primary reviewer can be any one of the following:

- **User Manager:** Selects the user's manager as the primary reviewer.
- **Organization Certifier:** Select's the organization certifier as the primary reviewer.

- **Search for a User:** Selects any user as the primary reviewer that you search and specify by clicking the lookup icon.
- **Search for a Role:** Selects all user members of any role that you select by clicking the lookup icon as the primary reviewer. Any user member of the role will be able to claim the task in order to review and certify. When the task is claimed by a user, other users in the role will not be able to view the task in the Inbox.

  Group certifier assignments are not supported with CertificationProcess composite. If you want to specify a role as the primary reviewer, then you must select the CertificationOverseerProcess composite in the Configurations page of the wizard.
- **Custom Access Reviewer:** A custom reviewer that you specify as the primary reviewer by populating the CERT_CUSTOM_ACCESS_REVIEWERS table in Oracle Identity Manager database. For detailed information about defining a custom access reviewer, see Custom Reviewer for User Certifications.

For multi-phased review, perform the following:

a. In the Phase 1 section, select any one of the following to select the Phase 1 reviewer:
   - **User Manager:** Selects the user's manager as the Phase 1 reviewer.
   - **Organization Certifier:** Selects the organization certifier as the Phase 1 reviewer.
   - **Search for a User:** Selects any user as the Phase 1 reviewer that you search and specify by clicking the lookup icon.
   - **Search for a Role:** Selects all user members of any role that you select by clicking the lookup icon as the Phase 1 reviewer. Any user member of the role will be able to claim the task in order to review and certify. When the task is claimed by a user, other users in the role will not be able to view the task in the Inbox.

     Group certifier assignments are not supported with CertificationProcess composite. If you want to select this option, then you must select the CertificationOverseerProcess composite in the Configurations page of the wizard.
   - **Custom Access Reviewer:** A custom reviewer that you specify as the Phase 1 reviewer by populating the CERT_CUSTOM_ACCESS_REVIEWERS table in Oracle Identity Manager database. For detailed information about defining a custom access reviewer, see Custom Reviewer for User Certifications.

b. In the Phase 2 (Optional) section, select the **Enable Phase 2 review process** option to specify that the privilege certifier will be the primary Phase 2 reviewer for each user privilege, such as role, account, and entitlement assignments. Then, select any one of the following as the Phase 2 reviewer:
   - **Certifier User:** Selects the catalog certifier user as the Phase 2 reviewer.
   - **Certifier Role:** Selects the catalog certifier role as the Phase 2 reviewer. If a catalog item does not have a certifier role, then the task goes to the certifier user. If entitlement certifier (both user and role) are not defined, then the task falls back to application instance (certifier user/role).

c. In the Final Review (Optional) section, select the **Enable Final Review process** option to enable a final review process by the Phase 1 reviewer for final validation and sign off.

14. Click **Next**. The Incremental page is displayed.

Incremental certification is not supported for group/role certification. Therefore, if you have selected the **Search for a Role** option in the Reviewers page, then the Incremental page is skipped and the Summary page is displayed.

15. Select **Enabled** for Generate Incremental Data. This setting enables certifiers to certify or revoke only changes or inclusions made to a certification. It eliminates the need to review the access of users who have been certified.

    When Incremental Certification is enabled, it takes the following parameters:

    - **Incremental Date Range** (required): This includes:
      - **Since Last Base** (default): When this option is selected, current access of the user is compared against the last certification of the same type, which was created without enabling incremental and all the incremental certifications since then, to the current date when the certification is created.
      - **Since Date:** When this option is selected, current access of the user is compared against all the certifications of the same type since the given date and when the certification is created.
    - **Show Previous Value** (optional): This includes:
      - **Disabled** (default): When this is deselected, then the values that have already appeared in the previous certifications based on the Incremental Date Range parameter are not included in the certification.
      - **Enabled:** When this is selected, all the current values that existed in previous certifications are displayed with the last decisions taken for those access.

16. Click **Next**. The Summary page is displayed with the details of the user certification.

17. Click **Create** to create the user certification. A message is displayed asking if you want to create a certification job based on the definition and run it now. You can edit the job name, and click **Yes** to run the certification job.

    Alternatively, click **No** to create a certification definition without creating and running the scheduled job. With this option, you must manually create a certification job later.

    The new user certification definition is displayed in the Certification Definition page.

> **Note:**
>
> For multi-phased review with advanced delegation:
>
> - The certification is not 100% complete till the Phase 2 reviewers or technical reviewers have completed all the reviews. The certification status displays the phase and percentage completion in each phase the certification is in during the two phased review. To view this status, click the In Progress certification in the Inbox or Dashboard.
> - The certification goes to the Phase 1 primary reviewer for final review. In Page 2, the Phase 1 primary reviewer can review the actions made by the users in the first and second phases (greyed out) as well as the system-generated default actions, which the Phase 1 primary reviewer can override.

13.3.1.2 Creating a Role Certification Definition

To create a role certification definition:

1. Log in to Oracle Identity Self Service.
2. Click the **Compliance** tab.
3. Click the **Identity Certification** box, and select **Definitions**. The Certification Definitions page is displayed.
4. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The General Details page of the New Certification wizard is displayed.
5. Enter values as follows:
   - **Name:** Enter a name for the certification.
   - **Type:** Select **Role** to create a role certification definition.
   - **Description:** Optionally enter a description for the new role certification definition.
6. Click **Next**. The Base Selection page of the New Certification wizard is displayed.
7. In the Base Selection section of the page, select a role selection strategy from the list, as shown:
   - **All Roles in All Organizations:** Selects all roles in all the organizations in Oracle Identity Manager.
   - **Roles from Selected Organizations:** Selects the roles from the organizations that you specify. Click Add to search and select an organization. To remove a selected organization, click Remove.

     > **Note:**
     >
     > When completing a certification, a certifier cannot see the organization name or any other details about the organization unless that person is also the organization administrator. If the certifier is not the organization administrator, only the users in the organization are displayed.

   - **All Roles:** Selects all roles in Oracle Identity Manager.

- **Role criteria:** Selects all of the roles that meet the given search condition. You can preview the results of this selection.

  > **Tip:**
  >
  > You can save the search and use it for specifying role criteria while creating another role certification definition. The saved search is not mapped to a specific certification. To use the role criteria saved search for another role certification definition:
  >
  > a. During certification creation, after selecting the **Role Criteria** option and specifying the search condition, you must click **Update and Preview Results**. This associates the selected criteria with the definition.
  >
  > b. If you want to save this search criteria as a template, then click **Save**. You are prompted to enter a name for the template that you are saving. You can then save this template and reuse it.
  >
  > c. The saved template is not specific to a certification. While creating another certification, this template is displayed by default. If you create another new template, then that template is displayed. In other words, the latest template is displayed for all criteria screens associated with a type of certification.
  >
  > d. If you do not want to use the generated template, then change the value in the Saved Search list to something else that you want to use.

- **Selected roles:** Allows you to manually select the roles.

8. Select any one of the following options to specify constraints:
   - Roles with Any Level of Risk
   - Only High Risk Roles
9. Click **Next**. The Content Selection page is displayed.
10. Select **Certify Policies** to specify the certification of policies. Select **Certify Members** to specify the certification of role members.
11. Click **Next**. The Configuration page is displayed.
12. Select the configuration options, as described in Table 13-3, and click **Next**. The Reviewers page is displayed.

    > **Note:**
    >
    > In the Configuration page, if you select the **Prevent self certification** option and choose an alternate reviewer, then the **Role - Certifier User** and **Role - Certifier Role** reviewer options are not available for selection.

13. From the Reviewer list, select a primary reviewer. The primary reviewer can be any one of the following:
    - **Role (Certifier User):** Selects the certifier user as the primary reviewer.

- **Role (Certifier Role):** Selects the certifier role as the primary reviewer.
- **Organization Certifier:** Selects the organization certifier as the primary reviewer.
- **Search for a User:** Selects any user as the primary reviewer that you search and specify by clicking the lookup icon.
- **Search for a Role:** Selects all user members of any role that you select by clicking the lookup icon as the primary reviewer. Any user member of the role will be able to claim the task in order to review and certify. When the task is claimed by a user, other users in the role will not be able to view the task in the Inbox.

  Group certifier assignments are not supported with CertificationProcess composite. If you want to specify a role as the primary reviewer, then you must select the CertificationOverseerProcess composite in the Configurations page of the wizard.

14. Click **Next**. The Incremental page is displayed.

    Incremental certification is not supported for group/role certification. Therefore, if you have selected the **Search for a Role** option in the Reviewers page, then the Incremental page is skipped and the Summary page is displayed.

15. Select **Enabled** for Generate Incremental Data. This setting enables certifiers to certify or revoke only changes or inclusions made to a certification. It eliminates the need to review the access of users who have been certified.

    When Incremental Certification is enabled, it takes the following parameters:

    - **Incremental Date Range** (required): This includes:
      - **Since Last Base** (default): When this option is selected, current access of the user is compared against the last certification of the same type, which was created without enabling incremental and all the incremental certifications since then, to the current date when the certification is created.
      - **Since Date:** When this option is selected, current access of the user is compared against all the certifications of the same type since the given date and when the certification is created.
    - **Show Previous Value** (optional): This includes:
      - **Disabled** (default): When this is deselected, then the values that have already appeared in the previous certifications based on the Incremental Date Range parameter are not included in the certification.
      - **Enabled:** When this is selected, all the current values that existed in previous certifications are displayed with the last decisions taken for those access.

16. Click **Next**. The Summary page is displayed with the details of the user certification.
17. Click **Create**. A message is displayed asking if you want to create a certification job based on the definition and run it now. You can edit the job name, and click **Yes** to run the certification job.

    Alternatively, click **No** to create a certification definition without creating and running the scheduled job. With this option, you must manually create a certification job later.

    The new role certification definition is displayed in the Certification Definition page.

13.3.1.3 Creating an Application Instance Certification Definition

To create an application instance certification definition:

1. Log in to Oracle Identity Self Service.

2. Click the **Compliance** tab.
3. Click the **Identity Certification** box, and select **Definition**. The Certification Definitions page is displayed.
4. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The General Details page of the New Certification wizard is displayed.
5. Enter values as follows:
   - **Name:** Enter a name for the certification.
   - **Type:** Select **Application Instance** to create an application instance certification definition.
   - **Description:** Optionally enter a description for the new application instance certification definition.
6. Click **Next**. The Base Selection page of the New Certification wizard is displayed.
7. In the Base Selection section of the page, select an application instance selection strategy from the list, as shown:
   - **All Application Instances:** Selects all application instances in Oracle Identity Manager.
   - **Selected application instances only:** Allows you to manually select the application instances. Click **Add** to search and select the application instances. To remove any selected application instance, click **Remove**.
8. Select any one of the following options to specify constraints:
   - Application Instances with Any Level of Risk
   - Only High Risk Application Instances
9. Click **Next**. The Content Selection page is displayed.
10. Select any one of the following:
    - **Accounts of Users from All Organizations:** Selects the accounts of users from all organizations in Oracle Identity Manager.
    - **Accounts of Users from Selected Organizations:** Allows you to manually select the organizations whose user accounts will be certified.
    - **Accounts of All Users:** Selects the accounts of all users in Oracle Identity Manager.
    - **Accounts of Selected Users:** Allows you to manually select the users whose accounts will be certified.
    - **Exclude Applications with no Accounts:** If this option is selected, then certification campaigns associated with this definition will not show the application instances which are not having any associated accounts.
      If this option is not selected, then certification campaign created against this definition will show the application instances which are not having any associated accounts with full completion status.
11. Click **Next**. The Configuration page is displayed.
12. Select the configuration options, as described in Table 13-3, and click **Next**. The Reviewers page is displayed.

> **Note:**
>
> In the Configuration page, if you select the **Prevent self certification** option and choose an alternate reviewer, then the **Application Instance (Certifier Role)** and **Search for a Role** reviewer options are not available for selection.

13. From the Reviewer list, select a primary reviewer. The primary reviewer can be application instance certifier, user manager, application instance certifier, organization certifier, or any other user that you select. The primary reviewer can be any one of the following:
    - **Application Instance (Certifier User):** Selects the application instance certifier user as the primary reviewer.
    - **Application Instance (Certifier Role):** Selects the application instance certifier role as the primary reviewer.
    - **User Manager:** Selects the user's manager as the primary reviewer.
    - **Organization Certifier:** Selects the organization certifier as the primary reviewer.
    - **Search for a User:** Selects any user as the primary reviewer that you search and specify by clicking the lookup icon.
    - **Search for a Role:** Selects all user members of any role that you select by clicking the lookup icon as the primary reviewer. Any user member of the role will be able to claim the task in order to review and certify. When the task is claimed by a user, other users in the role will not be able to view the task in the Inbox.

      Group certifier assignments are not supported with CertificationProcess composite. If you want to specify a role as the primary reviewer, then you must select the CertificationOverseerProcess composite in the Configurations page of the wizard.
14. Click **Next**. The Incremental page is displayed.

    Incremental certification is not supported for group/role certification. Therefore, if you have selected the **Search for a Role** option in the Reviewers page, then the Incremental page is skipped and the Summary page is displayed.
15. Select **Enabled** for Generate Incremental Data. This setting enables certifiers to certify or revoke only changes or inclusions made to a certification. It eliminates the need to review the access of users who have been certified.

    When Incremental Certification is enabled, it takes the following parameters:
    - **Incremental Date Range** (required): This includes:
      - **Since Last Base** (default): When this option is selected, current access of the user is compared against the last certification of the same type, which was created without enabling incremental and all the incremental certifications since then, to the current date when the certification is created.
      - **Since Date:** When this option is selected, current access of the user is compared against all the certifications of the same type since the given date and when the certification is created.
    - **Show Previous Value** (optional): This includes:
      - **Disabled** (default): When this is deselected, then the values that have already appeared in the previous certifications based on the Incremental Date Range parameter are not included in the certification.

- **Enabled:** When this is selected, all the current values that existed in previous certifications are displayed with the last decisions taken for those access.

16. Click **Next**. The Summary page is displayed with the details of the user certification.
17. Click **Create**. A message is displayed asking if you want to create a certification job based on the definition and run it now. You can edit the job name, and click **Yes** to run the certification job.

    Alternatively, click **No** to create a certification definition without creating and running the scheduled job. With this option, you must manually create a certification job later.

    The new application instance certification definition is displayed in the Certification Definition page.

13.3.1.4 Creating an Entitlement Certification Definition

To create an entitlement certification definition:

1. Log in to Oracle Identity Self Service.
2. Click the **Compliance** tab.
3. Click the **Identity Certification** box, and select **Definition**. The Certification Definitions page is displayed.
4. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The General Details page of the New Certification wizard is displayed.
5. Enter values as follows:
   - **Name:** Enter a name for the certification.
   - **Type:** Select **Entitlement** to create an entitlement certification definition.
   - **Description:** Optionally enter a description for the new entitlement certification definition.
6. Click **Next**. The Base Selection page of the New Certification wizard is displayed.
7. In the Entitlement Selection Strategy section of the page, select a role selection strategy from the list, as shown:
   - **Selected entitlements:** Allows you to manually select the entitlements. Click **Add** to search and select the entitlements. To remove any selected entitlement, click **Remove**.
   - **All Entitlements with Selected Certifiers:** Allows you to select a list of users including all the entitlements for which they are the certifier user in the catalog.
   - **Entitlements associated with certifiers in selected organizations:** Allows you to generate certifications for all entitlements whose certifiers belong to the selected organizations.
   - **All Entitlements:** Allows you to select all entitlements from the catalog.
   - **Entitlement Criteria:** Allows you to select entitlements based on a criteria. You can filter the criteria based on various entitlement attributes and catalog UDFs. To do so, select the **Apply further criteria** option in the Selection Constraints section, and then select the attributes and catalog UDFs.

> **Note:**
>
> You can save the search and use it for specifying entitlement criteria while creating another entitlement certification definition. The saved search is not mapped to a specific certification. To use the entitlement criteria saved search for another entitlement certification definition:
>
> a. During certification creation, after selecting the **Entitlement Criteria** option and specifying the search condition, you must click **Update and Preview Results**. This associates the selected criteria with the definition.
>
> b. If you want to save this search criteria as a template, then click **Save**. You are prompted to enter a name for the template that you are saving. You can then save this template and reuse it.
> The saved template is not specific to a certification. While creating another certification, this template is displayed by default. If you create another new template, then that template is displayed. In other words, the latest template is displayed for all criteria screens associated with a type of certification.
>
> c. If you do not want to use the generated template, then change the value in the Saved Search list to something else that you want to use.

8. (Optional) Under Selection Constraints, deselect the **Include entitlements provisioned by access policy** option to exclude the entitlements from the certification definition that are provisioned by access policies.

   Deselecting this option filters out all access granted via access policies during certification creation. For example, entitlement (Ent1) was granted to users (User1 and User2), and User2 got this Ent1 via role/policy. When you create an entitlement certification with this option deselected to exclude access policy grants, then the newly created certification will contain only User1.

   This option is selected by default, which means that the certification definition will include all entitlements that are provisioned by access policy and other mechanisms, such as direct provisioning, request, or reconciliation.

9. Select any one of the following options to specify constraints:
   - Entitlements with Any Level of Risk
   - Only High Risk Entitlements

10. Click **Next**. The Content Selection page is displayed.

11. Click **Next**. The Configuration page is displayed.

12. Select the configuration options, as described in Table 13-3, and click **Next**. The Reviewers page is displayed.

> **Note:**
>
> In the Configuration page, if you select the **Prevent self certification** option and choose an alternate reviewer, then the **Entitlement - Certifier Role** reviewer option is not available for selection.

13. From the Reviewer list, select a primary reviewer. The primary reviewer can be any one of the following:

- **Entitlement (Certifier User):** Selects the entitlement certifier user as the primary reviewer.
- **Entitlement (Certifier Role):** Selects the entitlement certifier role as the primary reviewer.
- **Search for a User:** Selects any user as the primary reviewer that you search and specify by clicking the lookup icon.
- **Search for a Role:** Selects all user members of any role that you select by clicking the lookup icon as the primary reviewer. Any user member of the role will be able to claim the task in order to review and certify. When the task is claimed by a user, other users in the role will not be able to view the task in the Inbox.

  Group certifier assignments are not supported with CertificationProcess composite. If you want to specify a role as the primary reviewer, then you must select the CertificationOverseerProcess composite in the Configurations page of the wizard.

14. Click **Next**. The Incremental page is displayed.

    Incremental certification is not supported for group/role certification. Therefore, if you have selected the **Search for a Role** option in the Reviewers page, then the Incremental page is skipped and the Summary page is displayed.

15. Select **Enabled** for Generate Incremental Data. This setting enables certifiers to certify or revoke only changes or inclusions made to a certification. It eliminates the need to review the access of users who have been certified.

    When Incremental Certification is enabled, it takes the following parameters:

    - **Incremental Date Range** (required): This includes:
      - **Since Last Base** (default): When this option is selected, current access of the user is compared against the last certification of the same type, which was created without enabling incremental and all the incremental certifications since then, to the current date when the certification is created.
      - **Since Date:** When this option is selected, current access of the user is compared against all the certifications of the same type since the given date and when the certification is created.
    - **Show Previous Value** (optional): This includes:
      - **Disabled** (default): When this is deselected, then the values that have already appeared in the previous certifications based on the Incremental Date Range parameter are not included in the certification.
      - **Enabled:** When this is selected, all the current values that existed in previous certifications are displayed with the last decisions taken for those access.

16. Click **Next**. The Summary page is displayed with the details of the user certification.

17. Click **Create**. A message is displayed asking if you want to create a certification job based on the definition and run it now. You can edit the job name, and click **Yes** to run the certification job.

    Alternatively, click **No** to create a certification definition without creating and running the scheduled job. With this option, you must manually create a certification job later.

The new entitlement certification definition is displayed in the Certification Definition page.

13.3.2 Modifying Certification Definitions

You can edit certification definitions by selecting them in the Certification Definitions page and using the Edit option.

To modify a certification definition:

1. In the **Compliance** tab of Oracle Identity Self Service, click the **Identity Certification** box, and select **Definition**. The Certification Definitions page is displayed.
2. Select the certification definition that you want to modify.

> **Note:**
>
> If there is a periodic scheduled task tied to this definition, then the next execution of the scheduled task will be run by using the modified changes.

3. From the Actions menu, select **Edit**. Alternatively, you can click **Edit** on the toolbar.

   A message is displayed stating that the definition is referenced by scheduled jobs and event listeners and asking for confirmation. This message is not displayed if you try to edit a certification definition for which you have not created certification jobs.
4. Click **Edit** to confirm. The Certification Definition pages are displayed on which you can edit the values in the fields.
5. Edit the fields to modify the certification definition by navigating through the pages by clicking the **Next** and **Back** buttons.
6. When finished, click **Save**. A message is displayed stating that the definition has been successfully updated.
7. Click **OK**.

13.3.3 Deleting Certification Definitions

You can delete certification definitions by selecting them in the Certification Definitions page and using the Delete option.

To delete a certification definition:

1. In the **Compliance** tab of Oracle Identity Self Service, click the **Identity Certification** box, and select **Definition**. The Certification Definitions page is displayed.
2. Select the certification definition that you want to delete.
3. From the Actions menu, select **Delete**. Alternatively, you can click **Delete** on the toolbar.

   A message is displayed stating that the definition is referenced by scheduled jobs and event listeners and asking for confirmation. This message is not displayed if you try to delete a certification definition for which you have not created certification jobs.
4. Click **Delete** to confirm. A message is displayed asking for confirmation.
5. Click **OK**.

13.4 Scheduling Certifications

You must create a certification definition before you can schedule it.

Certifications are scheduled as part of the certification creation process. For more information, see Creating Certification Definitions. Certifications can be scheduled to run once, or to repeat on a daily, weekly, or monthly basis.

After you create a certification definition by clicking Create on the Summary page of the New Certification wizard, a message is displayed asking if you want to create a certification job and run it. You can edit the scheduled job name in the Job Name box. When you click Yes, the certification job is created for the new certification definition and is run. You can go to the Scheduler section in Oracle Identity System Administration and search for the job. The default name of the job is Cert_*DEFINITION_NAME*.

The certification job is created based on the Certification Creation Task scheduled task. This scheduled task is used to create new certification jobs for a defined certification definition. When the job runs, the certification definition is used and certifications are generated.

See "Predefined Scheduled Tasks" in the *Administering Oracle Identity Governance* for information about the Certification Creation Task scheduled task. You can modify the certification jobs from the Scheduler section of Oracle Identity System Administration. See "Modifying Jobs" in the *Administering Oracle Identity Governance* for details.

You can also schedule a certification from the Scheduler section of Oracle Identity System Administration. To do so, follow the instructions in "Creating Jobs" in the *Administering Oracle Identity Governance*. In this method, select Certification Creation Task in the Task field in the Create Job page.

When you modify a certification job, specify the certification definition name in the Certification Definition Name field of the Job Details page.

13.5 About How Risk Summaries are Calculated

You can directly assign high, medium, and low risk levels to roles, application instances, and entitlements, as well as to certain predefined risk factors.

A risk-aggregation job calculates Risk Summaries for the remaining higher-order data objects that are required to support identity certification. These objects include every user, user-role assignment, account, and entitlement-assignment in Oracle Identity Manager. During identity certification, certifiers use Risk Summaries to separate high-risk certification items from medium-risk and low-risk items.

This section describes how the system processes risk levels to arrive at Risk Summaries. It also describes the risk-aggregation job, which you can run manually or on a scheduled basis. It contains the following topics:

- Understanding Item Risk and Risk-Factor Mappings
- About Risk Aggregation and Risk Summaries
- About How Changing Risk Configuration Values Impacts the System

> **Note:**
>
> Roles, application instances, and entitlements are *metadata* objects, whereas users, accounts, and entitlement-assignments are *instance-data* objects.
>
> Metadata objects are structural objects that represent and describe your information systems within Oracle Identity Manager, whereas instance-data objects are the individual instances of application data that populate the systems. For example, consider a customer service application (a resource) that has a predefined role that enables users to create trouble tickets (an entitlement). In this example, a single resource object represents the application and a single entitlement object represents a specific privilege within that application.
>
> Now consider there might be thousands of user accounts on this resource, some subset of which has the entitlement-assignment that allows the user to create a trouble ticket. A single resource (metadata object) can have multiple accounts (instance-data objects), and a single entitlement (metadata object) can have multiple assignment instances (instance-data objects). Oracle Identity Manager calculates the risk levels for instance-data objects because it would not be feasible for a human to process risk levels for every user, account, and entitlement-assignment on a recurring basis.

13.5.1 Understanding Item Risk and Risk-Factor Mappings

Item risk refers to the risk levels that you and other administrators can assign to specific roles, application instances, and entitlements. Risk-Factor Mappings are settings that map risk levels to certain predefined conditions.

Item risk and the risk-factor mappings are settings that are under your direct control.

This section contains the following topics:

- Setting Item Risk
- About Risk-Level Mappings (Risk Factors)

13.5.1.1 Setting Item Risk

Item risk refers to the risk levels that you and other administrators can assign to specific roles, application instances, and entitlements.

> **Note:**
>
> Three bars signifies high risk, two bars signifies medium risk, one bar signifies low risk.

If you do not directly assign an item-risk level to a metadata object, then Oracle Identity Manager assigns a default item-risk level for you. Roles, application instances, and entitlements can each have a default value.

To set the default item-risk level for the metadata objects:

1. Login to Oracle Identity Self Service.
2. Click the **Compliance** tab.
3. Click the Identity Certification box, and select **Risk Configuration**. The Risk Configuration page is displayed.
4. Select the High, Medium, or Low risk radio buttons for each item.
5. Click **Save**.

You should reserve high item-risk levels for metadata objects that confer highly-restricted privileges to users. Note that setting a high item-risk level on an object will cause its parent object to also have a high Risk Summary value. Similarly, setting a medium item-risk level on an object will cause its parent object to have at least a medium Risk Summary value. In order for a higher-order object to have a low Risk Summary value, all of the objects under it in the system hierarchy would have to have low risk settings.

13.5.1.2 About Risk-Level Mappings (Risk Factors)

Risk-Factor Mappings are settings that map risk levels to certain predefined conditions. For example, you might configure "items with open audit violations" as high risk, whereas "items that are closed as risk-accepted" you might configure as medium risk.

Generally speaking, you should reserve high Risk-Factor levels for conditions in which privileges are being extended to users that may be irregular or dangerous.

There are three Risk-Factor categories in Oracle Identity Manager, and each category contains multiple settings. Risk-Factor categories are described in Table 13-4.

Table 13-4 Risk Factors

Risk Factor	Description
Provisioning Scenarios / Assignment Scenarios	*Provisioning Scenarios* define the risk levels that should be associated with the method or mechanism used to assign a role, account, or entitlement-assignment to a user. For example, you might configure a risk level of *Medium* for objects that are provisioned directly by an administrator, and a risk level of *Low* for objects that are provisioned based on Policies that are tied to Roles. You might configure a risk-level of *High* for objects that are pulled into Oracle Identity Manager via reconciliation.
Last Certification Action	Defines risk level based on the status of the last certification for the account, entitlement-assignment, or user-role assignment under consideration. For example, configure a risk level of *Low* for any item for which the previous certification decision was to approve, and configure a risk level of *Medium* for any item for which the previous certification decision was to *Certify Conditionally*. Finally, you might configure a value of *High* for any item for which the previous certification decision was *Abstain* or *Revoke*.

Table 13-4 (Cont.) Risk Factors

Risk Factor	Description
Identity Audit Violation	Defines risk levels associated with causes contained in open identity audit violations. A cause may be associated with an account, entitlement-assignment, or user-role assignment. For example, you might configure a risk level of High for objects that have an associated cause in an active violation, because such a situation represents a Segregation of Duties (SoD) violation. Note that if an object has no associated causes in an open identity audit violation, then this risk factor is skipped when computing risk summaries.

Note:

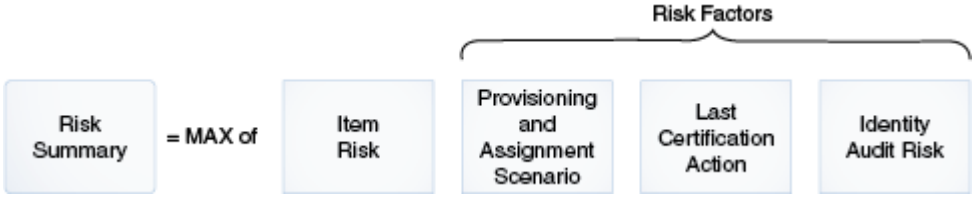
Changing Risk-Level mappings on the Risk Configuration page in the UI can cause major ripple effects that impact Risk Summaries throughout Oracle Identity Manager. During your initial setup you should configure mappings on the Risk Level configuration page, and then avoid making additional unnecessary changes. See About How Changing Risk Configuration Values Impacts the System for more information about the ripple effects that impact Risk Summaries.

13.5.2 About Risk Aggregation and Risk Summaries

The Risk Aggregation Task scheduled job processes Item-Risk levels and Risk-Factor levels, and calculates Risk Summaries for each higher-order object that supports identity certification.

Risk aggregation Task is used to seed the predefined Risk Aggregation Job. You do not need to create new jobs using this task. When a job of this task type runs, it calculates the risk of all the users in Oracle Identity Manager since they have been last updated. See "Predefined Scheduled Tasks" in the *Administering Oracle Identity Governance* for information about this scheduled task. You can enable the Risk Aggregation Task scheduled job by following the instructions in "Disabling and Enabling Jobs" in the *Administering Oracle Identity Governance*.

In the first phase of risk aggregation, the Risk Aggregation Task scheduled job evaluates each individual object's Item-Risk level and its three Risk-Factor levels, and assigns the highest of the four levels to the object's Risk Summary property. A Risk Summary value is calculated for each individual User object, User-Role Assignment object, Account object, and entitlement-assignment object. The following diagram illustrates this process.

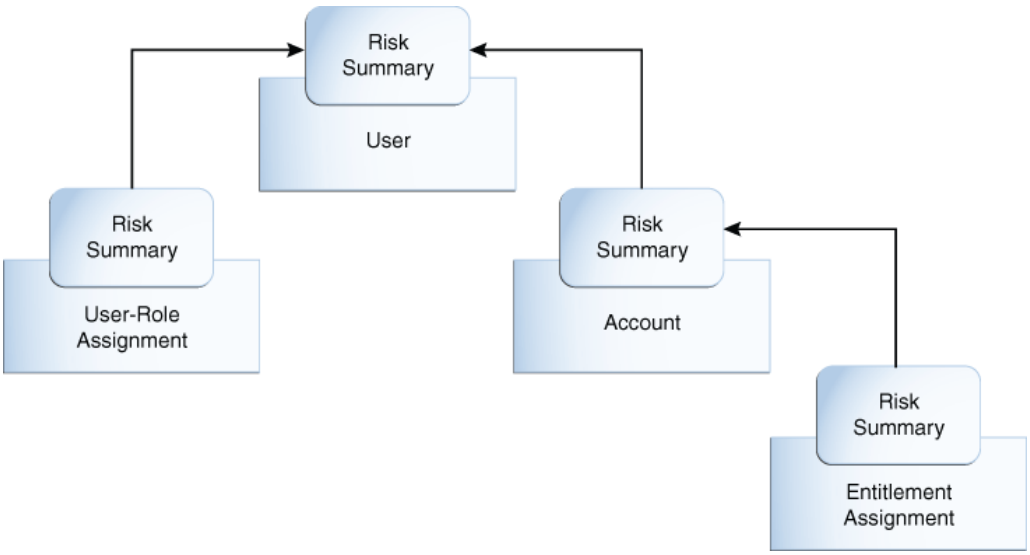


Once Risk Summaries are calculated for every object, the next phase of aggregation begins, in which the Risk Summary of each individual object rolls up to the Risk Summary of the parent object that contains it.

Above the entitlement-assignment level, each data object's Risk Summary value contributes to the Risk Summary of the parent-object that contains it. For example, Account objects are one hierarchy-level up from entitlement-assignment objects, and User objects are one hierarchy level up from there. So, the Risk Summary of every entitlement-assignment object within an Account object contributes to the Risk Summary for that Account, and, similarly, the Risk Summary for every Account object within the User object contributes to the Risk Summary for that User.

User objects are also one level above User-Role Assignment objects, so the Risk Summary for every User-Role Assignment object contributes to the Risk Summary for that User.

The following diagram illustrates this process.



In the diagram, the Risk-Summary value of the entitlement-assignment rolls up to the Account object. The Risk-Summary values of Accounts and the Risk-Summary values of User-Role Assignments roll up to the Risk Summary of any associated User.

13.5.3 About How Changing Risk Configuration Values Impacts the System

There are three main actions or system events that can impact Risk Summary values. Depending on the action or system event, the impact can be minor, moderate, or major.

Each action or event that can impact Risk Summary values and its consequences is described in Table 13-5.

Table 13-5 Actions or System Events That can Impact Risk Summary Values

Action or Event	Impact	Description
Users and/or Oracle Identity Manager make changes to individual entitlements	Minor	Applies to changes to individual data objects, such as accounts, entitlements, and user-role assignments. These values might change frequently. For example, the following types of changes are included in this category: • An entitlement is added to or removed from an account. • An account is added to or removed from a user. • A role assignment is added to or removed from a user. • A risk factor on an individual data object changes. The impact within Oracle Identity Manager is relatively minor because the changes happen at the level of each individual entitlement.
An administrator makes item-risk changes to roles, resources, and entitlements	Moderate	Applies to situations where you or another administrator change the risk-level of a role, an application instances, or an entitlement. The ripple-effect of these changes can be large. Changing the risk level on a metadata object can change the item-risk level on every data-object associated with the metadata object. Changing the risk level on a data-object may affect its risk summary and, in turn, the risk summary of every other data-object that contains it. For example, changing the risk level on an entitlement definition will change the Item Risk on every assignment of that entitlement that corresponds to it. Changing the Item Risk on an entitlement-assignment may change its Risk Summary. Changing the Risk Summary of an entitlement-assignment may affect the Risk Summary of the parent Account. Changing the Risk Summary of an Account may affect the Risk Summary of the User who owns the Account.
An administrator makes configuration changes to the Risk-Level Mappings	Major	Applies to situations where you or another administrator change the Risk-Level Mappings on the Risk Configuration page in Oracle Identity System Administration. Changing the risk level associated with a specific value of a specific risk factor could affect the risk summary of any user-role assignment, account, or entitlement-assignment that has that risk-factor value. Changing the risk summary of any user-role assignment, account, or entitlement assignment could in turn affect every user associated with an affected user-role assignment, account, or entitlement assignment. For this reason, you should change risk-level mappings only rarely.

13.6 About Closed-Loop Remediation and Remediation Tracking

Closed-loop remediation is a feature that allows you to directly revoke roles, application accounts, and entitlements from the provisioning solution as a result of roles and entitlements revoked during the certification process.

When a certification is complete and all primary review tasks have been signed off, Oracle Identity Manager attempts to remove every user and privilege for which the final decision was to revoke. Requests are created to de-assign any role-assignment that is revoked, to de-provision any account that is revoked, to remove any entitlement-assignment that is revoked, and to delete or disable any user that is revoked. Specifically:

- Revoking a user deletes/disables the user and removes all privileges of that user.
- Revoking a user's role-assignment removes that member from the role. This might eventually cause provisioning to remove accounts and entitlement-assignments granted by the role (if those accounts and entitlement-assignments are not otherwise granted to the user.)
- Revoking a user's account deletes/disables the account. This implicitly removes/disables any entitlement-assignments associated with that account.
- Revoking a user's entitlement-assignment removes the assignment from the account that contains it.

The remediation status can be tracked in the request catalog for auditing purposes. Each remediation-request contains the certification ID of the certification that spawned the request, which allows the Dashboard to link to the Track Requests page of Oracle Identity Self Service to display the status of all the requests associated with the certification that is being displayed.

13.7 Configuring Challenge Workflows

Some requests that are generated as a result of closed-loop remediation go through a challenge workflow. You can configure the requests that are auto-approved.

This section describes how to configure challenge workflows in the following topics:

- About Challenge Workflows
- Modifying Rules of Auto-Approval

13.7.1 About Challenge Workflows

The requests generated as a result of closed-loop remediation are either auto-approved or goes through a challenge workflow.

By default, closed-loop remediation functions in the following way:

- If the person who signed-off the certification (final reviewer) is the user's (beneficiary's) manager, then the requests are auto-approved.
- If the final reviewer is not the user's manager, then the requests go through a challenge workflow, which is as follows:
  1. A request is sent to the user (beneficiary) whose access is revoked.
  2. If the beneficiary accepts the revoke by approving the request, then closed-loop remediation takes place and access is revoked.
  3. If the beneficiary challenges the revoke by rejecting the request, then the request is sent back to the person who signed off the certification (final reviewer).

a. If the final reviewer accepts the challenge, then the process stops and the beneficiary's access is not revoked.

b. If the final reviewer rejects the challenge, then closed-loop remediation takes place and the access is revoked.

13.7.2 Modifying Rules of Auto-Approval

The auto-approval logic is defined within the DefaultRequestApproval composites in SOA by using rules. You can modify the rules to have all the closed-loop remediation requests to be auto-approved.

To modify the rules to have all the closed-loop remediation requests to be auto-approved:

1. Login to Oracle SOA Composer with Admin credentials, such as weblogic, by navigating to the following URL:

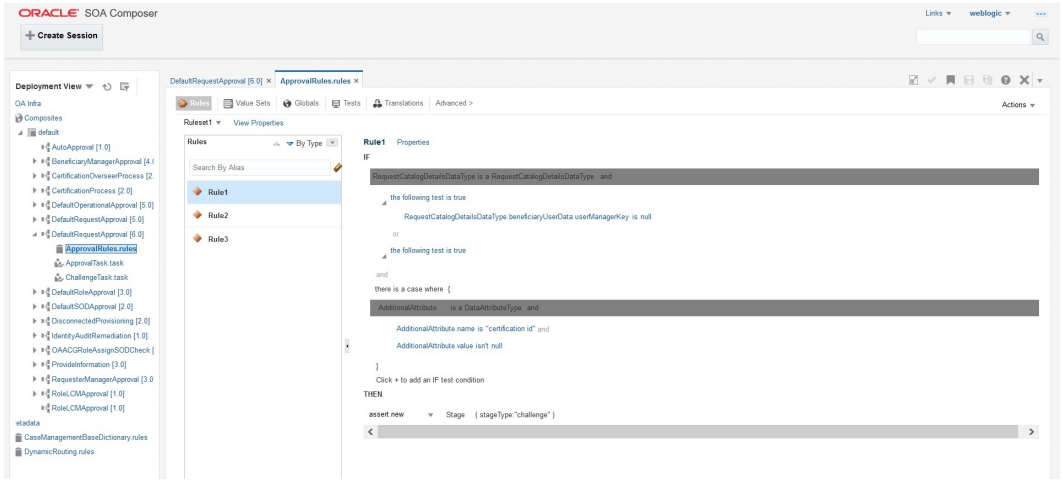
   http://*HOST_NAME*:*PORT_NUMBER*/soa/composer

2. In the Deployment View, select **Composites**. From Composites, select **default**.

3. From the default tree, select **DefaultRequestApproval[6.0]**, and then select **Approval Rules.rules**. The details appear in the pane on the right side of the window.

4. Select **Rule1**, and click **Edit Session** on the Oracle SOA Composer menu bar to view the details of the rule as shown in Figure 13-1.

Figure 13-1 Rule for Auto-approval



5. In the THEN area of the rule, click the **Edit Properties** button next to the rule action. The Properties dialog box is displayed where you can modify the property details. Change the stageType value from *challenge* to *auto*.

6. Verify that the value is updated successfully in the Properties pop-up.

7. When done with changes, click **Save Changes in Current Tab**. If you are ready to apply the changes to the runtime version, click **Publish**.

13.8 About Event Listeners

The Event Listener mechanism detects specific business events and stores the event details for certification.

The stored event details are called Certification Event Triggers, and these are processed into certifications by the Certification Event Trigger Task, running as a scheduled job. The business events currently detected by event listeners are modifications of Oracle Identity Manager users, either individually or in bulk.

Every event listener contains a ruleset and a certification definition, as described in Managing Certification Definitions. The ruleset contains one or more rules, each of which tests one or more conditions and specifies an action to take if its conditions are met. The standard action for event listener rules is to store a Certification Event Trigger that identifies the event listener, the user or users that were modified, and the certification definition that should be generated in response to this event.

Triggers accumulate between runs of the Certification Event Trigger Job. When the job runs, it groups the triggers by their event listener identifiers, and then processes each group according to the corresponding event listener's properties. By default, the trigger job creates a certification for all users in each group of triggers, using the listener's certification definition as the template for the certification. After this, the triggers from the completed group are deleted.

There are several properties that affect how an event listener's triggers will be processed by the trigger job. The first property determines whether the listener is in active or disabled state. If a listener is disabled, then its rules are no longer evaluated when business events occur, and therefore, no triggers are stored from that listener. If a listener stored triggers before being disabled, then the next trigger job run deletes those triggers without processing them. When a disabled listener is set back to active state, it can once again store triggers that are processed by the trigger job.

Another event listener property that affects trigger processing is its Event Count, which limits how many triggers may be processed for the listener during a single run of the trigger job. This setting is optional. If it is not specified, then the number is unlimited. If the event count is specified, then it represents the maximum number of triggers that may be processed. When the trigger job runs, it checks the listener's event count for each batch of triggers, and if the number of triggers exceeds the event count, then the triggers are discarded without generating a certification. This feature is useful for preventing huge certifications from being created when users are modified in bulk.

Finally, the trigger job itself may be configured to process the triggers from certain event listeners, but not others. This feature is controlled by a Certification Event Trigger Task parameter titled Event Listener Name List. If this parameter is left blank in the definition of the trigger job, then triggers from all listeners are processed when the trigger job runs. If the name list is defined, then only the listeners in that list have their triggers processed when the job runs; triggers from other listeners are ignored and retained for future trigger job runs. When multiple instances of scheduled jobs are defined for the Certification Event Trigger Task, then each list of event listeners can have its triggers processed on the most appropriate schedule.

> **Note:**
>
> If a listener name appears in more than one Event Listener Name List, or if one of the trigger jobs has an empty Event Listener Name List, then the first of these jobs to run consumes all of that listener's triggers. Triggers are always discarded after the first time they are processed.

13.9 Configuring Event Listeners and Certification Event Trigger Jobs

Configuring event listeners involves creating, modifying, and deleting event listeners. Configuring certification event trigger jobs involve setting the event listener name and adding mode trigger jobs.

This section describes about configuring event listeners and certification event trigger jobs in the following topics:

- Creating an Event Listener
- Modifying an Event Listener
- Deleting an Event Listener
- Configuring Certification Event Trigger Jobs

13.9.1 Creating an Event Listener

Creating an event listener involves providing values for the event listener attributes and adding a rule containing conditions that will be evaluated when an event takes place.

To create a new event listener:

> **Note:**
>
> Before creating an event listener, you must create a user certification definition or an application instance definition that will be executed when the Certification Event Trigger job is run.

1. Login to Oracle Identity Self Service.
2. Click the **Compliance** tab.
3. Click the **Identity Certification** box, and select **Event Listeners**. The Event Listeners page is displayed.
4. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Event Listener page is displayed.
5. In the Listener Properties section, specify the name with which the event will be identified, and the description.
6. From the Certification Definition list, select a certification definition that will be executed.
7. In the Event Count box, enter the maximum number of events that should be processed for this listener at the time the Certification Event Trigger Job runs. Use this to avoid executing an action for bulk updates.
8. From the Status list, select Active or Disabled status.
9. In the Event Trigger section, add a rule containing conditions that will be evaluated when an event takes place. For example, when a user is updated, a condition can check if the user's title property or location property has changed. Another example can be change of manager for a user.

To add a condition:

a. In the Rules panel, click the plus (+) icon, click the down arrow key and select **General Rule**. A new rule is included.

b. Select the rule, and the rule details are displayed on the right side.

c. Under IF, click the plus (+) icon, and then click the down arrow key to select the type of rule from the list. For example, Simple Test.

d. Click the lookup icon to open the Condition Browser.

e. Click **Modified User**, **previousValue**. Select **manager**, and click **OK**. This sets `ModifiedUser.previousValue.Manager`.

f. Select the condition operation, such as **isn't**.

g. Click the second lookup icon, search and select the attribute name and click **OK**, so that the following condition is set:

```
ModifiedUser.previousValue.Manager isn't
ModifiedUser.currentValue.Manager
```

h. Under THEN, click the plus (+) icon to the left of Add Action.

i. Click the down arrow key and select **call**.

j. From the list, select **certifyThisUser**.

When multiple rules are configured, you can set advanced properties like, priority, mode, and status. To provide advanced property for a rule:

a. In the Rules panel, select the rule. The rule details are displayed on the right side.

b. Click **Properties** link to open the Advanced Property window.

c. Provide the following information: **Name**, **Description**, **Priority**, **Active**, **Advanced Mode**, **Tree Mode**, and **Effective Date**.

For more information on the Advanced Property Setting for a rule, see How to Show and Edit Advanced Settings for Rules in *Designing Business Rules with Oracle Business Process Management*.

10. Click **Create** to create the event listener.

When the Certification Event Trigger job is run, a certification will be created for a user whose manager has changed.

An example of the event listener rule can be to check for an attribute's change to a specific value. For example:

```
ModifiedUser.previousValue.country isn't ModifiedUser.currentValue.country and
ModifiedUser.currentValue.country is "Brazil"
```

`ModifiedUser.previousValue.country isn't ModifiedUser.currentValue.country` checks for a change in the Country attribute. Any change causes this condition to evaluate to TRUE. Then, `and ModifiedUser.currentValue.country is "Brazil"` adds a second condition to the rule. This checks whether the attribute has changed to a specific value, for example Brazil. This condition is applicable if some special certification is required for employees moving to Brazil. For other employees who have moved to some other place, the rule's action is not triggered.

> **Note:**
>
> User-Defined Fields (UDFs) or custom attributes do not appear in ModifiedUser's lists of current and previous values, but these attributes can be specified in the Event Listener rule conditions. To do so, type an expression in the following format into the rule's condition field:
>
> ```
> ModifiedUser.{current|previous}Value.get{String|Integer|Long|Date|
> Boolean}Attribute("NAME")
> ```
>
> Here, *NAME* is the internal name of the UDF. For example, to retrieve the previous value of a string-valued UDF named FavoriteColor, insert the following expression:
>
> ```
> ModifiedUser.previousValue.getStringAttribute("FavoriteColor")
> ```

13.9.2 Modifying an Event Listener

Modifying an event listener involves selecting the event listener in the Event Listeners page and editing the event listener attributes in the event listener details page.

To modify an event listener:

1. In the **Compliance** tab of Oracle Identity Self Service, click the **Identity Certification** box and select **Event Listeners**. The Event Listeners page is displayed with a list of event listeners.
2. Select the event listener that you want to modify.
3. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar. The event listener details page is displayed.
4. Edit the values in the fields to modify the event listener.
5. Click **Save**.

13.9.3 Deleting an Event Listener

Deleting an event listener involves selecting the event listener in the Event Listeners page and using the Delete option.

To delete an event listener:

1. In the **Compliance** tab of Oracle Identity Self Service, click the **Identity Certification** box and select **Event Listeners**. The Event Listeners page is displayed with a list of event listeners.
2. Select the event listener that you want to delete.
3. From the Actions menu, select **Delete**. Alternatively, click **Delete** on the toolbar. A message is displayed asking for confirmation.
4. Click **Yes** to confirm.

13.9.4 Configuring Certification Event Trigger Jobs

The Certification Event Trigger Job offers an optional parameter called Event Listener Name List. If one or more event listener names are supplied in this field, then the trigger job will only

process the triggers for those listeners, which implies that you will need multiple trigger jobs to cover processing for your full set of listeners.

This section describes how to set the Event Listener Name List parameter and how to define multiple trigger jobs. It contains the following topics:

- Setting the Event Listener Name List
- Adding More Trigger Jobs

13.9.4.1 Setting the Event Listener Name List

To set the Event Listener Name List:

1. Login to Oracle Identity System Administration.
2. On the left pane, under System Configuration, click **Scheduler**.
3. In the search field, enter `Certification Event Trigger Job`, and perform the search.
4. Click the job name in the search result to display the trigger job details.
5. Scroll down to the Parameters section, where you can see a parameter titled Event Listener Name List (comma separated).
6. Enter one or more event listener names in this field, separated by commas. Make sure to type each listener's name exactly as it appears in the Name column of the Event Listeners table.
7. Click **Apply** to save the changes.

13.9.4.2 Adding More Trigger Jobs

In addition to the predefined instance of the Certification Event Trigger Job, you can create new trigger job instances by performing the following steps:

1. Login to Oracle Identity System Administration.
2. On the left pane, under System Configuration, click **Scheduler**.
3. On the left pane, from the Actions menu, select **Create**. Alternatively, you can click the icon with the plus (+) sign beside the View list.
4. In the Create Job panel, expand the Task field by clicking the icon to its right.
5. In the Search field, enter `Certification Event Trigger Task`, and perform the search.
6. In the search result, click the Certification Event Trigger Task row, and then click **Confirm**.
7. Enter the Job Name and any desired scheduling details for this trigger job instance.
8. In the Event Listener Name List field, enter a comma-separated list of the listener names that this trigger job instance will process.

Every instance of the trigger job can have its own schedule or can be run manually, and can be restricted to handling triggers for a specified subset of listeners. This enables you to trigger different event listeners at different intervals.

13.10 Configuring Certification Reports

Certification reports can be generated in PDF, RTF, HTML, Microsoft Excel, and CSV formats.

To configure the display of the Reports tab in the Detailed Information section of the Dashboard:

1. Log in to Oracle Identity System Administration.
2. Click the **Compliance** tab.
3. Click the **Identity Certification** box, and select **Certification Configuration**. The Certification Configuration page is displayed.
4. Select the **Enable Certification Reports** option.
5. Click **Save**.

Reports can be generated in the following formats:

- PDF
- RTF
- HTML
- Microsoft Excel
- CSV

13.11 Understanding Multi-Phased Review in User Certification

Two-phased review and advanced delegation (TPAD) is supported for user certifications only. It involves multiple phases of review, delegation to multiple reviewers within each phase, and stages of certification in TPAD.

This section describes two-phased review with advanced delegation in the following sections:

- About Functionality of Two-Phased Review with Advanced Delegation
- Multiple Phases of Review
- Delegation to Multiple Reviewers Within Each Phase
- Stages of Certification in TPAD

13.11.1 About Functionality of Two-Phased Review with Advanced Delegation

TPAD combines the perspectives of business-oriented and technical reviewers and allows a certifier to delegate decision-making to other reviewers.

Collaborative certification or TPAD provides the following functionalities:

- Two-phased review, which allows to combine within a single certification the perspectives of business-oriented and technical reviewers.
- Advanced delegation, which allows a certifier to retain overall responsibility while delegating decisions to others. Advanced delegation of individual line-items within a certification allows a reviewer to spread the work among several people who can work

simultaneously. This allows those who are responsible for reviewing access within an enterprise to spread the burden and thus complete the work more quickly.

> **Note:**
>
> Oracle Identity Manager supports TPAD for user certification only. TPAD is not supported for role certification, application instance certification, and entitlement certification.

13.11.2 Multiple Phases of Review

Multiple phases of review combines multiple perspectives on the same set of user-access-privileges.

For user certification, the phases are:

- **Business Review:** This is the required first phase of review. The business reviewer, typically the manager of each user, views all the certifiable access privileges of a user. First, the manager confirms that the user is a valid holder of privileges, such as an employee, within that enterprise. Then the manager confirms that the user's position within the enterprise justifies the user's access privileges, such as role assignments, account assignments, and entitlement assignments. The business reviewer certifies or approves any privilege that seems appropriate and revokes any privilege that seems unnecessary or unreasonable.
- **Technical Review:** This is an optional second phase of review. The technical reviewer, typically the owner or an authorizer of each privilege, reviews the members of the privilege or the assignments of that privilege to specific users or to specific accounts of specific users. The technical reviewer certifies or approves any privilege that seems appropriate and revokes any assignment of that privilege that seems unnecessary or unreasonable.
- **Final Review:** This is an optional final phase review. If the certification is configured to enable final review, then the primary reviewer from the first phase, for example the manager of each user, can see the decisions that reviewers made in the first two phases and can override those decisions if required.

> **See Also:**
>
> Who Is Involved in Completing Identity Certifications? for information about primary reviewer, technical reviewer, final reviewer, and delegated reviewer.

13.11.3 Delegation to Multiple Reviewers Within Each Phase

The primary reviewer in Phase One or Phase Two can reassign responsibility, and delegate and undelegate line-items.

The primary reviewer in Phase One or Phase Two can spread the work to other users in the following ways:

- The primary reviewer can reassign responsibility for any set of line items to another user. Reassignment transfers the responsibility to another person, whereas delegation retains the responsibility with the primary reviewer. Reassignment of line items in Phase One creates a new certification.
- The primary reviewer can delegate each line-item, or any set of line-items, to any user that the primary reviewer selects. This user is called a delegated reviewer. Delegating a line-item marks that line-item as delegated in the primary reviewer's task, and prevents the primary reviewer from acting on that line-item.
- The primary reviewer can undelegate any delegated line-item at any time within the phase before signing off the certification task. Undelegating a line-item removes it from the delegated reviewer's task, and allows the primary reviewer to act on the line-item, for example, by making certification-decisions or delegating or reassigning it.

In Phase One or Phase Two, whenever the primary reviewer delegates line-items and signs off with at least one line-item still delegated, which means that the primary reviewer has not undelegated all of those line-items before signing off, then Oracle Identity Manager generates a review task for Phase-One Verification or Phase-Two Verification, and assigns this task to the primary reviewer. This task allows the primary reviewer to see and override any decision that a delegated reviewer made in that phase.

13.11.4 Stages of Certification in TPAD

The stages of certification in TPAD are phase one with verification, phase two with verification, and final review.

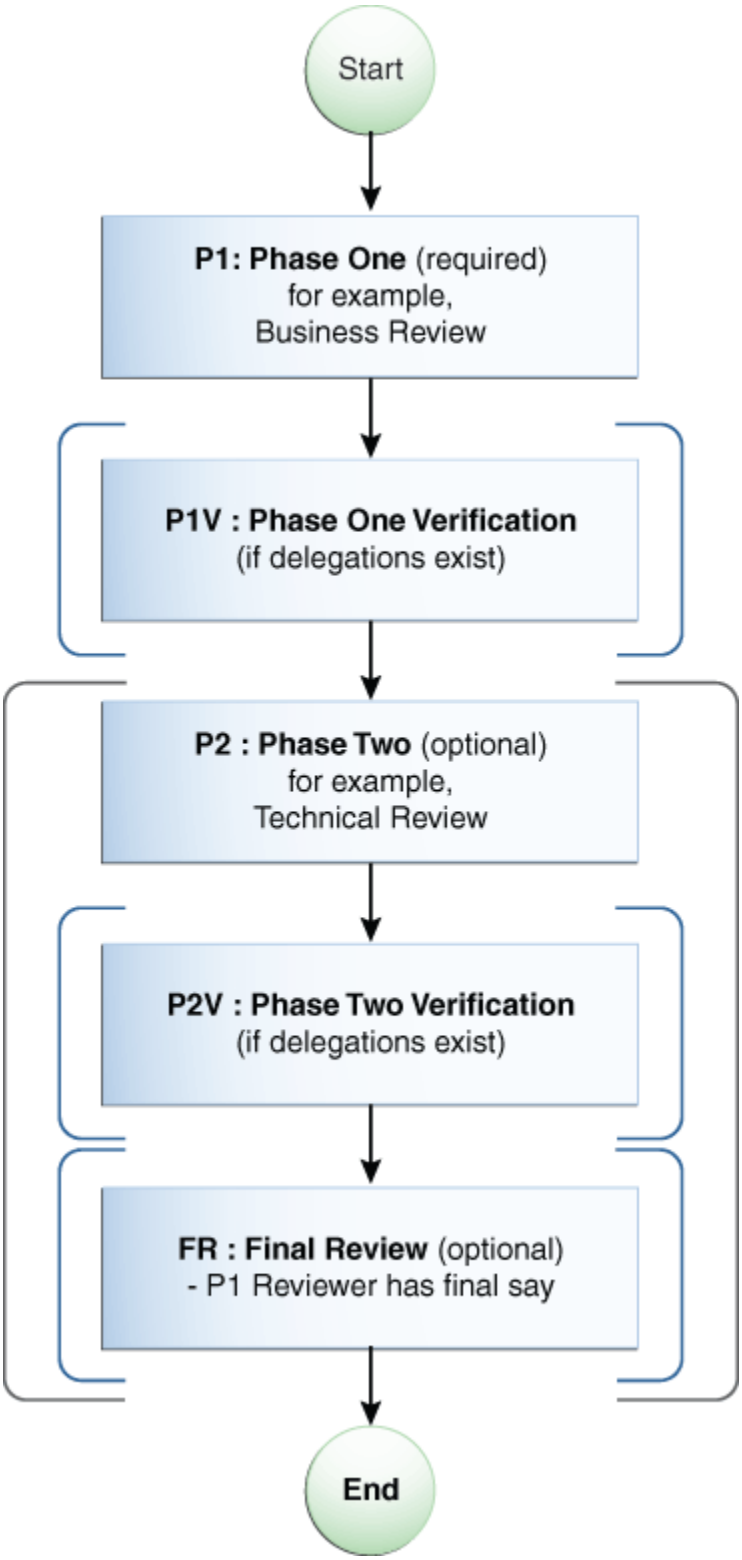
The certification stages in TPAD are described in the following sections:

- About Stages of Certification in TPAD
- Phase One With Verification
- Phase Two With Verification
- Final Review

13.11.4.1 About Stages of Certification in TPAD

Figure 13-2 illustrates the stages of certification in TPAD by combining the required Phase One, the optional Phase Two, and the optional Final Review phase that depends on Phase Two, with the conditional verification tasks.

Figure 13-2 Stages of Certification in TPAD



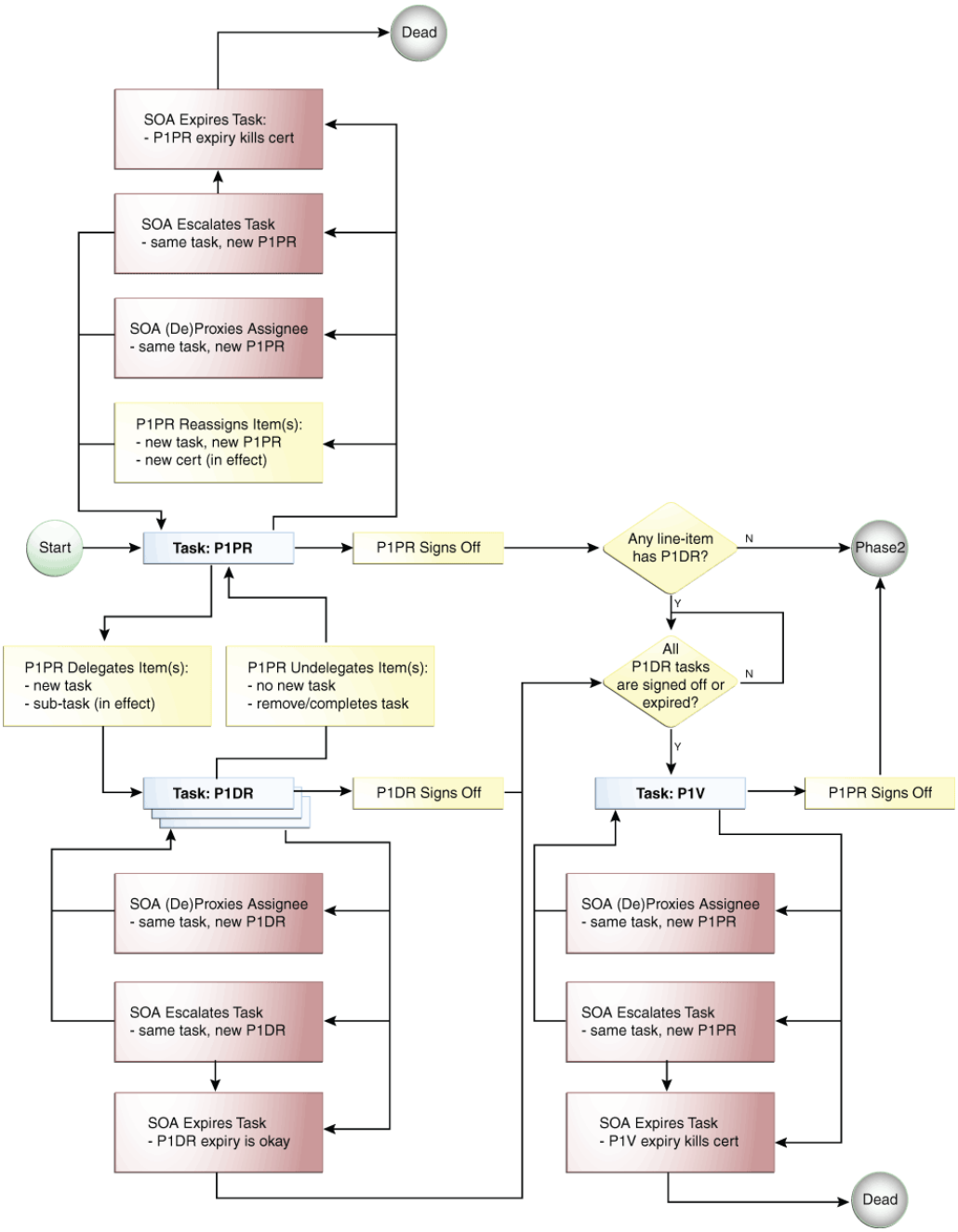
As shown in Figure 13-2, the overall sequence of stages within TPAD certification are:

1. **start:** Certification is created, and certification task is generated by running the Certification Creation Task scheduled job.
2. **Phase One Review:** This is always required.
3. **Phase One Verification:** This takes place only if Phase One is completed with delegations.
4. **Phase Two Review:** This is optional depending on configuration.
5. **Phase Two Verification:** This takes place only if Phase Two is completed with delegations.
6. **Final Review:** This is optional depending on configuration and takes place only if Phase Two is completed.
7. **end:** Certification task is completed. If any access has been revoked as a part of the certification completion, then closed-loop remediation takes place.

13.11.4.2 Phase One With Verification

Figure 13-3 shows the first phase of certification review with TPAD.

Figure 13-3 Phase One With Verification



Following is the process flow of the Phase One review with verification in TPAD:

1. **Start:** A set of certification objects are generated, and the review process starts. Every line-item within each particular certification object is assigned to a Phase One Primary Reviewer (P1PR).
2. **Task P1PR:** When the scheduled jobs for certification generation are run, Oracle Identity Manager uses Service-Oriented Architecture (SOA) to create a task, for each certification object, which is assigned to the Phase One Primary Reviewer (P1PR).

When the primary reviewer opens the task, the primary reviewer can see every line-item within the certification object. If the primary reviewer opens any particular line-item, then the primary reviewer can see every line-item-detail for that line-item.

The primary reviewer can act on any line-item within the task. The primary reviewer can delegate any line-item to another person, or can reassign any line-item to another person. By default, the primary reviewer owns every line-item and can decide, such as certify or revoke, the line-item-details.

After decision has been made for each line-item, or each detail for the line-item has a Phase-One Decision, or has been delegated or reassigned, the primary reviewer can sign off or complete the task.

3. **P1PR Reassigns Item(s):** If the primary reviewer during Phase One reassigns any set of line-items to another person, then Oracle Identity Manager removes those reassigned line-items (and their details) from the original certification and puts them into a new and separate certification. The person to whom the line-items were reassigned becomes the P1PR for that new and separate certification.

   The reassigned line-items disappear from the task of the original P1PR, and does not reappear within this review process. Even if the new P1PR reassigns or delegates the line-items back to the original P1PR, this creates a new task for the original P1PR so that it is part of a different review process in the following way:

   - If the new P1PR reassigns line-items back to the original P1PR, this will be a new certification with its own P1PR task.
   - If the new P1PR delegates the line-items back to the original P1PR, then this will be a new delegated review (P1DR) task within the review-process of the new P1PR.

4. **P1PR Delegates Item(s):** If the primary reviewer delegates any set of line-items to another person, then that person is the phase one delegated reviewer (P1DR) for each of those line-items. A new task is created and assigned to the new P1DR.

   > **Note:**
   >
   > In order to minimize the number of tasks, it is recommended that you select the set of line-items that you intend to delegate to a particular reviewer. Otherwise, the delegated reviewer can receive any number of tasks, each of which contains some subset of line-items from the same phase of the same certification object.

   When the primary reviewer delegates a particular set of line-items, the line-items are marked as delegated within the task from which the primary reviewer delegated them. The primary reviewer can no longer act within that task on those line-items unless the primary reviewer undelegates them. The primary reviewer has an opportunity during Phase One Verification to see and override the decisions made by any delegated reviewer.

5. **P1PR Undelegates Item(s):** The primary reviewer can undelegate or take back from a delegated reviewer any line-item that is delegated. Undelegating a line-item allows the primary reviewer to act on that line-item and removes that line-item from the task of the current delegated reviewer, which prevents the delegated reviewer from acting on it further.

6. **P1PR Signs Off:** After every line-item has been completed or delegated or reassigned, the primary reviewer can sign off on the task, which completes the task. A line-item is

completed when all of its details have a decision for the current phase. At this point, Oracle Identity Manager determines whether or not Phase One Verification (P1V) is required.

7. **SOA (De)Proxies Assignee (P1PR):** A proxy can be assigned for the assigned reviewer, such as P1PR. For example, when the reviewer is scheduled to go on vacation, the reviewer can activate a proxy. When the reviewer returns from vacation, the proxy is deactivated. When the newly assigned (proxy) reviewer opens the task, the proxy reviewer can view and act on each line-item and line-item-details. See Managing Proxies for information about adding, modifying, and removing proxies.
8. **SOA Escalates Task (P1PR):** The certification task can be escalated depending on configuration of the SOA composite that Oracle Identity Manager uses for certification-review tasks. For example, if the reviewer has not signed off or completed a task within a configured time-limit, SOA can escalate the task and reassign it to the manager of the currently-assigned reviewer. After the task is escalated the maximum number of times or has reached some other condition that terminates escalation, the task expires.
9. **SOA Expires Task (P1PR):** A certification review task can expire in certain conditions. For example, if the reviewer has not signed off a task within a configured time-limit, then the task can expire. If the task is configured to escalate before expiring, then SOA expires the task only after it has escalated the maximum number of times or reaches some other condition that terminates escalation. When a task expires, it cannot be acted upon.
10. **Task: P1DR:** Each delegated-review task contains a set of line-items that the primary reviewer has delegated to the delegated reviewer. When the delegated reviewer opens the task, the delegated reviewer can see only the line-items that are delegated in the particular delegation-event that produced the task. If the phase-one delegated reviewer (P1DR) opens any particular line-item, P1DR can see every detail for that line-item.

    The delegated reviewer can act on any line-item within the task. The delegated reviewer cannot delegate any line-item to another person, cannot undelegate any line-item, and cannot reassign any line-item to another person. By default, the delegated reviewer owns every line-item and can decide, such as certify or revoke, its line-item-details. After every line-item has been decided, or all the details for the line-item has a Phase-One Decision, the delegated reviewer can sign off or complete the task.
11. **P1DR Signs Off:** After every line-item within a delegated-review task has been decided, the delegated reviewer can sign off or the task. Every delegated-review task must complete or must expire before the certification review process can proceed to Phase-One Verification.
12. **Any line-item has P1DR:** This branch-point decides whether the Phase One Verification stage is required. This depends on whether any line-item is delegated:
    - If any line-item that is not reassigned remains delegated when the P1PR signs off, then the review process moves to Phase One Verification.
    - If no line-item that is not reassigned remains delegated when the P1PR signs off, then the review-process moves to Phase Two.
13. **All P1DR tasks are signed off or expired:** This branch loops until every Phase One delegated-review task has either been signed off (completed) or has expired.
14. **Task: P1V:** After the primary-reviewer (P1PR) has signed off and every delegated-review-task (P1DR) has either completed or expired, Phase One Verification

begins. Another task for the same certification-object is created and assigned to the primary reviewer. Within this task, the primary reviewer can see and override any decision made in Phase One. The primary reviewer also can complete any line-item that no delegated reviewer has completed. The primary reviewer cannot reassign and delegate, and therefore, cannot undelegate any line-item within this task.

15. **P1PR Signs Off (P1V):** After every line-item-detail within the certification-object for every line-item that has not been reassigned to another primary reviewer has a decision, the Phase-One Primary Reviewer can sign off. When the reviewer signs off on the Phase-One Verification task, the certification review process proceeds to Phase Two.
16. SOA can proxy the assignee, and escalate or expire the P1V task (similar to the P1PR task). See steps 7 through 9 for details.

13.11.4.3 Phase Two With Verification

Phase Two is an optional, plural, and rotated version of Phase One.

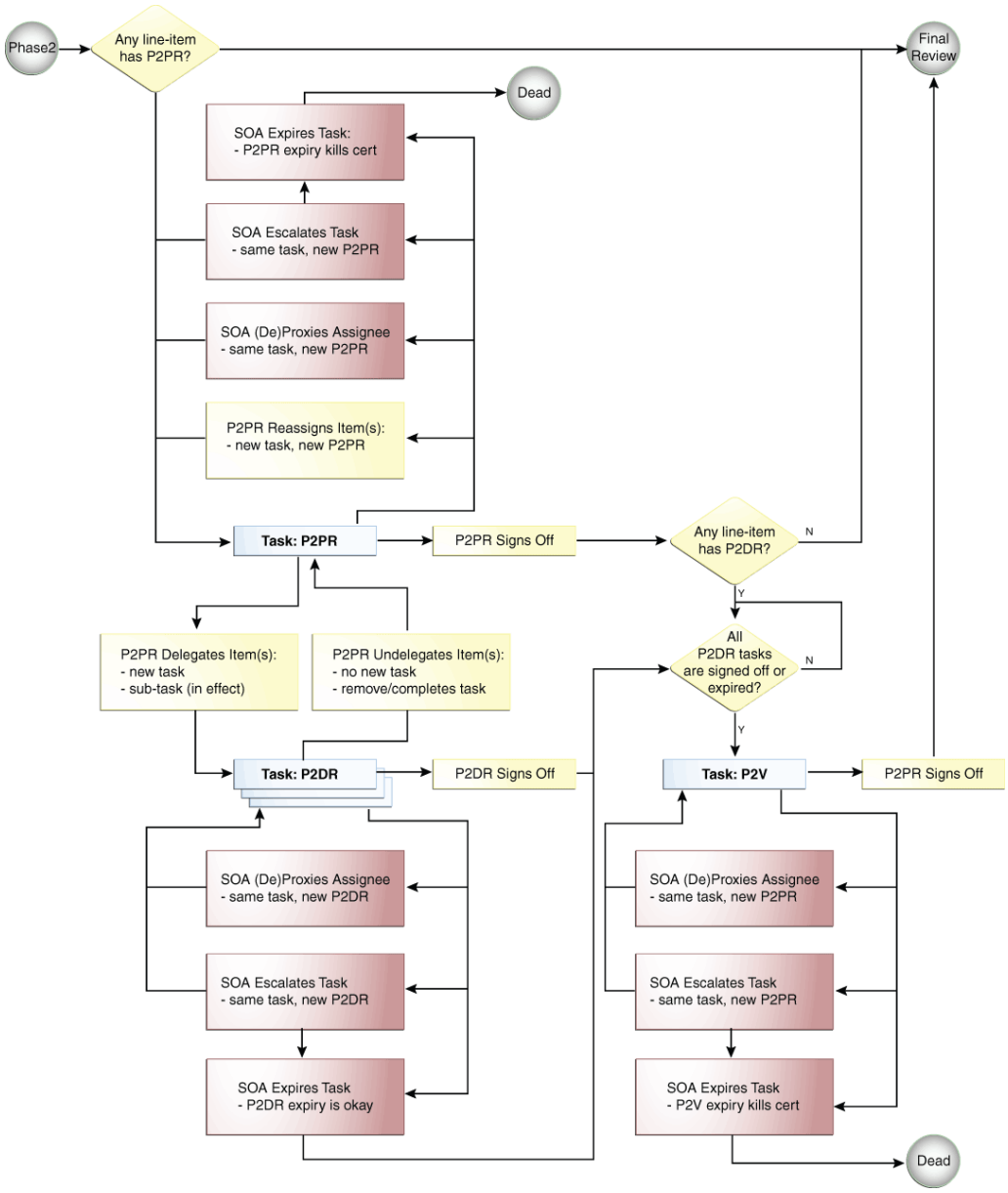
Optional: Phase Two is optional because it occurs only if Phase Two is enabled in configuration, the administrator specified a strategy to select a Phase Two Primary Reviewer, and the specified strategy assigned a Phase Two Primary Reviewer to at least one line-item within the certification.

Plural: There can be multiple Phase Two Primary Reviewers because each reviewer administers or authorizes a line-item-detail rather than a line-item. For example, in a user certification, each role assignment, account assignment, or entitlement assignment can have a different primary reviewer.

Rotated: Each reviewer in Phase Two can see a rotated view. For example, in Phase One of user certification, the business-reviewer can see users as line-items and each user's access-privileges as line-item-details. In Phase Two of user certification, each technical reviewer can see privilege-definitions, such as role, application instance, or entitlement definitions, as line-items and can see members of each privilege as line-item-details. This privilege-centric view is more useful to a technical-reviewer, who can delegate or reassign responsibility for individual privilege-definitions.

Figure 13-4 shows the second phase of certification review with TPAD.

Figure 13-4 Phase Two With Verification



The stages in Phase Two are similar to Phase One, except for the following:

- **Task: P2PR:** A review task is generated for each type of privilege for which each Phase Two primary reviewer (P2PR) must review assignments within that certification. When a Phase Two primary reviewer opens a P2PR task, that primary reviewer can see a list of line-items for which that primary reviewer is responsible within the certification object. For example, in Phase Two of a user certification, the Technical Reviewer who opens a P2PR task can see a list of privileges, such as role definitions, application instance definitions, or entitlement definitions, for which that primary reviewer is the certifier and for which that certification object contains assignments. Because this type of certification is user-centric, the rotated view is privilege-centric.

If the primary reviewer opens any particular line-item, the primary reviewer can see every line-item-detail for that line-item. The primary reviewer can act on any line-item within the task. The primary reviewer can delegate any line-item to another person or can reassign any line-item to another person. By default, the primary reviewer owns every line-item and can decide, such as certify or revoke, its line-item-details.

- **P2PR Reassigns Item(s):** If the primary reviewer in Phase Two reassigns any set of line-items to another person, then that person becomes the new primary reviewer (P2PR) for those line-items. Oracle Identity Manager creates a new primary-review task and assigns it to the new P2PR.

> **Note:**
>
> The Reassign operation in Phase Two does not generate a new certification. For example, if a primary technical reviewer reassigns a (rotated) line-item, then this does not split the certification.

The reassigned line-items disappear from the task of the original P2PR. The line-items are displayed within a separate task that is assigned to the new P2PR.

13.11.4.4 Final Review

Final Review is optional and is a tie-breaker. It is the simplest phase in TPAD.

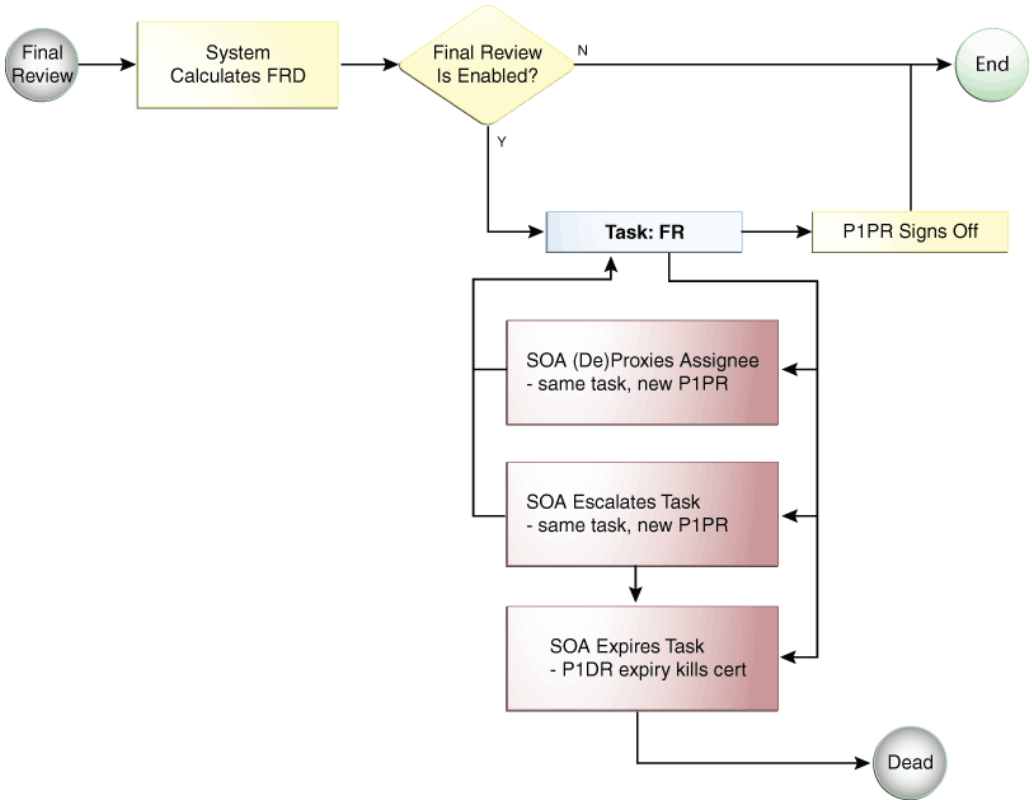
Optional: Final Review occurs only if it is enabled in configuration, the administrator specified in the certification definition that Final Review is to be performed, and Phase Two is performed because at least one line-item had a Phase Two Primary Reviewer.

Tie-breaker: Because the Phase Two reviewers may have made different decisions than the Phase One reviewers, the Phase One primary reviewer can view and override the decisions made in the two earlier phases. Therefore, Final Review is a tie-breaker.

Simplest phase: There is only one Final Reviewer, who is the Phase One Primary Reviewer. The Final Reviewer cannot delegate and cannot reassign. The Final Reviewer can see the decisions made during Phase One, the decisions made during Phase Two, and can override the decisions.

Figure 13-5 depicts the optional Final Review phase of certification review with TPAD.

Figure 13-5 Final Review Phase



In Final Review, the following stages are different from other review phases:

- **System Calculates FRD:** Oracle Identity Manager calculates a Final Review Decision (FRD) in the following manner:
  - For any line-item detail that has a Phase Two decision other than Abstain, the Phase Two decision becomes the Final Review decision.
  - If a particular line-item detail lacks a Phase Two decision, or if the Phase Two decision is to abstain, then the Phase One decision becomes the Final Review decision.
- **Final Review is enabled:** This branch decides whether or not to generate a task for Final Review and assign it to the Phase One Primary Reviewer. If Phase Two is disabled in configuration, or if Phase Two is not used in this certification review, or if Final Review is disabled in configuration, then task for Final Review is not generated. If Phase Two decisions have been made and Final Review is enabled in configuration, then the task for Final Review is generated.
- **Task: FR:** The Final Reviewer opens the Final Review task, and can see the following:
  - The decision made during Phase One on each line-item detail.
  - The decision made during Phase Two on each line-item detail.
  - The Final Review Decision.

  The Final Reviewer can override the FRD in the context of the Phase One and Phase Two decisions. The Final Reviewer cannot reassign and delegate, and

therefore, cannot undelegate any line-item within the task. The Final Reviewer can sign off after validating each FRD. At that point, the Final Review task is complete and the overall certification process is complete with the exception of closed-loop remediation, which Oracle Identity Manager performs automatically following signoff. If the Final Reviewer does not sign off and allows the Final Review task to expire, then the certification process is dead.

You can use Final Review to compare the Phase One decision with the Phase Two decisions and make a final decision. If you prefer the Phase Two decision, then do not enable Final Review in configuration.

13.12 About Pre-populate Certification Comments

This content applies only to OIG Bundle Patch 12.2.1.4.211010 Bundle Patch and later releases.

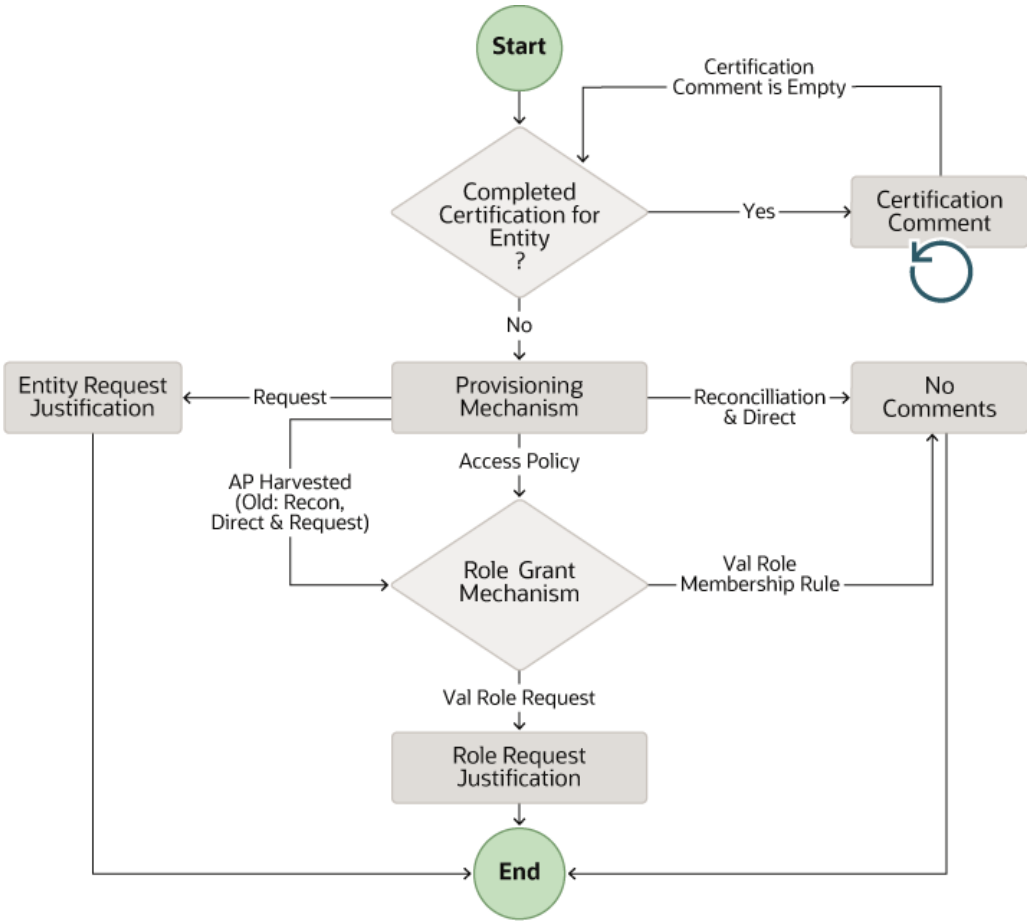
For certification definition, when the **Pre-populate comments on certify operations** configuration property is selected, the comments will be mined for the campaign and pre-populated on the UI against each line item of the campaign details page, where available.

The comment for each line item is populated with the first available in the following order when campaign is executed:

- Non-empty comment from last completed certification for line items
- Comment from the Request Justification from for line items
- For Account/entitlement granted via Access Policy, the justification for the associated Role Request

For more details on pre populated comments, refer to the following flowchart:

Figure 13-6 Certification Comments



> **Note:**
>
> To populate a campaign with the most recent comments, execute the **Certification Comments Mining** job before you start the run for a certification definition. For more information about this job, refer Predefined Scheduled Tasks.

13.13 About Certification UI New Features

This content applies only to OIG Bundle Patch 12.2.1.4.211010 Bundle Patch and later releases.

- From this release, the UI experience is enhanced based on the following values of the configuration properties:
  - Allow comments on certify operations

- Mandatory comments on certify operations
- Allow comments on all non-certify operations
- Mandatory comments on all non-certify operations

The following table provides the complete details:

Configuration Property Value	UI Behaviour
– Comments allowed for certify operation => False	1. In this case, when you select one/more rows and click **Certify**, then no dialog box is shown to enter comments. 2. If any comments exists, then it changes to null.
– Comments allowed for certify operation => True – Mandatory comments for certify operation => False	1. In this case the dialog box will not be shown for entering comments when you select one/more rows and click **Certify**. 2. The rows will be certified using the existing comments against each row. 3. To add/modify the comment for a row, select the row and use **Edit Comments** before performing the certify action.
– Comments allowed for certify operation => True – Mandatory comments for certify operation => True	1. Single row selected: The dialog box to set comments is shown if the comment does not exist for the row. If comment is present, then no dialog box is shown and it will be certified using existing comment. 2. Multiple rows selected and comments exists for all rows: Then no dialog box is shown and rows will be certified using the existing comment. 3. Multiple rows selected and comments doesn't exist for one or more row: The dialog box is shown with **Comments** and the check box **Use if comment does not exist**". Deselect the check box if you want to use the comment provided for all the selected rows. If the check box is selected, the new comment is used for only those rows which do not have comments. The other rows will be certified with the existing comments. 4. Select All: This uses the existing comments to certify all the rows across pages. If comment is missing for any row, then it displays an error for that and other rows are certified.
– Comments allowed on non-certify action => FALSE	1. In this case, when you select one/more rows and click **Revoke**,then no Dialog box will be shown. 2. Also if any comment exists, it will be updated to null.

Configuration Property Value	UI Behaviour
– Comments allowed for non-certify operation => True – Mandatory comments for non-certify operation => False/True	1. In this case, when you click **Revoke**, a dialog box is shown to enter the comments and it will always be shown. The comments need to be entered (the comments will be required if **Mandatory comments for non-certify operation** property is set to TRUE) 2. The existing comments against a row will not be used in this case.

13.14 About Certification Oversight

Certification *oversight* is the activity of reviewing, and possibly overriding, the decisions of the primary reviewer within the scope of a particular primary-review task.

A person who has the opportunity to override the certification decisions of a primary reviewer within the scope of a particular primary-review task is called an *overseer*. The overseer has the following characteristics:

- An overseer must be an Oracle Identity Manager user.
- Only one overseer at a time can oversee a primary-review task.
- An overseer has the right to view and override the decisions made by the primary reviewer or by any previous overseer.

As a part of the certification configuration, you can select a certification composite that defines the certification oversight workflow. A certification composite is a SOA workflow that the certification server launches for each primary reviewer, or delegated reviewer, during a phase of certification.

By default, the CertificationOverseerProcess composite defines the following behavior:

- A primary-review task is not completed until the primary reviewer and every overseer in the sequence has signed off.
- Decisions signed off by the final overseer in the sequence of overseers are final for that primary-review task.
- Closed-loop remediation begins after the overall certification is complete. No phase of certification is complete until every primary-review task is complete.
- For Phase Two and Final Review phase of certification:
  - Since Phase Two can have multiple primary reviewers, each primary-review task can have a separate sequence of overseers, one primary-review task per each primary reviewer. For detailed information about multi-phased reviews, see Understanding Multi-Phased Review in User Certification.
- For delegation, oversight takes place only for the verification task of a primary reviewer. If the primary reviewer delegates during the primary-review task, then the primary-review task does not have oversight. Instead, oversight takes place during the subsequent verification-task, which contains all the decisions for that phase.
- Reassignment of a line-item during Phase One of certification creates a new certification and creates a new primary-review task that is assigned to the re-assignee. Here, a new sequence of overseers are calculated for the new primary-review task.

You can extend the default oversight functionality to specify different levels of oversight or stop the oversight process when a certain stage is reached. To do so, you must create and deploy custom certification composites. For more information on creating and deploying custom certification composites, see Customizing Certification Oversight in *Developing and Customizing Applications for Oracle Identity Governance*.

13.15 Troubleshooting Identity Certification

Verify the certification configuration settings and ensure that the required SOA patches have been applied.

Table 13-6 lists possible issues encountered while using identity certification and the steps to resolve the issues.

Table 13-6 Troubleshooting Identity Certification Issues

Problem	Solution
You create certification definition and run the Certification Creation Task scheduled job, but no certification tasks are generated.	Make sure that all the certification configuration steps, as described in Configuring Certifications, have been performed.

> **Note:**
>
> Ensure that all required SOA patches are applied.

14

Managing Identity Audit

You can use the Identity Audit (IDA) feature of Oracle Identity Manager to detect Segregation of Duties (SoD) violations. The detection mechanism of IDA monitors users' actual access to resources, and captures any violations on a continuous basis.
This chapter describes about the Identity Audit feature in the following topics:

- About Identity Audit
- Understanding Identity Audit Concepts
- Enabling Identity Audit
- Configuring Identity Audit
- Managing Identity Audit Rules
- Managing Identity Audit Policies
- Managing Scan Definitions
- Managing Policy Violations

14.1 About Identity Audit

The identity audit feature detects SoD violation or identity audit policy violation, which is a violation whereby a user has been assigned privileges that should not be held individually or in combination.

Identity audit enables the creation of rules and policies that detect potentially dangerous combinations of privileges held by users or roles that can lead to access violation, and determines policy violations and policy violation causes.

This feature can be enabled or disabled by setting the value of the `Identity Audit` system property to true or false respectively. See Managing System Properties in *Administering Oracle Identity Governance* for information about this system property. Also, in an upgraded deployment of Oracle Identity Manager, you must manually set the value of the `Workflows policies enabled` system property in order to use the identity audit and role lifecycle management features.

14.2 Understanding Identity Audit Concepts

Key concepts related to identity audit are detection mechanism, identity audit rules, rule conditions, identity audit policies, scan definitions, scan jobs, policy violations, remediators, policy violation remediation, and policy violation reports.

The concepts related to Identity Audit are described in the following topics.

- About Modes of Detection
- About Identity Audit Rules
- About Rule Condition

- About Identity Audit Policies
- About Scan Definitions
- About Scan Jobs
- About Policy Violations
- About Remediators
- Understanding Policy Violation Remediation
- About Policy Violation Reports

14.2.1 About Modes of Detection

Identity audit uses detective mode or preventive mode for detecting policy violations.

You can use Identity Audit to detect SoD violations. The detection mechanism of Identity Audit monitors users' actual access to resources, and captures any violations on a continuous basis. This can be one of the following types:

- **Detective mode:** In a detective mode, the entire identity warehouse of users can be monitored for anomalies or toxic combinations of user access rights.
- **Preventive mode:** In preventative mode, any access that is requested via the access catalog in real-time can be automatically detected as an Identity Audit policy violation, and preventative action can be taken.

There may be multiple audit policies defined. A single audit policy detects a specific violation on users. An audit policy is composed of one or more audit rules, and each rule detects a cause of the violation. User profiles as well as their associated roles, accounts, entitlements, and organizations are then scanned for identity audit policy violations. User accounts (including entitlements), user attributes, and roles/access policies that violate an identity audit policy are flagged and tracked until the violation is resolved. The solution also maintains a comprehensive history of audit scans.

14.2.2 About Identity Audit Rules

An identity audit rule consists of a rule condition. These rules can be simple or complex based on the entities and user access privileges. You can define complex rules with nested conditions on the basis of user information, catalog metadata associated to applications, entitlements, roles, and organization metadata.

An identity audit rule can be associated with multiple policies. When a rule condition is modified, all policies associated with this rule are impacted. If the modified rule is the cause of any existing open violations in the system, then the cause and the associated violation are impacted by the change in condition.

A rule can be specified by entering an IF condition, and then return values when the condition matches.

Rules are associated with policies. When entities associated with an impacted violation are scanned against the policies associated with the rule, Oracle Identity Manager takes the following actions on the violation:

- Oracle Identity Manager checks whether the modified condition still causes an exception.

- If the rule condition still results in an exception, then Oracle Identity Manager sets the violation cause status to Active. Otherwise, the violation cause status is set to Inactive.

Identity audit rules must be owned by a user. Any user can be a rule owner irrespective of the admin role privileges of the user.

> **Note:**
>
> - See Managing Administration Roles for information about admin roles and admin role capabilities.
> - The following admin role capabilities related to identity audit policies cannot be used from Identity Self Service, but can be used through APIs:
>   - Identity Audit Policy - Assign Rule
>   - Identity Audit Policy - Unassign Rule
>   - Identity Audit Policy - Disable
>   - Identity Audit Policy - Enable
>   - Identity Audit Policy - Assign Rule
>   - Identity Audit Policy - Unassign Rule
>   - Identity Audit Rule - Enable
>   - Identity Audit Rule - Disable
>   - Identity Audit Scan Run - Delete
>
>   For information about using APIs, see Using APIs in the *Developing and Customizing Applications for Oracle Identity Governance* and *Java API Reference for Oracle Identity Governance*.

You can add new rules to an existing policy. However, this change can impact some existing unresolved violations. The next time the modified policy is scanned, existing open violations that are impacted by this change are updated and new ones are created if the new rules have caused exceptions.

14.2.3 About Rule Condition

A rule has a single condition. A rule's condition is the IF portion of the rule and is evaluated to be either true or false against the input values passed to the rule at policy evaluation time.

A condition is a set of one or more criteria, which can be logically conjugated together with AND or OR operators. The criteria can be grouped, and the groups can be logically conjugated together with AND or OR operators. This allows for complex nested Boolean expressions. A condition criterion consists of an attribute, operators, and value, as shown:

```
Condition criterion = ATTRIBUTE OPERATOR VALUE
```

14.2.4 About Identity Audit Policies

An identity audit policy is a collection of audit rules that together enforce SoD business policies. Identity audit policies consist of metadata, such as the identity audit policy name,

description, severity, creation date, and update data. Identity audit policies have designated policy owners and policy remediators.

An identity audit policy must be owned by any user. The policy owner can create, search, view, modify, or delete policies.

By default, policies will report a violation if any of its rules evaluate to true.

An identity audit policy owner is responsible for the definition of the policy. However, it is the remediator's responsibility to take action on an identity audit policy violation and fix the violation.

14.2.5 About Scan Definitions

An identity audit scan is the action of executing an identity audit policy along with its associated rules against a given population of entities (users). A scan definition specifies a particular identity audit scanning ‘recipe’ that can be used by a scheduled task to run and repeat the desired scan in the future.

Scan definitions contain a base selection of users or organizations to scan, and a collection of one or more policies to evaluate when scanning. In addition, other configuration settings can also be specified in a scan definition.

Scan definitions act as templates that configure a scheduled task (scan job) with audit scan parameters. Scan definitions themselves contain no scheduling information.

Identity Audit scan can be of the following types:

- **Detective scan:** A scheduled job that performs an Identity Audit scan according to a specified Identity Audit scan definition, and generates a persistent policy violation for each user SoD conflict that it detects. This type of scan is used to find latent problems in access privileges.

  A detective scan is the process of applying a scan definition to a user population and generating Identity Audit policy violations. A scan definition consists of policies and user-selection criteria. Each policy contains rules that define the combination of access privileges that will result in a violation being detected by the scan. Detective scans are run as Oracle Identity Manager scheduled jobs. Detected violations are persisted to the data store if they are new and updated if they already exist. You can also use the capability of running a detective scan on-demand for a single policy in a "preview" mode. In preview mode, the scan returns a collection of preview violations that it has detected, but these violations are not actionable and can only be saved temporarily.

- **Preventive scan:** A synchronous (not scheduled) Identity Audit scan that reports a list of violations. This type of scan is used to detect hypothetical policy violations that might be introduced as a direct result of a particular access grant during the request process.

  A preventive scan is a synchronous IDA scan that returns a list of potential violations against a specified set of IDA policies, initiated as part of access request processes. This type of scan is used to detect potential policy violations that would be introduced if a particular request is submitted by a requestor. The preventive scan violation results may be discarded, or the requestor can be stopped from submitting the request. OIG IDA provides APIs for invoking preventive scans and for managing their results. The IDA Policies included in a preventive scan are those policies marked with the Evaluate flag during access request.

14.2.6 About Scan Jobs

You can save an identity audit scan as a scheduled task. This scheduled task is called scan job that you can run to perform an audit scan.

An identity audit scan can be effectively saved as a scheduled task (a scan job) in the Oracle Identity System Administration that performs an audit scan, using selection criteria from its scan definition with a preface of Identity Audit_ScanDefinitionName, and can be scheduled by an administrator with a given date and time, or on a repeated basis.

Multiple scan jobs can exist, allowing individual scans to be performed on their own schedule. Multiple scan jobs can run concurrently.

14.2.7 About Policy Violations

An identity audit policy violation occurs if one or more rules associated with an identity audit policy is broken by a user account (including entitlements within the account), a user attribute, or a user role.

The goal here is for the solution to track the violation until it is resolved. The solution must display a unique violation per policy and the objects, such as users, roles, entitlements, and accounts, that have been violated within the policy. By default, a policy violation occurs when one or more rules associated with a policy is matched by a user account including entitlements within the account, a user attribute, or a user role.

14.2.8 About Remediators

An identity audit policy must have one or more remediators. A remediator can be a role, a manager, or any user with or without any particular role associated.

You cannot assign multiple users as remediator. Assigning multiple users as remediator can be achieved only by assigning any role as the remediator. A remediator is responsible for fixing an identity audit policy violation or for reassigning the violation to another eligible remediator.

Identity Audit policies have designated remediators who are responsible for taking action when violations are discovered. Notification for policy violations are sent to the Inbox of the remediators. When a policy detects a violation during a scan, the violation is assigned to the remediator(s) designated by the policy. Remediators are notified when they have been assigned a new policy violation. The remediator role allows remediators to view and edit their assigned policy violations.

A remediator may reassign a policy violation to another eligible remediator, after which the original remediator is no longer responsible for the policy violation and can take no further action on it or reclaim it.

14.2.9 Understanding Policy Violation Remediation

Policy violation remediation involves generation of policy violation tasks based on the policy violation causes. A policy violation transitions through a sequence of states during the remediaton process.

This section describes about policy violation remediation in the following topics:

- About Policy Violation Remediation

- About Violation Causes
- About Policy Violation States

14.2.9.1 About Policy Violation Remediation

An Identity Audit scan creates a Policy Violation when the scan detects a target entity (for example, a User) matching one or more rules specified in the policy set referenced by the scan definition. The Policy Violation comprises a set of attributes including the violation target, the policy violated, a violation count, along with a collection of (Policy Rule) Violation Causes. Violation Causes are included to give remediators specific information about the rule conditions that produced the Segregation of Duties conflict. A remediation task is created and assigned to the remediator(s) designated by the policy to initiate the remediation workflow.

14.2.9.2 About Violation Causes

Each violation cause includes the rule, condition, and attributes resulting in the violation.

- About Violation Cause Actions
- About Violation Cause StatesAbout Violation Cause States

14.2.9.2.1 About Violation Cause Actions

The remediator can take one of the following actions:

- **Request for Remediation (remediate):** This action is available for causes that involve catalog items, such as user role, account, and entitlements, within the account. The remediator requests revocation of the catalog item mentioned as a cause of the violation.
- **Close As Fixed:** The remediator has taken an action independent of the provisioning system to fix the violation cause.
- **Close As Risk Accepted:** This action indicates that the violation cause condition should be ignored in subsequent policy re-evaluations for a limited time.

14.2.9.2.2 About Violation Cause States

An Identity Audit policy violation transitions through a sequence of states during the remediaton process. The possible states of an Identity Audit policy violation are:

- **Active:** The initial state of a violation cause. This state indicates that the rule condition still matches.
- **Risk Accepted:** The state after the remediator temporarily disables a rule condition by selecting the Risk Accepted action. This state expires when the specified time limit is reached, and the rule condition is evaluated at the subsequent scan.
- **Manually Fixed:** The state after the remediator takes the Close as Fixed action.
- **Remediation Requested:** The state after the remediator takes the Request Remediation action.
- **Resolved:** This state is set by system when a scan detects that a violation cause condition no longer matches the target entity. Typically, resolved state is reached

when a remediator's action has been applied and an identity audit scan confirms it. However, an external change to the remediation can also resolve a violation cause.

Remediators take action on violation causes to resolve the identity audit policy violation so that it no longer matches any rule of the violated policy. Subsequent scans re-evaluate the policy (re-apply the rules to the target entity) and confirms if the violation cause has been resolved and update the violation cause statuses accordingly. The remediator can also indicate that a violation cause can be accepted (ignored) for a limited time.

14.2.9.3 About Policy Violation States

An Identity Audit policy violation transitions through a sequence of states during the remediaton process. The possible states of an Identity Audit policy violation are:

- **Open:** The initial state of Policy Violation, before it is assigned to the remediator(s) designated by the policy.
- **Assigned:** The state after an Identity Audit Policy Violation has been assigned to a remediator.
- **Remediation In Progress:** The state after the first remediator action and until the remediator completes the remediation.
- **Remediation Under Review:** Policy Violation state is moved to this state if the remediation has overseers. The Policy Violation remains in this state until the last reviewer action.
- **Remediation Completed:** The state after the remediation (and review, if required). From this state, an Identity Audit Scan either closes or re-opens the Policy Violation.
- **Closed:** The state after an Identity Audit Policy Violation is evaluated and no outstanding violations are detected. An administrator can also force the Policy Violation into this state by invoking the Close action.

14.2.10 About Policy Violation Reports

Oracle Business Intelligence Publisher is used for Identity Audit Policy Violation Reports. Reports are available in BI Publisher RTF template format.

BI Publisher uses the appropriate SQL queries (defined in the data model) to query Oracle Identity Manager database (specifically IDA tables) for the violation data.

Identity Audit Policy Violation Reports are available for download from Reports link in the **Compliance** tab of Oracle Identity Self Service. An Identity Audit Policy Violation report can be generated for a Policy, Scan Stop Date, Manager, Remediator or selected users.

For information about generating identity audit policy violation reports, see Generating Identity Audit Policy Violation Reports.

For information about each type of identity audit policy violation report, see "Identity Audit Reports" in the *Administering Oracle Identity Governance*.

14.3 Enabling Identity Audit

By default, the Identity Audit feature is disabled in a Oracle Identity Manager deployment. As a result, the Compliance tab of the Identity Self Service is not available. You can enable

Identity Audit by setting the value of the `Identity Auditor Feature Set Availability` system property to `TRUE`.

To enable Identity Audit:

1. Login to Oracle Identity System Administration.
2. On the left navigation pane, under System Management, click **System Configuration**.
3. Search for the `Identity Auditor Feature Set Availability` system property. This property has the `OIG.IsIdentityAuditorEnabled` keyword.
4. Change the value of this system property to TRUE. By default, the value is FALSE. Changing this value to TRUE enables the Identity Audit feature.
5. Save the change.
6. Restart Oracle Identity Manager server.

   Identity audit is enabled and the Compliance tab in Identity Self Service is available.

14.4 Configuring Identity Audit

After enabling identity audit, you can configure the way identity audit will work. This involves setting the Identity Audit options, and configuring reminders, notifications, escalations, and expiry for identity audit.

This section describes how to configure Identity Audit after it is enabled. It contains the following topics:

- Setting Identity Audit Options
- Understanding Configuring Reminders, Notifications, Escalations, and Expiry for Identity Audit

14.4.1 Setting Identity Audit Options

After identity audit is enabled, you can configure the way identity audit will work by using the Configuration page in Identity Self Service.

To configure identity audit:

1. Login to Oracle Identity Self Service.
2. Click the **Compliance** tab.
3. Click the **Identity Audit** box, and select **Configuration**. The Configuration page is displayed.
4. Under General Settings, specify values for the fields described in Table 14-1.

Table 14-1 Identity Audit or IDA Configuration Settings

Field	Description
Prevent self remediation	Selecting this option prevents the assigned remediator from remediating a policy violation when the remediator's attribute-values are among the causes of the violation. When this option is selected, the administrator must ensure that the scan definition specifies an alternate remediator. Any policy violation that involves the primary remediator will be assigned to the alternate remediator.
Scan Run Details Retention Period	This field specifies the number of days for the retention period. Scan details older than the specified days will be purged. Data is purged only from the IDA_SCAN_RUN_POLICIES and IDA_SCAN_RUN_USERS tables when the retention period or deadline is crossed.
User Batch Size	This field specifies the number of users per batch for a single processing thread.
Threads per scan	This field specifies the number of threads to be used while running a scan.
Composite Name	This property specifies the SOA composite to be used to generate policy violation tasks. The default value is the `default/IdentityAuditRemediation` composite. If you want to use a custom composite to generate policy violation tasks, then click the search icon adjacent to this field, search and select the composite from the Select a Composite dialog box, and click **Select**. **Note:** See "Customizing the Identity Audit Composite" in *Developing and Customizing Applications for Oracle Identity Governance* for information about customizing and deploying the identity audit composite to use a custom identity audit flow.
Maximum Risk Acceptance period for Policy Violation Causes	This field specifies the maximum number of days for which risk is accepted for policy violation causes.

5. Click **Save**.

   You can click Reset to reset the values in the fields to default.

14.4.2 Understanding Configuring Reminders, Notifications, Escalations, and Expiry for Identity Audit

If email notifications is configured in SOA, then email notifications are sent by default when a policy violation is assigned to a user or when a policy violation is completed. You can optionally change this default configuration by using Oracle SOA Composer.

This section describes about configuring reminders, notifications, escalations, and expiry for identity audit in the following topics:

- Understanding Email Notification and Reminders for Identity Audit
- Configuring Reminders, Notifications, Escalations, and Expiry for Identity Audit (Optional)

14.4.2.1 Understanding Email Notification and Reminders for Identity Audit

If email notifications is configured in SOA, as described in "Configuring SOA Email Notification" in the *Administering Oracle Identity Governance*, then email notifications are sent by default in the following scenarios:

- when a policy violation is assigned to a user
- when a policy violation is completed

By default, two reminders are sent one day after and two days after the policy violation task has been created. There is no escalation or expiry set for the policy violations by default.

14.4.2.2 Configuring Reminders, Notifications, Escalations, and Expiry for Identity Audit (Optional)

To change the default configuration for identity audit:

1. Login to Oracle SOA Composer with Admin credentials, such as weblogic, by navigating to the following URL:

   http://*HOST_NAME*:*PORT_NUMBER*/soa/composer
2. Expand the composites, click **Default**, and select **IdentityAuditRemidiation**. The Event Driven Configuration page is displayed.
3. In the Notification Settings section, perform the following:
   a. The assignees of the task are selected as recipients of the notification for Assign and Complete tasks. To change the default setting, you can select the task status in the Task Status column, and select the notification recipient in the Recipient column. You can click the pencil icon for each task to edit the default notification message, and click **OK**.
   b. In the drop-down below, change the default setting for reminders.
4. In the Expiry and Escalation Policy section, you can change the default value for escalation and expiry.
5. Click **Publish** to save the changes.

14.5 Managing Identity Audit Rules

Managing identity audit rules involves searching identity audit rules, creating rules using rule expressions, and modifying, duplicating, and deleting identity audit rules.

This section describes how to create and manage Identity Audit rules. It contains the following sections:

- Searching Identity Audit Rules
- Creating Identity Audit Rules
- Understanding Identity Audit Rule Expressions
- Modifying Identity Audit Rules
- Duplicating Identity Audit Rules
- Deleting Identity Audit Rules

14.5.1 Searching Identity Audit Rules

You can perform basic and advanced search for identity audit rules in the Rules page of Identity Self Service.

This section describes how to perform basic search and advanced search for rules:

- Performing Basic Search for Identity Audit Rules
- Performing Advanced Search for Identity Audit Rules

14.5.1.1 Performing Basic Search for Identity Audit Rules

To perform a basic search for Identity Audit rules:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Rules**. The Rules page is displayed.
3. If fields for advanced search is displayed, then click **Basic**. Otherwise, ignore this step and continue with step 4.
4. From the Search list, select an attribute based on which you can search the rules. The attributes are Rule Name, Description, Created Date, and Owner Login.
5. In the Search box, enter a value of the selected attribute as the search criterion.
6. Click the Search icon. The search result is displayed in a tabular format.

14.5.1.2 Performing Advanced Search for Identity Audit Rules

To perform an advanced search for rules:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Rules**. The Rules page is displayed.
3. Click **Advanced**. The fields for advanced search are displayed.
4. Select any one of the following:
   - **All:** To specify that the search result must match all the specified search criteria.
   - **Any:** To specify that the search result must match any one of the specified search criteria.
5. Specify values for one or more of the Rule Name, Description, Created Date, and Owner Login attributes. The search result will be displayed based on the values that you specify for these attributes.

   For each attribute, select a search operator from the lists, such as Starts With, Ends With, Equals, Does Not Equal, Contains, and Does Not Contain. For any date field, the search operators are Equals, Before, After, On or before, On or after, Between.
6. Optionally, you can add fields to your search criteria by clicking **Add Fields** and selecting fields from the list. A cross icon is displayed with the added fields. You can click the cross icon to remove the added field.
7. Click **Search**. The search result is displayed in a tabular format.

14.5.2 Creating Identity Audit Rules

You can create identity audit rules by using the Create option from the Rules page of Identity Self Service, and specifying the rule conditions in the Condition Builder.

To create Identity Audit rules:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Rules**. The Rules page is displayed.
3. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Rule page is displayed.
4. In the Name box, enter a name of the rule. This is a mandatory field.
5. In the Description box, enter a description for the rule.
6. Click the search icon adjacent to the Owner box, and search and select a user.
7. Verify that **Enabled** is selected in the Status list so that the rule you create is in enabled state. By default, rules are in enabled state. To disable the rule, you can select **Disabled** from the Status list.
8. In the Condition Builder section, click the icon to the right of the Condition field to open the Condition Builder dialog box to start building your condition. The Condition Builder dialog box enables you to search and navigate through all the attributes so that you can select them to include in your rule condition.
9. Search for an entity type based on which you want to specify the condition, for example User.
10. Click **User**. The user attributes are displayed.
11. Search for the user attribute that you want to include in the rule condition, for example, Manager Display Name. Alternatively, you can navigate through the user attributes by clicking the page number icons, and then select the attribute.

    Click **OK**. The following expression is added in the Condition field:

    ```
    user.Manager Display Name
    ```
12. From the list of operators, select an operator, such as EQUAL.
13. In the right hand side field, enter the Manager Display Name, for example, Sony Palmentieri. Alternatively, you can click the icon adjacent to the field to open the Condition Builder dialog box. To specify the Manager Display Name, select any one of the following:
    - **Value:** Selecting this option enables you to select a specific value for the attribute.

      > **Note:**
      >
      > If you select value, based on the left hand side, only the values for that field are displayed. However, the values are not displayed for all attributes. For some attributes, the value must be entered.

    - **Expression:** Selecting this option enables you to specify an expression based on the selected attribute, for example `$(user.Country)`.

Search and select the desired value, and click **OK**. The value is added to the right hand side field, and adding the first line of the rule condition is complete.

> **Note:**
>
> You can enter an expression in the rule condition fields instead of searching and selecting the values.

14. To add another line to the rule condition, click **Add Condition**.

    To remove a line from the rule condition, you can select the checkbox to the left of the line, and then click **Remove**. You can select multiple checkboxes to remove those lines at a time.

15. From the operators list to the right of the first line, select **AND**. This is to specify that both the first and second lines must be true.

16. In the left hand side field, enter the expression or search and select the attribute. For the purpose of this example, specify `user.Job Title`. Select the `EQUAL` operator, and specify a value for the Job Title attribute in the right hand side field, for example, Administrator.

17. Add another line and specify the following:

    ```
    user.Organization Name EQUAL Avitek
    ```

18. To group the first two lines together, select the checkboxes adjacent to the first two lines, and click **Group**.

    You can ungroup the lines by selecting the checkboxes adjacent to the lines and clicking **Ungroup**.

> **Note:**
>
> You can group only two conditions at a time. If you select more than two conditions, then the **Group** button is disabled. Alternatively, the **Ungroup** button is enabled only when you select one of the conditions that is grouped, but it is disabled when you select more than one group.

19. Add the fourth line, and click the icon to the right of the condition field to open the Condition Builder dialog box.

20. To add an entitlement, make the following selections:

    a. Select **Application**. The application types are displayed.

    b. Then select the resource, for example eBusiness Suite User. click **appinstance**.

    c. Select **Vision Purchasing** as the application instance.

    d. Select **account** as you are selecting an entitlement, and select wildcard character * to specify all accounts.

       Click the arrow in the first row to go back, and then select **UD_EBS_RESP** as the entitlement, and select wildcard character * to specify all responsibilities.

> **Note:**
>
> For application instances, there is no mechanism to filter out the attributes. All the attributes for application instances are displayed in the Condition Builder with which a rule can be written.
>
> For roles, select the role name to display the list of attributes for the role entities. You can select the asterisk (*) wildcard character to display the list of attributes.

e. Select **Responsibility Name**.

   Note that the selection is displayed at the top of the dialog box, as follows:

   ```
   Home > appType[eBusiness Suite User].appinstance[Vision
   Purchasing].account[*].UD_EBS_RESP[*].Responsibility Name
   ```

f. Click **OK**. The expression is added in the condition field.

g. Select EQUAL and specify a value for the Responsibility Name, such as `9~170~52448`.

21. Add another line, and add an expression for the entitlement of the AD User resource in the condition field. The expression can look similar to the following:

    ```
    appType[AD
    User].appinstance[VisionEmployeesDomain].account[*].UD_ADUSRC[*].catalog.Disp
    lay Name
    ```

22. Select EQUAL and specify a value for the Display Name, such as CN=Account Operators,CN=Builtin,DC=adlrg,DC=us,DC=mydomain,DC=com.

23. Group the fourth and fifth lines and specify OR operator between them. If you do not specify an operator, then it is taken to be AND by default.

24. Join the first and second groups with an AND operator.

> **Note:**
>
> A maximum of two conditions can be grouped together. Therefore, if you create a rule with four conditions that are grouped together with the AND operator, then the conditions are grouped into two sets. But if one of the conditions are grouped with the OR operator, then rule is updated correctly.

25. Click **Create**. The rule is created and the Rules page is displayed. To display the rule you created in the search result of the Rules page, you can click **Refresh**.

> **Note:**
>
> When Risk attributes are used to define the conditions in a rule, for the rule to be evaluated correctly, the Risk Aggregation Job scheduled job must be run before the request is made.

14.5.3 Understanding Identity Audit Rule Expressions

Some sample identity audit rules include rules for testing the group name attribute, finding conflicting attribute values within a single entitlement in a single account, and finding conflicting attribute values within the same account.

This section describes the following sample Identity Audit rules:

- There are restrictions on how rules can be written when their conditions involve account entitlements. Identity Audit rules that use catalog-based conditions do not produce matches if the entitlements are being requested as child form data in a new/modify account request. For example, if a user requests an ActiveDirectory group entitlement as part of an account request in the AD Group form, then the following rule operand does not match the name of the AD group:

  ```
  appType[AD
  User].appInstance[VisionADAppInst].account[*].UD_ADUSRC[*].catalog.Display Name
  ```

  To work around this restriction, the operand must be testing for the group name attribute (Group Name) directly, as shown:

  ```
  appType[AD User].appInstance[VisionADAppInst].account[*].UD_ADUSRC[*].Group Name
  ```

- The following rule shows how to find conflicting attribute values within a single entitlement in a single account by using the discriminator character `#`:

  ```
  appType[*].appInstance[*].account[#x].UD_VISDUMC[#x].VISDUM lookup ==
  8~CN=VISDUM1,DC=abc,DC=com
  AND
  appType[*].appInstance[*].account[#x].UD_VISDUMC[#x].ss == admin
  ```

  In this example, both the rule conditions reference the same entitlement (in bold).

- The following rule shows how to find conflicting attribute values within the same account by using the discriminator to pin the account instance:

  ```
  appType[AD User].appInstance[VisionADAppInst].account[#x].Organization Name ==
  6~OU=Vision,DC=oia,DC=mydomain,DC=com
  AND
  appType[AD User].appInstance[VisionADAppInst].account[#x].Department == avitek
  ```

14.5.4 Modifying Identity Audit Rules

Modifying identity audit rules involves searching and opening the rule, and then using the Condition Builder to edit the rule conditions.

To modify a rule:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Rules**. The Rules page is displayed.
3. Search for the rule that you want to modify. See Searching Identity Audit Rules for information about searching rules.
4. Open the rule that you want to modify in one of the following ways:
   - Click the rule name.
   - Select the rule by clicking to the left of the row. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar.

The Edit Rule page is displayed. You can modify any attributes in this page, add/modify/delete the rule conditions, or group/ungroup the rule conditions.

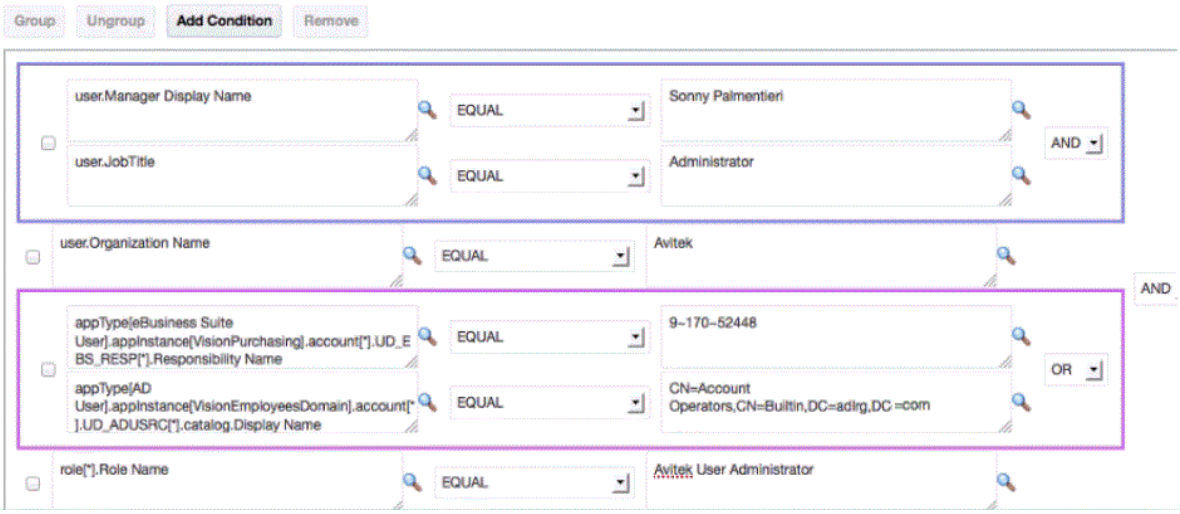
5. (Optional) For the purpose of the example used in Creating Identity Audit Rules, add a line with a rule condition for roles. Specify the rule condition as:

```
role[*].Role Name EQUAL Avitek User Administrator
```

See Creating Identity Audit Rules for information about adding rule conditions and grouping them.

6. Specify the AND operator between the second group and the last line. If you do not specify an operator, then it is taken to be AND by default. The rule conditions will look similar to Figure 14-1.

Figure 14-1 Rule Conditions



7. Click **Update**.

14.5.5 Duplicating Identity Audit Rules

You can use the rule conditions specified for a rule in another rule by duplicating the rule.

To duplicate a rule:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Rules**. The Rules page is displayed.
3. Search for the rule that you want to duplicate. See Searching Identity Audit Rules for information about searching rules.
4. Select the rule by clicking to the left of the row.
5. From the Actions menu, select **Duplicate**. Alternatively, click **Duplicate** on the toolbar. A duplicate of the selected rule is created with a number appended to the rule name.

   You can modify the duplicated rule to create a new rule.

14.5.6 Deleting Identity Audit Rules

You can delete a rule if no policies or policy violations are associated with the rule.

To delete a rule:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Rules**. The Rules page is displayed.
3. Search for the rule that you want to delete. See Searching Identity Audit Rules for information about searching rules.
4. Select the rule that you want to delete by clicking to the left of the row.
5. From the Actions menu, select Delete. Alternatively, click Delete on the toolbar.

   A message box is displayed asking for confirmation.
6. Click **Yes** to confirm.

14.6 Managing Identity Audit Policies

Managing identity audit policies involves searching, creating, modifying, duplicating, and deleting identity audit policies, and previewing the results of identity audit policies.

This section describes how to create and manage identity audit policies. It contains the following sections:

- Searching Identity Audit Policies
- Creating Identity Audit Policies
- Modifying Identity Audit Policies
- Duplicating Identity Audit Policies
- Deleting Identity Audit Policies
- Previewing the Results of Identity Audit Policies

14.6.1 Searching Identity Audit Policies

You can perform basic and advanced search for identity audit policies in the Policies page of Identity Self Service.

This section describes how to perform basic search and advanced search for identity audit policies:

- Performing Basic Search for Identity Audit Policies
- Performing Advanced Search for Identity Audit Policies

14.6.1.1 Performing Basic Search for Identity Audit Policies

To perform a basic search for Identity Audit policies:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Policies**. The Policies page is displayed.

3. If fields for advanced search is displayed, then click **Basic**. Otherwise, ignore this step and continue with step 4.
4. From the Search list, select an attribute based on which you can search the policies.
5. In the Search box, enter a value of the selected attribute as the search criterion.
6. Click the Search icon. The search result is displayed in a tabular format.

14.6.1.2 Performing Advanced Search for Identity Audit Policies

To perform an advanced search for policies:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Policies**. The Policies page is displayed.
3. Click **Advanced**. The fields for advanced search are displayed.
4. Select any one of the following:
   - **All:** To specify that the search result must match all the specified search criteria.
   - **Any:** To specify that the search result must match any one of the specified search criteria.
5. Specify values for one or more of the policy attributes. The search result will be displayed based on the values that you specify for these attributes.

   For each attribute, select a search operator from the lists, such as Starts With, Ends With, Equals, Does Not Equal, Contains, and Does Not Contain. For any date field, the search operators are Equals, Before, After, On or before, On or after, Between.
6. Optionally, you can add fields to your search criteria by clicking **Add Fields** and selecting fields from the list. A cross icon is displayed with the added fields. You can click the cross icon to remove the added field.
7. Click **Search**. The search result is displayed in a tabular format.

14.6.2 Creating Identity Audit Policies

You can create identity audit policies by using the Create option from the Policies page of Identity Self Service, and specifying values for the policy attributes and adding one or more rules to the policy.

To create Identity Audit policies:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Policies**. The Policies page is displayed.
3. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Policy page is displayed.
4. Enter values in the fields of the Create Policy page, as described in Table 14-2.

Table 14-2 Fields in the Create Policy Page

Field	Description
Name	The Identity Audit policy name.
Description	The description for the Identity Audit policy.
Status	The status of the Identity Audit policy, which is Enabled by default.
Owner	The display name of the policy owner. Click the search icon adjacent to this field to search and select a policy owner.
Type	The policy type is Identity Audit by default. This value cannot be modified because only policies of type Identity Audit can be created from the Create Policies page.
Severity	Select a severity level, such as High, Medium, or Low, which will be associated with the policy violations generated by this policy.
Evaluate during Requests	Select this option to display the policy violation during user's access request. User can either cancel the request or submit the request with violation.
Disable Close as Risk Accepted Action	Select this option to disable the **Close As Risk Accepted** action for any violation corresponding to the policy.
Workflow Name	The workflow name that will be invoked during a user's access, if you select the **Evaluate during Requests** option. By default, the `default/Identity/AuditRemediation` workflow is selected.
Remediator	Specify a remediator for violations generated by the policy. To do so, select any one of the following: • **User:** Select this option to specify a user as the remediator. Search and select the user by clicking the Search icon. • **Manager:** Select this option if you want the manager of the user for whom the violation is generated to be the remediator. • **Role:** Select this option if you want to specify the members of a certain role to be the remediator. Search and select the role by clicking the Search icon.

5. To add one or more rules to the policy:
   a. Click **Add**. The Add Rule dialog box is displayed.
   b. Search for the rule or rules that you want to add to the policy. To do so, select a rule attribute name from the search list, enter a search criterion on the search field, and click the Search icon. The rules that match the search criterion are listed in the Results table.
   c. Select one or more rules that you want to add to the policy, and click Add Selected. To select all rules, you can click **Add All**. The selected rules are added in the Selected Rules table.
   d. Click **Select**. The selected rules are added to the table in the Create Policy page.
   e. (Optional) To remove any rule from the table in the Create Policy page, select the rule, and click **Remove**.
6. Click **Create**. The policy is created. The policy is listed in the Policies page. You can now run a preview of the policy.

14.6.3 Modifying Identity Audit Policies

Modifying identity audit policies involves searching and opening the policy, and then modifying the values of the policy attributes and adding or removing the rules.

To modify Identity Audit policies:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Policies**. The Policies page is displayed.
3. Search for the policy that you want to modify. See Searching Identity Audit Policies for information about searching policies.
4. Open the policy that you want to modify in one of the following ways:
   - Click the policy name.
   - Select the policy by clicking to the left of the row. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar.

   The Edit Policy page is displayed. You can modify any attributes in this page and add/remove the rules. See Creating Identity Audit Policies for information about adding/removing rules associated with policies.
5. Click **Update**. The policy is modified with the changes.

14.6.4 Duplicating Identity Audit Policies

You can use the rules specified for a policy in another policy by duplicating the policy.

To duplicate a rule:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Policies**. The Policies page is displayed.
3. Search for the rule that you want to duplicate. See Searching Identity Audit Rules for information about searching rules.
4. Select the rule by clicking to the left of the row.
5. From the Actions menu, select **Duplicate**. Alternatively, click **Duplicate** on the toolbar. A duplicate of the selected rule is created with a number appended to the rule name.

   You can modify the duplicated rule to create a new rule.

14.6.5 Deleting Identity Audit Policies

You can delete a rule if no policies or policy violations are associated with the rule.

To delete a rule:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Policies**. The Policies page is displayed.
3. Search for the rule that you want to delete. See Searching Identity Audit Rules for information about searching rules.
4. Select the rule that you want to delete by clicking to the left of the row.

5. From the Actions menu, select Delete. Alternatively, click Delete on the toolbar.

   A message box is displayed asking for confirmation.

6. Click **Yes** to confirm.

14.6.6 Previewing the Results of Identity Audit Policies

You can preview results of the Identity Audit policies to understand the policy violations that will be generated as a result of a scan. When you preview a policy, the policy violations are displayed, but the violations are not assigned to the remediators.

To preview the results of an Identity Audit policy:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Policies**. The Policies page is displayed.
3. Search for the policy that you want to modify. See Searching Identity Audit Policies for information about searching policies.
4. Select the policy that you want to preview.
5. From the Actions menu, select **Preview**. Alternatively, click **Preview** on the toolbar. The Base Selection page is displayed.
6. Select a set of users that you want to scan by selecting any of the following options:
   - **All Organizations:** To specify that all organizations will be scanned.
   - **Selected Organizations:** To specify one or more organizations that will be scanned. After selecting this option, click **Add Organizations**, search and select one or more organizations, and then click **Select**.
   - **All Users:** To specify that all users will be scanned.
   - **User Criteria:** To specify criteria parameters so that users that match the criteria will be scanned. To specify the user criteria:
     a. Under the Criteria Parameters section, select any one of the following:

        All: To specify that all the parameters must match.

        Any: To specify that any one parameter must match.

     b. Enter values in the Manager and Organizations fields.

     c. Optionally, you can click **Advanced** to include more attributes in the criteria.

     d. Click **Update and Preview Results**. The selected criteria is added to the Criteria String section.
   - **Selected Users:** To specify one or more users that will be scanned. After selecting this option, click **Add Users**, search and select one or more users, and then click **Select**.
7. Click **Submit**. The scan is submitted.
8. To view the policy violations detected by the scan, select the policy in the Policies page, and click **View Scans**. Alternatively, from the Actions menu, select **View Scans**.

   The Scans page is displayed with the results of the scan. The scan name, status of the scan, start time, end time, the number of users scanned, and number of violations are displayed in a table.

9. Click the scan name. Alternatively, click **Open**. The Policy Violations page is displayed with a list of all the policy violations.

   The remediator will get the policy violations in the Policy Violations of the Self Service after the scan is run.

10. You can click each policy name to view the policy violation details in the Violation details page. This page has the following sections:

    - **Violation Details:** Displays the details of the policy violation, such as the policy attributes, status, detection count, and the user name for which the violation is generated.
    - **Access Details:** Displays the cause of the violation, the rules that have been violated, the status and attributes of the violation, and comments, if any.

14.7 Managing Scan Definitions

Managing scan definitions involves searching, creating, and modifying scan definitions, and running and viewing scans.

This section describes how to create and manage scan definitions. It contains the following topics:

- Searching Scan Definitions
- Creating Scan Definitions
- Modifying Scan Definitions
- Running and Viewing Scans

14.7.1 Searching Scan Definitions

You can perform basic and advanced search for scan definitions in the Scan Definitions page of Identity Self Service.

This section describes how to perform basic search and advanced search for scan definitions:

- Performing Basic Search for Scan Definitions
- Performing Advanced Search for Scan Definitions

14.7.1.1 Performing Basic Search for Scan Definitions

To perform a basic search for scan definitions:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Scan Definitions**. The Scan Definitions page is displayed.
3. If fields for advanced search is displayed, then click **Basic**. Otherwise, ignore this step and continue with step 4.
4. From the Search list, select an attribute based on which you can search the scan definitions.
5. In the Search box, enter a value of the selected attribute as the search criterion.
6. Click the Search icon. The search result is displayed in a tabular format.

14.7.1.2 Performing Advanced Search for Scan Definitions

To perform an advanced search for scan definitions:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Scan Definitions**. The Scan Definitions page is displayed.
3. Click **Advanced**. The fields for advanced search are displayed.
4. Select any one of the following:
   - **All:** To specify that the search result must match all the specified search criteria.
   - **Any:** To specify that the search result must match any one of the specified search criteria.
5. Specify values for one or more of the attributes. The search result will be displayed based on the values that you specify for these attributes.

   For each attribute, select a search operator from the lists, such as Starts With, Ends With, Equals, Does Not Equal, Contains, and Does Not Contain. For any date field, the search operators are Equals, Before, After, On or before, On or after, Between.
6. Optionally, you can add fields to your search criteria by clicking **Add Fields** and selecting fields from the list. A cross icon is displayed with the added fields. You can click the cross icon to remove the added field.
7. Click **Search**. The search result is displayed in a tabular format.

14.7.2 Creating Scan Definitions

You can create scan definitions by using the Create option from the Scan Definitions page of Identity Self Service, and specifying values, policy selection strategy, base selection, and configuration parameters for the scan definition.

To create scan definitions:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Scan Definitions**. The Scan Definitions page is displayed.
3. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Attributes page of the Create Scan Definitions wizard is displayed.
4. In the General Policy Information section, enter the scan definition name in the Name box. This is a mandatory field.
5. In the Description box, enter a description for the scan definition.
6. In the Owner box, specify the user name of the owner of the scan definition. You can click the Search icon, and search and select a user as the owner. This is a mandatory field.
7. Click **Next**. The Select Policy page of the Create Scan Definitions wizard is displayed.
8. From the Policy Selection Strategy list, select any one of the following options:
   - **All Policies:** Select this option to associate all the Identity Audit policies with the scan definition.

- **Selected Policies:** Select this option to associate the policies you select to associate them with the scan definition. To do so, click **Add Policies**, and search and select a policy.
- **Policy Criteria:** Select this option to specify criteria parameters based on which the policies will be dynamically associated with the scan definition. To do so:
  a. Select any one of the following options:

     All: To specify that all parameters must match.

     Any: To specify that any one parameter must match.

  b. Enter values in the Policy Name and Description fields.

  c. Optionally, you can click **Advanced** to include more attributes in the criteria.

  d. Click **Update and Preview Results**. The selected criteria is added to the Criteria String section.

9. Click **Next**. The Base Selection page of the Create Scan Definitions wizard is displayed.
10. In the Base Selection section, specify the users that you want to scan by using this scan definition. Select a set of users that you want to scan by selecting any of the following options:
    - **All Organizations:** To specify that all organizations will be scanned.
    - **Selected Organizations:** To specify one or more organizations that will be scanned. After selecting this option, click **Add Organizations**, search and select one or more organizations, and then click **Select**.
    - **All Users:** To specify that all users will be scanned.
    - **User Criteria:** To specify criteria parameters so that users that match the criteria will be scanned. To specify the user criteria:
      a. Under the Criteria Parameters section, select any one of the following:

         All: To specify that all the parameters must match.

         Any: To specify that any one parameter must match.

      b. Enter values in the Manager and Organizations fields.

      c. Optionally, you can click **Advanced** to include more attributes in the criteria.

      d. Click **Update and Preview Results**. The selected criteria is added to the Criteria String section.
    - **Selected Users:** To specify one or more users that will be scanned. After selecting this option, click **Add Users**, search and select one or more users, and then click **Select**.
11. Click **Next**. The Configuration page of the Create Scan Definitions wizard is displayed.
12. (Optional) Select the Prevent Self Remediation option if you want to prevent the owner of the scan definition to take remediation action. Then you must specify a different user as the remediator by selecting any one of the following options from the Alternate remediator ID list:

- **User Manager:** To specify the manager of the user for whom the policy violation has been detected as the remediator.
- **Selected User:** To specify a user that you select as the remediator. To do so, click the Search icon, and search and select a user.

13. If you do not want to prevent self remediation, then accept the default settings, and click **Next**. The Summary page of the Create Scan Definitions wizard is displayed.
14. Review the attributes, policies, base selection, and configuration that you specified, and then click **Finish**. The scan definition is created.

After a scan definition is created, when it is run for the first time, a scheduled job is created that can be configured to run periodically.

14.7.3 Modifying Scan Definitions

Modifying scan definitions involves searching and opening the scan definition, and then modifying the values of the scan definition attributes, policies, base selection, and configuration.

To modify scan definitions:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Scan Definitions**. The Scan Definitions page is displayed.
3. Open the scan definition that you want to modify in one of the following ways:
   - Click the scan definition name.
   - Select the scan definition, and click **Open**. Alternatively, from the Actions menu, select **Open**.

   The scan definition details page is displayed.
4. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Attributes page of the Create Scan Definitions wizard is displayed.
5. You can modify the attributes and selections in the Attributes, Policies, Base Selection, and Configuration tabs. See Creating Scan Definitions for information about the options available in these tabs.
6. Click **Apply**. The scan definition is successfully modified.

14.7.4 Running and Viewing Scans

Running a scan can be performed either using the Scheduler section of Identity System Administration or by using the Scan Definitions page of Identity Self Service.

Running a scan can be performed in any one of the following ways:

- From the Scheduler section of Identity System Administration, run the scheduled job that is generated when the scan definition is created. See "Managing the Scheduler" in the *Administering Oracle Identity Governance* for information about scheduled jobs.
- From the Scan Definitions page of the Identity Self Service, as described in this section.

To run a scan based on a scan definition and view the scan:

1. In the Scan Definitions page, select the scan definition that you want to run.

2. Click **Run Now** on the toolbar. When you click this button, the corresponding scan jobs for the selected scan definition run and policy violations are detected. In addition, the policy violations are assigned to the respective remediators.
3. To view the results of the scan job run, select the scan definition, and click **View Scan** on the toolbar. Alternatively, from the Actions menu, select **View Scan**.

   The Scans page is displayed with the results of the scan. The scan name, status of the scan, start time, end time, the number of users scanned, and number of violations are displayed in a table.
4. Click the scan name. The Policy Violations page is displayed with a list of all the policy violations.
5. You can click each policy name to view the policy violation details in the Violation details page. This page has the following sections:
   - **Violation Details:** Displays the details of the policy violation, such as the policy attributes, status, detection count, and the user name for which the violation is generated.
   - **Access Details:** Displays the cause of the violation, the rules that have been violated, the status and attributes of the violation, and comments, if any. This section allows you to either close the violation or request of remediation.
6. Close the Violation Details page.

14.8 Managing Policy Violations

Managing policy violations involves searching, opening, completing, and closing policy violations, remediating or closing policy violation causes, and generating policy violation reports.

This section describes how to manage identity audit policy violations from the Policy Violations page. It contains the following topics:

- Introducing Identity Audit Policy Violation Page in Identity Self Service
- Searching Policy Violations
- Opening Policy Violation Details
- Completing Policy Violations
- Closing Policy Violations
- Remediating or Closing Policy Violations Causes
- Generating Identity Audit Policy Violation Reports

14.8.1 Introducing Identity Audit Policy Violation Page in Identity Self Service

You can manage identity audit policy violations either by using the Pending Violations page or by using the Policy Violations page of Identity Self Service.

Identity audit policy violations can be managed from the following sections of Identity Self Service:

Pending Violations page: As a remediator of identity audit policy violations that are assigned to you, you can access the pending violations and take action on them by using the Pending Violations page. See Managing Pending Violations for details.

Policy Violations page: You can view and take actions on the identity audit policy violations for administrative purpose by using the Policy Violations page, which you can open from the Compliance tab of the Identity Self Service.

14.8.2 Searching Policy Violations

You can perform basic and advanced search for policy violations in the Policy Violations page of Identity Self Service.

This section describes how to perform basic search and advanced search for policy violations:

- Performing Basic Search for Policy Violations
- Performing Advanced Search for Policy Violations

14.8.2.1 Performing Basic Search for Policy Violations

To perform a basic search for policy violations:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Policy Violations**. The Policy Violations page is displayed.
3. If fields for advanced search is displayed, then click **Basic**. Otherwise, ignore this step and continue with step 4.
4. From the Search list, select an attribute based on which you can search the policy violations.
5. In the Search box, enter a value of the selected attribute as the search criterion.
6. Click the Search icon. The search result is displayed in a tabular format.

14.8.2.2 Performing Advanced Search for Policy Violations

To perform an advanced search for policy violations:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Policy Violations**. The Policy Violations page is displayed.
3. Click **Advanced**. The fields for advanced search are displayed.
4. Select any one of the following:
   - **All:** To specify that the search result must match all the specified search criteria.
   - **Any:** To specify that the search result must match any one of the specified search criteria.
5. Specify values for one or more of the attributes. The search result will be displayed based on the values that you specify for these attributes.

For each attribute, select a search operator from the lists, such as Starts With, Ends With, Equals, Does Not Equal, Contains, and Does Not Contain. For any date field, the search operators are Equals, Before, After, On or before, On or after, Between.

6. Optionally, you can add fields to your search criteria by clicking **Add Fields** and selecting fields from the list. A cross icon is displayed with the added fields. You can click the cross icon to remove the added field.
7. Click **Search**. The search result is displayed in a tabular format.

14.8.3 Opening Policy Violation Details

Before taking action on policy violations, the remediator must open the policy violation and review the details.

To open a policy violation:

1. In Identity Self Service, click the **Compliance** tab.
2. Click the **Identity Audit** box, and select **Policy Violations**. The Policy Violations page is displayed.
3. You can click each policy name to view the policy violation details in the Violation details page.

   In the Violation details page, you can take action on the policy violations, such as remediate, close, or complete the violation. For information about the actions you can take on the policy violation, see Remediating or Closing Policy Violations Causes.
4. Click the **Details** tab, if it is not already active. This tab has the following sections:
   - **Violation Details:** Displays the details of the policy violation, such as the policy attributes, status, detection count, and the user name for which the violation is generated.
   - **Access Details:** Displays the cause of the violation, the rules that have been violated, the status and attributes of the violation, and comments, if any. This section allows you to either close the violation or request for remediation, as described in Remediating or Closing Policy Violations Causes.

     You can place your mouse pointer on the information icon in the Rules Violated column to display a popup with details of the violated rule, such as rule name, description, and rule condition.
5. Click the **Action History** tab. This tab displays all the actions on the policy till the current state.

14.8.4 Completing Policy Violations

Completing policy violations include searching and selecting the policy violations and clicking **Complete**.

To complete policy violations:

1. Open the Policy Violations page, as described in Opening Policy Violation Details.
2. Search for the policy violation you want to complete. See Searching Policy Violations for information about searching policy violations.

3. Select the policy violation you want to complete.
4. To complete a policy violation, open the policy violation details by clicking the policy name, and then click **Complete** in the Details tab.

14.8.5 Closing Policy Violations

Closing policy violations include searching and selecting the policy violations and clicking **Close**.

To close policy violations:

1. Open the Policy Violations page, as described in Opening Policy Violation Details.
2. Search for the policy violation you want to close.
3. Select the policy violation you want to close.
4. From the Actions menu, select **Close**. Alternatively, click **Close** on the toolbar.

14.8.6 Remediating or Closing Policy Violations Causes

Remediating or closing policy violation causes involves three options: **Remediate**, **Close as Fixed**, and **Close as Risk Accepted**.

To remediate or close policy violation causes:

1. Open the policy violation details, as described in Opening Policy Violation Details.
2. In the Details tab, under Access Details, select the violation cause that you want to remediate or close.
3. Perform any one of the following:
   - **Remediate:** To remediate the violation cause, from the Actions menu, select **Request for Remediation**. Alternatively, click **Remediate** on the toolbar. Depending on the actor selected to remediate, such as user, manager, or role, the policy violation cause is assigned to them.
   - **Close as Fixed:** To close the violation cause as fixed, from the Actions menu, select **Close as Fixed**. Alternatively, click **Close** on the toolbar, and then select **Close as Fixed**. The Provide Comments dialog box is displayed. Enter a comment, and click **Submit**.
   - **Close as Risk Accepted:** To close the policy violation cause by accepting the violation risk, from the Actions menu, select **Close as Risk Accepted**. Alternatively, click **Close** on the toolbar, and then select **Close as Risk Accepted**. The Provide Comments dialog box is displayed. In the Expiration Date field, specify a date after which the violation will be re-opened if it still exists. In the Comments field, enter a comment, and click **Submit**.

> **Note:**
>
> During creating a Audit Policy, or modifying the policy, if you have selected the option **Disable Close as Risk Accepted**, action then this option will be disabled.

14.8.7 Generating Identity Audit Policy Violation Reports

Generating identity audit reports involves specifying the report type, report category, and report format.

To generate identity audit policy violation reports:

1. In the Identity Self Service, click the **Compliance** tab.
2. Click the **Reports** box. The Identity Audit Reports page is displayed.
3. From the Report Type list, select the type of report that you want to generate. See "Identity Audit Reports" in the *Administering Oracle Identity Governance* for information about each report type.
4. From the Category list, select any one of the following:
   - **By Remediator:** To generate the report by the remediator of the policy violation reports. Search and select a remediator user by clicking the search icon.
   - **By Scan Stop Date:** To generate the report by the scans run during a specified date range. Specify the dates in the From and To fields.
   - **By Policy:** To generate the report by the identity audit policies. Search and select a policy by clicking the search icon.
   - **By Manager:** To generate the report by the manager of the user entities for which policy violation occurred. Search and select the manager user by clicking the search icon.
   - **By User:** To generate the report by the user for which policy violation occurred. Search and select a user by clicking the search icon.
5. From the Report Format list, select a report format. The available report formats are PDF, HTML, and Excel.
6. Click **Generate**. The report is generated, which you can open or download.
7. Optionally, you can click **Email Me** if you want the report to be sent via mail to a specified email address. Specify the details about the email, such as email address, subject of the mail, and body of the email. Click **OK**.

Part IV
Working with Identity Administration

This part describes Oracle Identity Manager delegated administration functionalities by using the identity administration features.

It contains the following chapters:

- Managing Users
- Managing Roles
- Managing Access Policies
- Managing Organizations
- Managing Administration Roles
- Managing Password Policies
- Managing Application Onboarding
- Managing the Scheduler
- Managing System Properties

15
Managing Users

The user management feature in Oracle Identity Manager includes creating, updating, deleting, enabling and disabling, resetting passwords, locking, and unlocking of user accounts.

You can perform the following user management tasks by using Oracle Identity Self Service:

- Searching Users
- Creating a User
- Viewing User Details
- Modifying Users
- Disabling a User
- Enabling a User
- Deleting a User
- Locking a User Account
- Unlocking a User Account
- Resetting the User Password

15.1 Searching Users

Use the Users page to perform simple and advanced search for users.

To search for users, you can perform one of the following:

- Performing Basic Search for Users
- Performing Advanced Search for Users
- Operations on Search Results

15.1.1 Performing Basic Search for Users

1. Log in to Identity Self Service.
2. Click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
3. To perform basic search, select any one of the following search criteria from the **Search** drop-down and click **Search** icon:
   - User Login
   - First Name
   - Last Name
   - Identity Status
   - E-mail

- Start Date
- End Date
- Display Name
- Account Status
- Organization

It lists the Users that match the selected Search Criteria.

15.1.2 Performing Advanced Search for Users

To perform advanced search:

1. Log in to Identity Self Service.
2. Click **Manage**, click **Users**. The Users page is displayed.
3. Click **Advance** link. Advance Users search page is displayed.
4. Select any one of the following options.
   - **All:** On selecting this option, the search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.
   - **Any:** On selecting this option, the search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.
5. In the searchable user attribute fields, such as User Login, specify a value. You can include wildcard characters (*) in the attribute value.

   For some attributes, select the attribute value from the list. For example, to search all users with locked accounts, select **Locked** from the Account Status list.
6. For each attribute value that you specify, select a search operator from the list.

   The following search operators are available for String type of attributes:
   - Starts with
   - Ends with
   - Equals
   - Does not equal
   - Contains
   - Does not contain

   The following search operators are available for Date type of attributes:
   - Equals
   - Before
   - After
   - On or before
   - On or after
   - Between

The search operator can be combined with wildcard characters to specify a search condition. The asterisk (*) character is used as a wildcard character. For example, you can specify the value of the User Login attribute to be Jo* as the search criteria, and select Equals as the search operator. The users with login names that begins with Jo are displayed.

7. To add a searchable user attribute to the Search Users page, click **Add Fields**, and select the attribute from the list of attributes.

   For example, if you want to search all users with the Country attribute as US, then you can add the Country attribute as a searchable field and specify a search condition.

   > **Note:**
   >
   > You can configure the attributes that are searchable. The attributes available for search must be a subset of the attributes defined for the user entity that are marked with the Searchable = Yes property.

8. Optionally click **Reset** to reset the search conditions and values that you specified. Typically, you perform this step to remove the specified search conditions and specify a new search condition.
9. Click **Search**. The search results is displayed in a tabular format.
10. If you want to hide columns in the search results table, then perform the following steps:
    a. Click **View** on the toolbar, select **Columns**, **Manage Columns**. The Manage Columns dialog box is displayed.
    b. From the Visible Columns list, select the columns that you want to hide.
    c. Click the left arrow icon to add the columns in the Hidden Columns list.
    d. Click **OK**. The selected columns are not displayed in the search results. A status message displays along the bottom of the search table to identify how many columns are currently hidden.

15.1.3 Operations on Search Results

This section describes the operations that you can perform based on selection of row(s) in the search results table. It is divided into single selection operations and multiple selection operations.

You can perform the following single selection operations by selecting a user from the search results table:

- View detail
- Modify
- Enable, only if the user status is disabled
- Disable, only if the user status is enabled
- Lock, only if the selected user's account is unlocked
- Unlock, only if the selected user's account is locked
- Reset password
- Delete

You can perform the following multiple selection operations by selecting multiple users from the search results table:

- Modify
- Enable, only if the user status is disabled
- Disable, only if the user status is enabled
- Lock, only if the selected user's account is unlocked
- Unlock, only if the selected user's account is locked
- Delete

15.2 Creating a User

You can create a new user in Oracle Identity Manager by using the Create User page. You can open this page only if you are authorized to create users as determined by the authorization policy on the Create User privilege on any organization in Oracle Identity Manager.

To create a user:

1. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
2. 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.
3. Enter details of the user in the Create User page.

   Table 15-1 describes the fields in the Create User page:

Table 15-1 Fields in the Create User Page

Section	Field	Description
Justification and Effective Date	Justification	Justification for creating the user.
Justification and Effective Date	Start Date	Date on which the user must be created.
Justification and Effective Date	Stop Date	Date till which the user must be active.
Basic Information	First Name	First name of the user.
Basic Information	Middle Name	Middle name of the user.
Basic Information	Last Name	Last name of the user.
Basic Information	E-mail	E-mail address of the user.
Basic Information	Manager	The reporting manager of the user.
Basic Information	Organization	The organization to which the user belongs. This is also known as the home organization.
Basic Information	User Type	The type of employee, such as consultant, contractor, contingent worker, employee, full-time employee, intern, non-worker, other, part-time employee, or temporary.

Table 15-1 (Cont.) Fields in the Create User Page

Section	Field	Description
Basic Information	Display Name	It can have localized values, which can be added by clicking Manage Localizations, and selecting from a list of languages. Display Name is available in 33 languages.
Account Settings	User Login	The user name to be specified for logging in to the Administration Console.
Account Settings	Password	The password to be specified for logging in to the Administration console.
Account Settings	Confirm Password	Re-enter the password to be specified for logging in to the Administration console.
Account Effective Dates	Start Date	The date when the user will be activated in the system.
Account Effective Dates	End Date	The date when the user will be deactivated in the system.
Contact Information	Telephone Number	The telephone number of the user.
Contact Information	Home Phone	The telephone number of the user's residence.
Contact Information	Fax	The fax number of the user.
Contact Information	Mobile	The mobile number of the user.
Contact Information	Pager	The pager number of the user.
Contact Information	Home Postal Address	The postal address of the user's residence.
Contact Information	Postal Address	The postal address of the user.
Contact Information	Postal Code	The postal code number of the user's address.
Contact Information	PO Box	The post box number of the user's address.
Contact Information	State	The state name of the user.
Contact Information	Street	The street name where the user resides.
Contact Information	Country	The country where user resides.
Preferences	Locale	The locale code of the user.
Preferences	Timezone	The timezone of the user.
Other Attributes	Common Name	The common name of the user.
Other Attributes	Department Number	The department number of the user.
Other Attributes	Employee Number	The employee number of the user.
Other Attributes	Generation Qualifier	Whether the user qualifies the generation.
Other Attributes	Hire Date	The hiring date of the user.
Other Attributes	Locality Name	The name of the locality where user resides.
Other Attributes	Initials	The initials of the user.
Other Attributes	Title	The title for the user.

4. Click **Submit** or **Save as Draft.** A message is displayed stating that the user is created successfully.

> **Tip:**
>
> Users can be created by any one of the following methods:
>
> - By using Oracle Identity Administration
> - By self registration
> - By using SCIM-based APIs
>
> For all the above methods, Oracle Identity Manager uses the default password policy or Password Policy against Default Rule. If you want to use a different password policy, then you must attach the new password policy to the default rule. To do so, see Managing Password Policies.
>
> For more information about how to use SCIM/REST services, see "Using SCIM/REST Services" in the *Developing and Customizing Applications for Oracle Identity Governance*.

15.3 Viewing User Details

The view user operation allows you to view detailed user profile information in the User Details page. You can open this page if you are authorized to view the user's profile as determined by the authorization policy through the View User Details privilege.

To display user details:

1. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
2. Search for the user for which you want to display the details. Follow steps shown in Searching Users.
3. The user details are displayed in the following tabs:
   - **The Attributes Tab:** Displays the attribute profile that includes details about basic user information, account effective dates, and provisioning dates. For more details, see "Editing User Attributes".
   - **The Roles Tab:** Displays a list of roles to which the user belongs. You can click each role to display summary information about the role.

     In the Roles tab, you can assign roles to the user and remove roles from the user. For more information, see Requesting, Removing, and Modifying Roles.
   - **The Entitlements Tab:** Displays a list of entitlements for the user. You can click each entitlement to display a summary of the entitlement.

     In the Entitlements tab, you can request for entitlements and remove entitlements from the user. For more information, see Requesting and Removing Entitlements.
   - **The Accounts Tab:** Displays a list of accounts for the user. You can click each account to display a summary of the account.

     Typical tasks you perform in this tab are request for an account, modify and remove accounts, mark an account as primary, and disable and enable accounts. For more information, see Requesting, Removing, and Modifying Accounts.

- **The Direct Reports Tab:** Displays a read-only table of users for whom the user is set as the manager. In other words, this tab lists the direct reportees of the user. For each user in the table, it displays the following:
  - Display Name
  - User Login
  - Identity Status
  - Organization

  If you select a row in the table, then summary information about the direct reportee is displayed at the bottom.

  Direct reports allows you to open the user details of the direct reportees. To do so, select a row in the table of direct reportees, and click the open icon on the toolbar.
- **The Admin Roles Tab:** Displays a list of admin roles assigned to the user. You can select an admin role to display a summary of the admin role.

  Using the admin role detail information, you can select or deselect the **include sub-orgs** option. When this option is selected, it specifies that the admin role is applicable to the users of the organization and all the suborganizations of the organization. When this option is not selected, it specifies that the admin role is applicable to the users of the organization only. For more information, see Managing Admin Roles.
- **Proxy Users Tab**: The **Proxy Users** tab allows you to view and manage the proxy information. It displays the proxies currently set up within Oracle Identity Manager for you, and also allows you to view previously set up proxies. The past proxies view, which displays all proxies that were added in the past, is read-only, and no modifications are allowed.
  The existing proxy view allows you to cancel an upcoming proxy whose start date is in the future. You can also edit only the end date of an in-progress proxy whose start date is in the past and end date is in future.

  > **Note:**
  >
  > The **Proxy Users** tab is visible only for users with the required admin role capabilities. For details, see List of Authorization Functional Capabilities.

  For more information, see Managing Proxies.

15.4 Modifying Users

You can perform administrative user modification tasks from the user details. The modification is broken up across the different tabs in the page that displays user details, which means that modifications done in each tab are independent of each other and must be saved individually.

> **Note:**
>
> The modify user operation can be a direct operation or generate a request, which is subject to approval, based on the authorization privileges you have.

- Editing User Attributes
- Requesting, Removing, and Modifying Roles
- Requesting and Removing Entitlements
- Requesting, Removing, and Modifying Accounts
- Modifying Details of Direct Reports
- Managing Proxies

15.4.1 Editing User Attributes

You can modify the user attributes from the Attribute tab.

To edit the attributes of a user:

1. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
2. Search for the user for which you want to display the details. Follow steps shown in Searching Users.
3. Select the user in the search results table.
4. Modify the user in one of the following ways:
   - Click **Edit** on the toolbar.
   - From the Actions menu, select **Edit.**
   - Click the user login link. In the user details page, click **Modify**.
5. In the Modify User page, change values of the attributes in the respective fields as required.
6. Click **Submit**. The modify attribute operation is completed successfully.

15.4.2 Requesting, Removing, and Modifying Roles

You can request for new roles, modify the roles associated with the user, remove roles or modify the role grant duration from the Roles tab.

You can perform the following operations from the Roles tab of the User Details page:

- Requesting Roles for a User
- Modifying a Role
- Removing Roles from a User
- Modifying Role Grant Duration

15.4.2.1 Requesting Roles for a User

In the Roles tab of the User Details page, you can add and remove roles. To assign roles to a user:

1. In the User Details page, click the **Roles** tab. The Roles tab is displayed with the list of roles assigned to the user.

   Click the **Granted** tab to view the roles that are granted to you. This includes both direct and indirect roles.

Click the **Pending** tab to view the roles that are pending for approval.

2. From the Actions menu, select **Request**. Alternatively, you can click **Request** on the toolbar. The Catalog page is displayed.
3. Click the search icon next to the Catalog field. A list of catalog items available for requesting is displayed.

> **Note:**
>
> The catalog items that are available for requesting by a user is governed by authorization privileges defined for the admin roles of the user.

4. Select the catalog item for the role that you want to request.
5. Click **Add Selected to Cart**. The selected role catalog item is added to the request cart.
6. Click **Checkout**. The role will be assigned to the user when an approver approves the request.

   You can edit the catalog item by clicking **View & Edit**.

15.4.2.2 Modifying a Role

To modify a role assigned to a user:

1. In the User Details page, click the **Roles** tab.
2. Select the role that you want to modify.
3. From the Actions menu, select **Open**. The role details is displayed, which is available for editing.
4. Edit the fields that you want to modify. You can click each tab and modify the role hierarchy, role membership, access policies, and organizations. For more information, see Viewing and Administering Roles.
5. Click **Apply**.

15.4.2.3 Removing Roles from a User

To remove roles from a user:

1. In the User Details page, click the **Roles** tab. The Roles tab is displayed with the list of roles assigned to the user.
2. Select the role that you want to remove.
3. From the Actions menu, select **Remove**. Alternatively, you can click **Remove** on the toolbar. The Remove Roles page is displayed.
4. Fill in the Justification, click **Submit**.

15.4.2.4 Modifying Role Grant Duration

To modify the grant duration fields for the role:

1. In the Roles tab of the User Details page, select a role for which you want to modify the grant duration.

The grant duration fields, Start Date and End Date, are displayed in the Roles tab.

2. From the Actions menu, select **Modify Grant Duration**. The Modify Grant Duration dialog box is displayed.
3. In the Justification box, enter a justification for modifying the start date, or end date, or both.
4. Enter values in any one or both of the following fields:
   - **Start Date:** The start date when the role will be provisioned. This must be a future date. This field is not available for modification if the role is already assigned to you.
   - **End Date:** The end date when the role will be revoked from you.

   For more information about grant duration, see "Adding and Removing Grant Duration".
5. Click **OK**.

   The Start Date and End Date fields in the Roles tab are updated with the values you specified immediately if no approver is assigned else if approver is assigned it is updated after the approval.

15.4.3 Requesting and Removing Entitlements

You can request for new entitlements, remove entitlements or modify the entitlements grant duration from the Entitlements tab.

You can perform the following entitlement modification operations from the Entitlements tab of the User Details page:

- Requesting Entitlements for a User
- Removing Entitlements from a User
- Modifying Entitlement Grant Duration

15.4.3.1 Requesting Entitlements for a User

To request entitlements for a user:

1. In the User Details page, click the **Entitlements** tab. The Entitlements tab is displayed with the list of entitlements assigned to the user.
2. From the Actions menu, select **Request**. Alternatively, you can click **Request** on the toolbar. The Catalog page is displayed.
3. Click the search icon next to the Catalog field. A list of catalog items available for requesting is displayed.

> **Note:**
>
> The catalog items that are available for requesting by a user is governed by authorization privileges defined for the admin roles of the user.

4. Select the catalog item for the entitlement that you want to request.

5. Click **Add Selected to Cart**. The selected entitlement catalog item is added to the request cart.
6. Click **Checkout**. The Cart Details page is displayed.
7. (Optional) For the requested entitlements, enter any additional information as needed. This additional information can be added using a form associated with the entitlement, provided the entitlement forms have been generated or re-generated by system administrators.

   For example, you can enter effective start and end dates for the entitlement. Then, the approver can review and/or modify this additional information and decide whether the entitlements can be provisioned or not. The entitlements will be assigned to the user when the approver approves the request.

15.4.3.2 Removing Entitlements from a User

To remove entitlements from a user:

1. In the User Details page, click the **Entitlements** tab. The Entitlements tab is displayed with the list of entitlements assigned to the user.
2. Select the entitlement that you want to remove.
3. From the Actions menu, select **Remove**. Alternatively, you can click **Remove** on the toolbar. The Remove Entitlement page is displayed.
4. Fill in the justification, and click **Submit**.

15.4.3.3 Modifying Entitlement Grant Duration

To modify the grant duration fields for the entitlement assigned to the open user:

1. In the Entitlements tab of the User Details page, select an entitlement for which you want to modify the grant duration.

   The grant duration fields, Start Date and End Date, are displayed in the Entitlements tab.
2. From the Actions menu, select **Modify Grant Duration**. The Modify Grant Duration dialog box is displayed.
3. In the Justification box, enter a justification for modifying the start date, or end date, or both.
4. Enter values in any one or both of the following fields:
   - **Start Date:** The start date when the entitlement will be provisioned. This must be a future date. This field is not available for modification if the entitlement is already assigned to the user.
   - **End Date:** The end date when the entitlement will be revoked from the user.

   For more information, see Adding and Removing Grant Duration.
5. Click **OK**.

   The **Start Date** and **End Date** fields in the **Entitlements** tab are updated with the values you specified immediately if no approver is assigned else if approver is assigned it is updated after the approval.

15.4.4 Requesting, Removing, and Modifying Accounts

You can request for new account, remove an account, modify an account, mark an account as primary account, enable or disable an account, or modify the entitlements grant duration from the Accounts tab.

You can perform the following account modification operations from the Accounts tab of the User Details page:

- Understanding Requesting for an Account
- Modifying an Account
- Removing an Account
- About Multiple Accounts in Single Application Instance
- Marking an Account as Primary
- Disabling an Account
- Enabling an Account
- Modifying Account Grant Duration

15.4.4.1 Understanding Requesting for an Account

This section describes about requesting for an account in the following topic:

- Types of Account
- Requesting for an Account

15.4.4.1.1 Types of Account

You can request accounts by requesting an application instance. You can request for the following types of accounts (application instances):

- **Primary account:** A primary account is the first account created for a user in a target application. In other words, a primary account is the first application instance that is being requested. Oracle Identity Manager supports multiple accounts for a single application instance. The first account that is created is tagged as primary account, and there can be only one primary account for a user. The other accounts (non-primary accounts) are associated with the primary account. When the user requests entitlements, the entitlements are appended to the primary account.
- **Non-primary account:** If a user already has a primary account and requests for another account in the same target application, then that account is a non-primary account. A user can have multiple non-primary accounts, but only one primary account.

> **See Also:**
>
> Marking an Account as Primary for more information on marking an account as primary

15.4.4.1.2 Requesting for an Account

To request for an account:

1. In the User Details page, click the **Accounts** tab. This tab lists the accounts of the user.
2. From the Actions menu, select **Request**. Alternatively, click **Request** on the toolbar. The Catalog page is displayed.
3. Click the search icon next to the Catalog field. A list of catalog items available for requesting is displayed.

> **Note:**
>
> The catalog items that are available for requesting by a user is governed by authorization privileges defined for the admin roles of the user.

4. Select the catalog item for the account that you want to request. In other words, select the application instance that you want to request.
5. Click **Add Selected to Cart**. The selected account catalog item is added to the request cart.
6. Click **Checkout**. The account will be granted to the user when an approver approves the request.

   You can edit the catalog item by clicking **View & Edit.**

15.4.4.2 Modifying an Account

To modify an account for the user:

1. In the **Accounts** tab, select the account that you want to modify.
2. From the **Actions** menu, select **Modify**. The account details is displayed which is available for editing.
3. Edit the fields that you want to modify.
4. Click **Ready to Submit** and then click **Submit.**

15.4.4.3 Removing an Account

To remove an account from the user:

1. In the **Accounts** tab, select the account that you want to modify.
2. From the **Actions** menu, select **Remove**. Alternatively, click **Remove** on the toolbar. The Remove Accounts page is displayed.
3. Click **Submit.**

15.4.4.4 About Multiple Accounts in Single Application Instance

Oracle Identity Manager supports multiple accounts in a single application instance. The first account that is created is tagged as the primary account, and there can be only one primary

account for a user. The other accounts (non-primary accounts) are associated with the primary account.

All types of entitlements are available for request in the request catalog. If the request for an entitlement is approved, it is associated with the primary account and not the non-primary account.

When the user gets provisioned to an application instance, Oracle Identity Manager checks if it is the first account provisioned for the user in that application instance. If so, the account is marked as primary. When existing user accounts are reconciled from application instances, the first account that gets reconciled is marked as primary.

A user can have only one primary account. However, Oracle Identity Manager supports multiple accounts for a single application instance. If the account marked as primary is not supposed to be the actual primary account, you can manually change the primary tag for the account and mark another account as primary. By doing so, you can ensure that when the user requests entitlements, the entitlements are appended to the primary account.

15.4.4.5 Marking an Account as Primary

To mark an account as a primary account:

1. In the **Accounts** tab, select the account that you want to mark as primary.
2. From the **Actions** menu, select **Make Primary**.

   A message is displayed asking for confirmation.
3. Click **Yes** to confirm. The account is marked as primary.

15.4.4.6 Disabling an Account

You can disable an account that is in enabled state. To disable an account:

1. In the **Accounts** tab, select the account that you want to disable.
2. From the **Actions** menu, select **Disable**.
3. Click **Submit.** The account is disabled.

15.4.4.7 Enabling an Account

You can enable an account that is in disabled state. To enable an account:

1. In the **Accounts** tab, select the disabled account that you want to enable.
2. From the **Actions** menu, select **Enable**.
3. Click **Submit.** The account is enabled.

15.4.4.8 Modifying Account Grant Duration

To modify the grant duration fields for the account assigned to the open user:

1. In the Accounts tab of the User Details page, select an account for which you want to modify the grant duration.

   The grant duration fields, Start Date and End Date, are displayed in the Accounts tab.

2. From the Actions menu, select **Modify Grant Duration**. The Modify Grant Duration dialog box is displayed.
3. In the Justification box, enter a justification for modifying the start date, or end date, or both.
4. Enter values in any one or both of the following fields:
   - **Start Date:** The start date when the account will be provisioned. This must be a future date. This field is not available for modification if the account is already assigned to the user.
   - **End Date:** The end date when the account will be revoked from the user.

   For detailed information about grant duration, see Adding and Removing Grant Duration.
5. Click **OK**.

   The Start Date and End Date fields in the Accounts tab are updated with the values you specified immediately if no approver is assigned else if approver is assigned it is updated after the approval.

15.4.5 Modifying Details of Direct Reports

You can modify the direct reportee details from the Direct Reports tab.

The modify the details of direct reports:

1. In the User Details page, click the **Direct Reports** tab. This tab lists the direct reports of the open user.
2. Select the user or direct report you want to modify.
3. From the Actions menu, click **Open.** Alternatively, click **Open** on the toolbar. The User details page of the selected direct report is displayed. Use the toolbar and tabs to modify the details of the direct report.

15.4.6 Managing Proxies

A user can assign another user as a proxy. The **Proxy Users** tab allows you to view and manage the proxy information for the selected user.

> **Note:**
>
> - The **Proxy Users** tab is not available for the Weblogic and OIM Internal user roles.
> - The **Proxy Users** tab is enabled only when the system property `Administrator capability to manage proxies` is set to TRUE. For details, see Default System Properties in Oracle Identity Governance.
> - The **Proxy Users** tab is visible only for users with the required admin role capabilities. For details, see List of Authorization Functional Capabilities.

The **Proxy Users** tab allows you to view and manage the proxy information. It displays the proxies currently set up within Oracle Identity Manager for the user, and also allows users to

view previously set up proxies. The past proxies view, which displays all proxies that were added in the past, is read-only, and no modifications are allowed.

The current proxy view allows you to cancel an upcoming proxy whose start date is in the future. You can also edit only the end date of an in-progress proxy whose start date is in the past and end date is in future.

In the section for current proxies, you can also add new proxies. When adding new proxies, you must specify a start date, an end date, and the proxy user.

This section contains the following topics:

- Adding a Proxy User
- Editing a Proxy User
- Removing a Proxy User

15.4.6.1 Adding a Proxy User

To add a proxy user:

1. In the User Details page, click the **Proxy Users** tab.

   The **Current** section displays a list of users currently set up as proxy. The **Past** section displays a list of past proxies.
2. In the Current section, from the Actions menu, select **Add.** Alternatively, you can click **Add** on the toolbar.

   The **Add Proxy** dialog box is displayed.
3. For Proxy Name, select any one of the following:
   - **Manager:** To specify the user's manager as proxy.
   - **Other User:** To specify any other user as proxy. To do so, click the lookup icon to search for the user you want to specify as proxy. Search for and select the user, and then click **Select** in the Search and select dialog box.
4. In the **Start Date** field, specify a start date. To do so, click the Select Date icon to the right of the Start Date field, and select a date from the calendar.
5. In the **End Date** field, specify an end date.
6. Click **Apply**. The proxy is added to the list of proxies in the Proxies section.

> **Note:**
>
> Oracle Identity Manager does not allow adding another proxy whose start and end dates overlap with the existing proxy.

Oracle Identity Manager will prevent user to add proxy which will result in recursive proxy condition.

Recursive proxy condition is when, User A is proxy for User B (for a time duration, say 17th Nov to 25th Nov), User B is proxy for User C (for a time duration, say 18th Nov to 20th Nov) and during a overlapping time duration (say 19th Nov to 26th Nov) User C is proxy for User A.

An email notification is sent on adding a proxy. The add proxy notification has the following characteristics:

- The date value in the notification is always in GMT timezone.
- The start date and end date value during proxy user creation are based on Oracle Identity Manager server timezone. For example, if the start date is specified as "6/28/2013 00:00:00 PDT", then this value is converted to GMT timezone as "06/28/2013 07:00:00 AM GMT".
- The date format in the notification is always in LONG Date/Time format and cannot be modified in its notification template.

15.4.6.2 Editing a Proxy User

To edit a proxy:

1. In the User Details page, click **Proxy Users** tab.
2. Select a proxy that you want to edit.
3. From the Actions menu, select **Edit.** Alternatively, you can click **Edit** on the toolbar.

   The **Edit Details** dialog box is displayed.
4. In the **Proxy Name** field, select **Manager** to specify the user's manager as proxy. Otherwise, select **Other User** to specify any other user as proxy. You can search for the user name.

   > **Note:**
   >
   > - To change the proxy user, you can search only those users for which you have search permission.
   > - You cannot modify the Proxy Name field for proxy that is in the "In Progress" state.
5. In the Start Date and End Date fields, if required, specify revised dates.

   > **Note:**
   >
   > You cannot modify the Start Date field for a proxy that is in the "In Progress" state.
6. Click **Apply**. The edited proxy information is saved.

15.4.6.3 Removing a Proxy User

To remove a proxy:

1. In the User Details page, select the **Proxy Users** tab.
2. Select the proxy that you want to remove.
3. From the Actions menu, select **Remove**. Alternatively, you can click **Remove** on the toolbar.

When a current proxy is deleted, its end date is set as the date when it is deleted and when a future proxy is deleted, it is removed from the system.

To remove all proxies, click **Remove All** on the toolbar, or select **Remove All** from the Actions menu.

A message is displayed asking for confirmation.

4. Click **Yes**. The selected proxy is removed from the Current section.

15.5 Disabling a User

You can disable a user that is in enabled state from a specific date.

To disable a user:

1. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
2. Search for the user for which you want to display the details. Follow steps shown in Searching Users.
3. Select the user you want to disable.
4. Disable the user in one of the following ways:
   - Click **Disable** on the toolbar.
   - From the Actions menu, select **Disable.**
   - Click the user login of the user record that you want to disable. On the User Details page, click **Disable User** on the toolbar.
5. In the Target Users section, click the plus icon to search for more target users and add to the list of users that you want to disable. You can also view the user details by clicking the **User Details** link for each user.
6. In the Justification and Effective Date section, specify a justification and effective date for disabling the selected user.Click **Submit**. A message is displayed stating that the user is successfully disabled.

15.6 Enabling a User

You can enable a disabled user from a specific date.

To enable a disabled user:

1. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
2. Search for the user for which you want to display the details. Follow steps shown in Searching Users.
3. Select the user you want to enable.
4. Enable the user in one of the following ways:
   - Click **Enable** on the toolbar.
   - From the Actions menu, select **Enable.**
   - Click the user login of the user record that you want to enable. On the User Details page, click **Enable User** on the toolbar.

5. In the Target Users section, click the plus icon to search for more target users and add to the list of users that you want to enable. You can also view the user details by clicking the **User Details** link for each user.
6. In the Justification and Effective Date section, specify a justification and effective date for enabling the selected user.Click **Submit**. A message is displayed stating that the user is successfully enabled.

15.7 Deleting a User

You can delete the user that are not required or are not in use.

To delete a user:

> **Note:**
>
> When a user is deleted, the deleted record would still exist in the database, marked as deleted. These records are not available for any operations.

1. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
2. Search for the user for which you want to display the details. Follow steps shown in Searching Users.
3. Select the user you want to delete.
4. Delete the user in one of the following ways:
   - Click **Delete** on the toolbar.
   - From the Actions menu, select **Delete.**
   - Click the user login of the user record that you want to delete. On the User Details page, click **Delete User** on the toolbar.
5. Verify that the selected user is displayed in the Target Users section.
6. If required, in the Target Users section, click the plus icon to search for more target users and add to the list of users that you want to delete. You can also view the user details by clicking the **User Details** link for each user.
7. In the Justification field, enter a justification for deleting the user.
8. In the Effective Date field, specify a date from which the user account must be removed.
9. Click **Submit**. A request to delete the user is created, which is subject to approval.

15.8 Locking a User Account

You can lock the account of a user from the Users page.

To lock the account of a user:

1. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
2. Search for the user for which you want to display the details. Follow steps shown in Searching Users.

3. Select the user you want to lock.
4. Lock the user in one of the following ways:
   - Click **Lock Account** on the toolbar.
   - From the Actions menu, select **Lock Account.**
   - Click the user login of the user record that you want to lock. On the User Details page, click **Lock Account** on the toolbar.
5. In the confirmation message that is displayed, click **Lock**. The account of the selected user is locked.

> **Note:**
>
> Users with special characters in the user login name cannot be locked.
>
> When you try to lock a user account that contains some special characters in the user login name, the following error is displayed:
>
> `An unknown exception occurred, please review server logs.The user with the key USER_KEY does not exist.`
>
> The following special characters are not allowed in the user login name:
>
> [!@#$%^&*()_-+=[{]}\|;:'",<.>/?

15.9 Unlocking a User Account

You can unlock the account of a user from the Users page.

To unlock the account of a user:

1. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.
2. Search for the user for which you want to display the details. Follow steps shown in Searching Users.
3. Select the user you want to unlock.
4. Unlock the user in one of the following ways:
   - Click **Unlock Account** on the toolbar.
   - From the Actions menu, select **Unlock Account.**
   - Click the user login of the user record that you want to unlock. On the User Details page, click **Unlock Account** on the toolbar.
5. In the confirmation message that is displayed, click **Unlock**. The account of the selected user is unlocked.

15.10 Resetting the User Password

You can reset the user log in password by manually changing it or by auto-generating the password.

To reset the password for a user:

1. In Identity Self Service, click **Manage**.
2. Click the icon in the Users box. The Users page is displayed.
3. Search and select the user for which you want to reset the password.
4. From the Actions menu, select **Reset Password**. Alternatively, you can click **Reset Password** on the toolbar. You can also open the user details, and then click **Reset Password** on the toolbar.

   The Reset Password dialog box is displayed.
5. Select any one of the following options:
   - **Manually change the Password:** To reset the password by entering a new password. To do so, select this option, and enter a new password in the New Password and Confirm Password fields. You can click the information icon to view the criteria to specify a password.

     When you select the **Manually change the Password** option, you can select the **E-mail the new password to the user** option if you want the new password to be sent via e-mail to the user. Otherwise, do not select this option.
   - Auto-generate the Password (Randomly generated): To enable Oracle Identity Manager to generate a random password. When you select this option, the **E-mail the new password to the user** option is selected by default.
6. Click **Reset Password**. The password of the open user is reset.

16

Managing Roles

The role management feature in Oracle Identity Manager provides a Role-based access control capability which make it easier to assign access levels to users and to audit those assignments on an ongoing basis.
This chapter describes about Roles and the different tasks related to roles in the following sections:

- About Roles
- Role Membership Inheritance
- Default Roles
- Creating Roles
- Managing Roles

16.1 About Roles

Roles make it easier to assign access levels to users and to audit those assignments on an ongoing basis.

Oracle Identity Manager provides a comprehensive set of role-based access control capabilities. Role-based access control ensures higher visibility and ease in assigning and unassigning access privileges to users, enforces the notion of least privilege, and enables compliance and audit insight.

Role-based administration typically grows and expands as new situations occur, such as applications are onboarded or phased out, as business requirements evolve. The main advantage of using this approach is ease of implementation and compliance oversight. Role-based administration can be established in a centralized fashion, distributed throughout your network, or hybridized.

Using this feature in Oracle Identity Manager, you can:

- Create, edit, and delete roles via role owner approvals to enforce increased accountability and audit
- Assign users to roles and remove users from roles
- Assign a role as a parent role to an existing role
- View access policies assigned to a role
- Add, edit, or remove user membership rule of a role
- Publish roles to organizations and unpublish roles from organizations
- Make educated decisions to administer role content via advanced role analytics

16.2 Role Membership Inheritance

Oracle Identity Manager supports inheriting the access granted via access policies from the parent role to child role.

This section discusses the following topics:

- About Role Membership Inheritance
- Evaluating Access Granted to User Through Role Inheritance

16.2.1 About Role Membership Inheritance

Membership inheritance means that the members of the inheritor role inherit from the inherited role. For example:

> **Note:**
>
> The role that inherits membership is called the member-inheritor role. The role from which the member-inheritor role inherits membership is called the inherited-member role

- Role B inherits memberships from Role A. Role B is the member-inheritor role to Role A.
- Role C also inherits memberships from Role A. Role C is also a member-inheritor role of Role A.

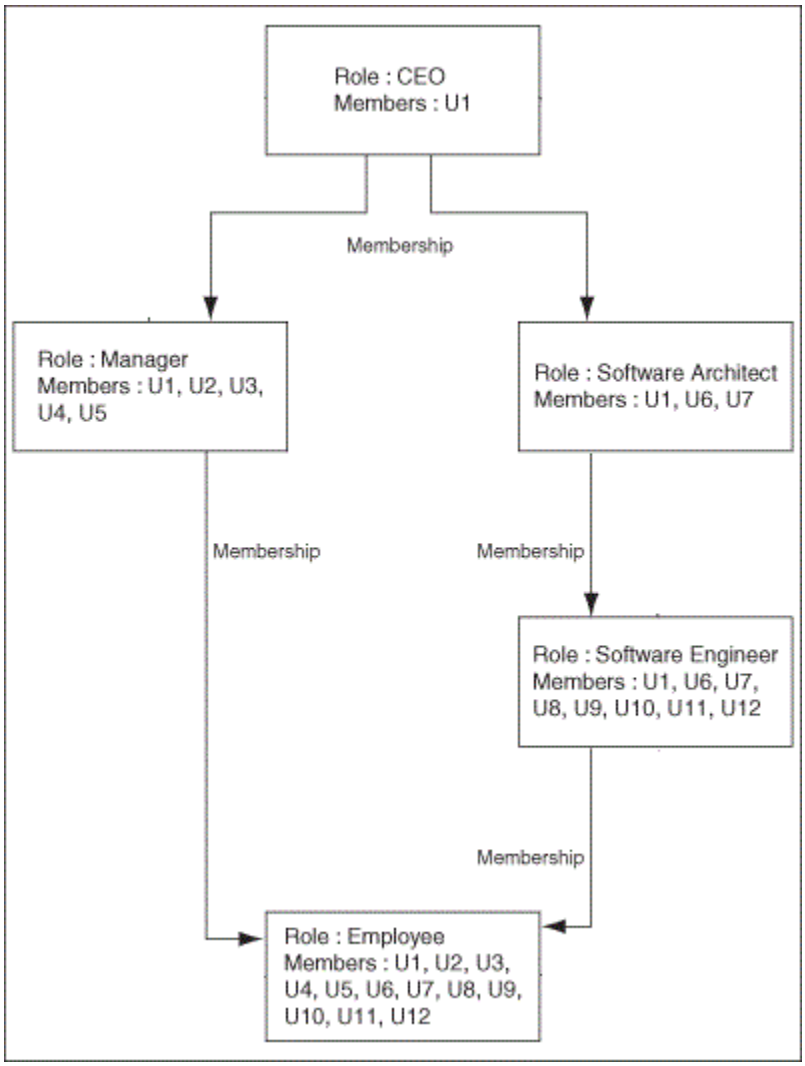
In this example, all members of Role A are also implicit or indirect members of Role B and Role C, but members of Role B are not automatically members of Role A. In other words, Roles B and C are the member-inheritor roles of Role A, and Role A is the inherited-member role of Role B and Role C. A real example for this is that the Employee Role (Role B) inherits memberships from the Manager Role (Role A).

Role membership inheritance is described with the help of the following scenario:

- The role of CEO is an inherited-member role of the Manager role, as a list of managers will include the CEO role.
- The role Manager is an inherited-member role of the Employee role.
- The role Software Architect is an inherited-member role of the Software Engineer role.
- The role Software Engineer is an inherited-member role of the Employee role.
- The Employee role has two inherited-member roles - the Manager role and the Software Engineer role.

Figure 16-1 shows the parent and child roles in this example, along with the membership inheritance:

Figure 16-1 Role Membership Inheritance



Each user in an inherited-member role automatically becomes a member in any of its member-inheritor roles. If that member-inheritor role is itself an inherited-member role, then the user is also added to its member-inheritor roles, and so on. This continues until there are no more member-inheritor roles in the inheritance chain. For example, a CEO is a manager and is automatically a member of the Manager role. Similarly, a manager is automatically an employee. This is why a member added to an inherited-member role gets inherited by its member-inheritor roles, and so on. This explains why the direct membership of the Employee role is empty, and considering membership inheritance, the Employee role has more members than all other roles.

A user can be a member of a role in one of the following ways:

- The member has been inherited from the inherited-member role, which is called indirect membership.
- The user is directly assigned to the role, which is called direct membership.
- The user is directly assigned to the role by using membership rules, which is also called direct membership.

An indirect member can be assigned as a direct member as well. If a user's direct membership in a role is revoked, the user is still a member of that role because of inheritance.

16.2.2 Evaluating Access Granted to User Through Role Inheritance

Inheriting the access granted via access policies from the parent role to child role is enabled by setting **XL.AllowRoleHierarchicalPolicyEval** system property to TRUE. This is explained in the following example:

- Role1 contains Policy1 which contains account A1 and entitlement E1.
- Role2 contains Policy2 which contains account A1 and entitlement E2.
- Role1 is parent role of Role 2.
- If **XL.AllowRoleHierarchicalPolicyEval** is set to TRUE, then when you grant Role2 to User1, User1 will get account A1 and entitlements E1 and E2.
- If **XL.AllowRoleHierarchicalPolicyEval** is set to FALSE, then when you grant Role2 to User 1, User1 will get account A1 and Entitlement E2 (which are part of Role2).

> **Note:**
>
> It is not required to restart the server after this property is changed.

16.3 Default Roles

Oracle Identity Manager supports many default roles that are assigned to internal use only.

In Oracle Identity Manager, the following types of roles are available:

- **Enterprise roles:** These are roles that users (depending on the permissions granted) can create, modify, or delete in Oracle Identity Manager and request for the roles by using the access catalog.
- **Admin roles:** These are predefined roles in Oracle Identity Manager that have a one-to-one mapping with the application roles defined in Oracle Entitlement Server. Admin roles are not visible to the end users. Therefore, admin roles cannot be requested. However, you can create and manage admin roles, as described in Managing Administration Roles .

  Table 16-1 shows the list of default roles in Oracle Identity Manager.

Table 16-1 Default Roles in Oracle Identity Manager

Role	Description
ALL USERS	Members of this role have minimal permissions, including the ability to access the user's own user record. By default, each user belongs to the ALL USERS role.

Table 16-1 (Cont.) Default Roles in Oracle Identity Manager

Role	Description
SYSTEM ADMINISTRATORS	For this role, name and display name are read-only. All other operations are permitted on this role, such as adding/removing parent roles, access policies, organizations, rules, and members. **Note:** By default, XELSYSADM and OIMINTERNAL users are members of this role.
Administrators	This role is for internal use only, meaning it is for Oracle Identity Manager users, and other users can only view it on UI. Oracle WebLogic Server administrator is a member of this role.
OPERATORS	This role is for internal use only, meaning it is for Oracle Identity Manager users, and other users can only view it on UI.
SELF OPERATORS	This role is for internal use only, meaning it is for OIM users, and other users can only view it on UI. No users are associated with this role. **Note:** Oracle Identity Manager recommends that you do not modify the permissions associated with the SELF OPERATORS user role. In addition, you should not assign any users to this role.
BIReportAdministrator	This role is for internal use only, meaning it is for Oracle Identity Manager users, and other users can only view it on UI. This role is an Administrators role for BI Publisher Reports.

16.4 Creating Roles

Using the Create Roles page, you can create a role by providing role details, choosing parent roles, adding access policies to define access rights to the role, adding members to the role, and specifying the organizations to which the role will belong.

> **Note:**
>
> A role, SELF OPERATORS, is added to Oracle Identity Manager by default. No users are associated to this role.
>
> Oracle recommends that you do not modify the permissions associated with the SELF OPERATORS role and do not assign users to this role.

To create a role:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab.
3. Click the **Roles and Access Policies** box.
4. Click **Roles**. The Roles page is displayed.
5. From the **Actions** menu, select **Create**. Alternatively, click **Create** on the toolbar. The Attributes page of the Create Role wizard is displayed.

6. Under General Role Information, specify values for Name, Display Name, Role E-mail, Role Description, and Owned By details.

   By default, the value in the Role Display Name field is populated by the value of the Role Name field. You can change the value if you want.

   If a value of the Owned By field is not specified, then it takes the logged-in user as the role owner.

7. Under Catalog Attributes, specify values for the attributes. These attributes are displayed in the role details of the request catalog. See Requesting New Access for more information about viewing the details of a role in the request catalog.

> **Note:**
>
> A role can be created without role hierarchy, associated access policies, role members and organizations to which the role is published. Therefore, steps 5 through 8 are optional.

8. Click **Next**. The Hierarchy page of the Create Role wizard is displayed.
9. In the Hierarchy page, you can choose parent roles for the role you are creating.

   To inherit permissions from the existing role, click **Add Parent Roles**. The Search Role dialog box is displayed. To search and select a parent role:

   a. From the Search list, select an attribute based on which you want to search the parent role.
   b. In the Search box, enter a value of the selected attribute, and click the Search icon. The asterisk (*) character is used as a wildcard character.

      Roles matching the search criteria are listed.

      If you do not specify a search criterion, all the default roles are listed.
   c. From the list of roles, select the required Role and click **Add Selected**.

      Alternatively, you can add all the listed roles. To do so, click **Add All**.
   d. If you want to deselect any roles from Selected roles list, click **Remove Selected** or **Remove All** options.
   e. Click **Select**. The Define Role Hierarchies panel lists the selected roles.
   f. If you want to undo adding the parent role, then click **Undo** on the toolbar. A warning is displayed. Click **Undo** to confirm.
   g. If you want to remove any parent role, then click **Remove** on the toolbar. A warning is displayed. Click **Remove** to confirm.

> **Note:**
>
> You can click the **Undo** button for undoing the addition of any items in multiple pages of the Create Role wizard. Similarly, you can click the **Remove** button to remove any selected item from multiple pages of the wizard. This is applicable to the Hierarchy, Access Policy, Members, and Organization pages.

h. Click **Next**. The Access Policy page of the Create Role wizard is displayed.

10. In the Select Access Policy panel, you can add access policies to define access rights to this role.

    The access policies that are available for associating with a role are created by using Oracle Identity System Administration. See Managing Access Policies for information about creating and managing access policies.

    To add access policies to the role:

    a. Click **Add Access Policies**. The Add Access Policies dialog box is displayed.

    b. Select the desired search criteria and click the **Search** icon. The access policies that match the search criteria are listed.

    c. From the list of Access Policies, select the required access policy and click **Add Selected** or to add all the listed capabilities click **Add All**.

    d. If you want to deselect any Access Policy from Selected Access Policy list and click **Remove Selected** or **Remove All** options.

    e. Click **Select**. The Define Access Policy panel lists the selected access policies.

       If you want to add more policies or remove policies from this list follow procedure in The Access Policy Tab.

    f. Click **Next**. The Members page of the Create Role wizard is displayed.

11. In the Members page, you can add members to the role either statically by selecting one or more users , dynamically by specifying membership rules or by SQL membership rule.

    To add a member to a role:

    a. Search for Users by using appropriate search criteria and click the Search icon. Users matching the search criteria are listed.

    b. From the list of users select the required user and click **Add Selected** or to add all the listed users click **Add All**.

       If you want to deselect any User from Selected users list click **Remove Selected** or **Remove All** options.

    c. Click **Select**. The Members tab is displayed with the assigned users in the Member Assignment section.

       Select the **Start Date** and **End Date** for with this role is assigned to the user. If you do not specify a value in the **Start Date** field, then the role is assigned immediately as soon as the role is created either directly or after role creation request approval.

       If the **Start Date** is of future then grant will happen on that day, when the *Process Pending Role Grants* job is run, which is scheduled to run daily. On the **End Date** the grant on the role is revoked when the *Process Pending Role Grants* job is run.

    To create membership rules for dynamically assigning members to a role:

    a. Click **Create Membership Rule** to open the User membership rules for role tab.

    b. In the Expression Builder tab, under Attributes tab, select an attribute, such as Country, and then click **Add**. The attribute is added to the expression builder for which you can specify a value. In addition, the Literals tab is displayed.

    c. In the Value field, enter a value for the selected attribute, such as US, and then click **Add**. The value is added to the expression builder. The expression for the membership rule specifies that users with Country as US will be members of the selected role.

d. Click the **Preview Results** tab. The role members that match the expression you specified are listed. You can use this preview for offline impact analysis to view the role members that meet the rule criteria.

e. Click **Save**. The Members tab is displayed with the membership rule added in the User Membership Rule section.

f. If you want the membership rule to be evaluated as soon as the role is created, then select the **Evaluate membership rule now** option.

   If you want to add/remove more role members or membership rules, then perform the procedures described in The Members Tab.

g. Click **Next**. The Organization page of the Create Role wizard is displayed.

To create membership rules for dynamically assigning members to a role using an SQL query:

> **Note:**
>
> - You must enable the property **RoleUserMembershipRuleSQLSupported** to view the **Create SQL Membership Rule** option. You can also enable property **RefreshRoleMembershipJob.EvaluateAllRolesForSQLMembershipRule** to evaluate all SQL membership rule when the **Refresh Role Membership** job is executed. For more information, see Default System Properties in Oracle Identity Governance.
> - If you revert these system properties, then you must first delete the **SQL Membership Rules** that is created for the Role and then revert back.

a. Click **Create SQL Membership Rule** to open the SQL User membership rules for role sample.

b. Under **SQL Query** tab, enter the SQL Query details.

c. Click the **Preview Results** tab. The role members that match the expression you specified are listed. You can use this preview for to view the role members that meet the SQL query rule criteria

   > **Note:**
   >
   > In case the SQL query is incorrect then the results are not displayed.

d. Click **Save**. The Members tab is displayed with the SQL Query added in the **User Membership Rule** section.

e. If you want the membership rule to be evaluated as soon as the role is created, then select the **Evaluate membership rule now** option.

   If you want to add/remove more role members or membership rules, then perform the procedures described in The Members Tab.

f. Click **Next**. The Organization page of the Create Role wizard is displayed.

12. In the Organizations page, you can specify the organizations to which the role will belong. In other words, you can publish the role to one or more organizations. See The Organizations Tab for more information about publishing roles to organizations.

> **Note:**
>
> After you create the Role using the **SQL Membership Rule**, if you delete the rule and want to return to **Membership Rule** for adding the role, then click **Apply** and click **Role** to add using the **Membership Rule**.

To assign organizations:

a. Click **Add Organizations**. The search panel is displayed.

b. From the list of Organizations, select the required organization and click **Add Selected** or to add all the listed organizations click **Add All**.

If you want to deselect any organization from Selected Organization list click **Remove Selected** or **Remove All** options.

c. Click **Select**. The Organizations tab is displayed with the list of Organizations to which this role will be published.

If you want to add more organizations or remove them from this list follow procedure in The Organizations Tab.

d. Click **Next**.The Summary page of the Create Role wizard is displayed.

13. The Summary page displays the role summary information of the role that will be created. Role summary contains all information related to role, such as parent roles, access policies, members, and organizations. The Summary tab also has the **View Analytics** button when the Identity Audit feature is enabled.

Optionally, click **View Analytics** to open the analytic details of the role that is being created. This button is displayed only when the Identity Audit feature is enabled. For detailed information about role analytics, see Displaying Role Analytics.

14. Click **Finish**. The role is created successfully.

Depending on the admin role assignment of the logged-in user and the applicable approval workflow rule, a request is generated, or the role is created directly and the role details page is displayed. In addition, a request is generated when the Identity Audit feature is enabled.

> **Note:**
>
> When role workflows are enabled, the role is created only after all the approvers in the workflow have approved. The role is not created successfully unless approved.
>
> If new members are added, then a separate request is submitted for role grant (which is controlled by its own approval workflow). And if there are multiple grants, then the request is a parent request. On its approval, child requests will be raised for each role grant. Each child request must be approved before the grant happens.

16.5 Managing Roles

You can find roles, add information to them, and perform other administrative functions for roles.

> **Tip:**
>
> Managing role category is deprecated in the current release and any reference to it in this version of Oracle Identity Manager is only for backward compatibility.

This section discusses the following topics:

- Searching for Roles
- Viewing and Administering Roles
- Displaying Role Analytics
- Deleting Roles

16.5.1 Searching for Roles

Use the Roles page to perform simple and advanced search for roles.

To search for Role you can perform one of the following:

- Performing Basic Search for Roles
- Performing Advanced Search for Roles

16.5.1.1 Performing Basic Search for Roles

To perform basic search:

1. Log in to Identity Self Service.
2. Click the **Manage** tab, and then click the **Roles and Access Policies** box. Click **Roles**. The Roles page is displayed.
3. Select any one of the following search criteria from the Search list:
   - Display Name
   - Name
   - Role Namespace
4. In the Search field, enter a search criteria. You can optionally use the asterisk (*) wild card character in the search criteria for basic search. The asterisk (*) character is used as a wildcard character. For example, you can specify the value of the Display Name attribute to be Jo* as the search criteria, and select Equals as the search operator. The roles with Display Name that begins with Jo are displayed.
5. Click the search icon. The roles that match the selected search criteria are listed.

16.5.1.2 Performing Advanced Search for Roles

To perform advanced search:

1. Log in to Identity Self Service.
2. Click the **Manage** tab, and then click the **Roles and Access Policies** box. Click **Roles**. The Roles page is displayed.
3. Click the **Advanced** link. Advance Roles search page is displayed.
4. Select any one of the **Match** options:
   - **All:** On selecting this option, the search is performed with the AND condition. The roles are displayed in search result for which all the search criteria specified have matched.
   - **Any:** On selecting this option, the search is performed with the OR condition. The roles are displayed in search result for which any one of the search criteria specified has matched.
5. In the searchable role attribute fields, such as Display Name, specify a value.

   For some attributes, select the attribute value from the lookup. For example, to search all roles in the Default role category, select Default in the Role Category field.
6. For each attribute value that you specify, select a search operator from the list. The following search operators are available for text type of attributes:
   - Starts with
   - Ends with
   - Equals
   - Does not equal
   - Contains
   - Does not contain
7. To add a searchable role attribute to the Search Roles page, click **Add Fields**, and select the attribute from the list of attributes.

   For example, if you want to search all roles whose description contains `custom admin role` , then select **Role Description** from Add Fields, and specify a search condition as Contains and value as `custom admin role`.

   > **Note:**
   >
   > You can configure the attributes that are searchable. All default and custom-defined searchable role attributes are shown in Add Fields. The searchable attribute are the ones marked with the `Searchable = Yes` property.
8. Optionally click **Reset** to reset the values that you specified as search conditions. Typically, you perform this step to remove the specified search conditions and specify a new search condition.
9. If you want to save the search criteria for future use, then click **Save**. See Using Saved Search for information about creating and managing saved search.

10. Click **Search**. The search results is displayed in a tabular format.
11. If you want to hide columns in the search results table, then perform the following steps:
    a. Click **View** on the toolbar, select **Columns**, **Manage Columns**. The Manage Columns dialog box is displayed.
    b. From the **Visible Columns** list, select the columns that you want to hide.
    c. Click the left arrow icon to add the columns in the **Hidden Columns** list.
    d. Click **OK**. The selected columns are not displayed in the search results.

16.5.2 Viewing and Administering Roles

You can open the details of a role and edit the role attributes, modify the role inheritance and membership, and then publish roles to organization.

The details of the role is displayed in a new page. The role display name is displayed at the top of the page. You can display the details of the role and modify role information in the following tabs of this page:

- Opening Role Page
- About Attributes Tab
- Understanding Hierarchy Tab
- The Access Policy Tab
- The Members Tab
- The Organizations Tab
- The History Tab

> **Note:**
>
> - After you make changes in any one or more of the tabs in the role details page, click **Apply** to save the changes.
> - Depending upon the approval workflow configuration, a request might be generated for any change made to a role.

16.5.2.1 Opening Role Page

You can open the details of a role and edit the role attributes, modify the role inheritance and membership, and then publish roles to organization. To open the details of a role and modify it, perform one of the following:

- In the Search Roles page, search and select the role that you want to open. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar.
- In the search results table of the Search Roles page, click the name of the role.

> **Note:**
>
> After modifications are made to the role, the modifications go through an approval process, if role workflows are configured. Only when the approvers approve, the role changes are reflected in Oracle Identity Manager.

16.5.2.2 About Attributes Tab

The Attributes tab displays the role attributes. Except for the Role Namespace field (which is a read-only field), the rest of the fields in the Attributes tab are same as available in the Create Role page. The Role Namespace field displays the namespace to which the role is assigned.

> **Note:**
>
> Modifying the values of Name and Display Name attribute for default roles, for example OPERATORS, ALL USERS, and SELF OPERATORS, is not supported.

If you modify the attribute values in the Catalog Attributes section, then the modifications are also displayed in Detailed Information section of the corresponding catalog item in the request catalog. See Requesting New Access for more information about viewing the details of a role in the request catalog.

To modify the role attributes, change the values in the fields, and click **Apply**.

> **Note:**
>
> Roles with same names are allowed with different name spaces.

16.5.2.3 Understanding Hierarchy Tab

In the Hierarchy tab, you can perform the following:

- About Role Hierarchy
- Adding a Parent Role to a Child Role
- Removing a Parent Role from a Role
- Displaying Summary Information for Parent/Child Roles

16.5.2.3.1 About Role Hierarchy

The Hierarchy tab displays the role hierarchy information in the following sections:

- **Inherits From:** This section displays the parent roles from which the open role is inherited. The base role has the same permissions and privileges on the members as the inherited roles. Only inherited roles can be added or removed from the base role, but the base role cannot be added or removed from the inherited role.

- **Inherited By:** This section lists the child roles that are inherited by the open role. This is a read-only display of the roles.

16.5.2.3.2 Adding a Parent Role to a Child Role

To add a parent role to a role:

1. Open the role.
2. Click the **Hierarchy** tab. In the Inherits From section, this tab lists the parent roles of the opened role and the opened role inherits the permissions from these parent roles.
3. Verify that Inherits From is active.
4. From the Actions menu, select **Add**. Alternatively, click **Add** on the toolbar. The Search Roles dialog box is displayed.
5. From the Search list, select a role attribute based on which you want to search for the role. Then, select an attribute by using the lookup icon. You can also include wildcard characters (*) in your search criterion. Then, click the search icon. A list of roles that matches your search criterion is displayed.
6. Select one or more roles that you want to add as parent roles. Then, click **Add Selected** to move the selected roles to the Selected Roles list.

   Alternatively, you can click **Add All** to add all the roles in the Selected Roles list.
7. Click **Select**. The selected roles are added as parent roles to the opened role and the role hierarchy is displayed in the Inherits From section of the Hierarchy tab.
8. Select the inherited role that is added. A summary information of the selected role is displayed in a popup.

16.5.2.3.3 Removing a Parent Role from a Role

To remove a parent role from a role:

1. In the Inherits From section of the Hierarchy tab, select the role that you want to remove.
2. From the Actions menu, select **Remove**. Alternatively, click **Remove** on the toolbar. A message box is displayed asking for confirmation.
3. Click **Remove**. Pending action is filled with Remove. Repeat this if you want to remove more than one role. And click **Undo** if you do not want to remove the role that is already marked for removal.
4. Click **Apply**. If workflow is configured, then the inherited roles selected are removed from the Inherits From section of the Hierarchy tab after approval.

16.5.2.3.4 Displaying Summary Information for Parent/Child Roles

You can display read-only summary information of the parent roles from the Inherits From section of the Hierarchy tab. You can also display summary information of the child roles from the Inherited By section.

To display the summary information of a parent/child role:

1. To display the summary of the parent role, in the Inherits From section of the Hierarchy tab, click the Display Name of the role for which you want to display the summary information.

   A popup is displayed with the summary information of the parent role. It displays the role name, role display name, role description, role category, and the user who owns the role.
2. Close the popup.
3. To display the summary of the child role, in the Inherited By section of the Hierarchy tab, click the Display Name of the role for which you want to display the summary information.

   A popup is displayed with the summary information of the child role. It displays the role name, role display name, role description, role category, and the user who owns the role.
4. Close the popup.

16.5.2.4 The Access Policy Tab

The Access Policy tab displays the access policies assigned for the role. In this tab, you can assign the access policies to the role or remove the access policies that are already assigned to the role.

In the Access Policies tab, you can perform the following:

- Adding an Access Policy to a Role
- Removing an Access Policy

16.5.2.4.1 Adding an Access Policy to a Role

To add access policies to a role:

1. From the **Actions** menu, select **Add**. Alternatively, click **Add** on the toolbar.
2. Select the desired search criteria and click the **Search** icon. Access Policies matching the search criteria are listed.
3. From the list of Access Policies, select the required Access Policy and click **Add Selected** or to add all the listed capabilities click **Add All**.
4. If you want to deselect any access policy from the Selected Policies list, then select the access policy from the Selected Policies list, and click **Remove Selected**. You can click **Remove All** to deselect all the selected access policies.
5. Click **Select**. The selected access policies are displayed in the Access Policy tab. Pending action is filled with Add. Repeat this if you want to add more policies. You can click **Undo** if you do not want to add the policy that is already marked with add.
6. Click **Apply**. The request is to be approved if it raises a workflow. Then the selected policies are added to the role.

16.5.2.4.2 Removing an Access Policy

To remove the access policy assigned to this role:

1. From the list of access policies assigned, select the access policy that you want to remove.
2. From the **Actions** menu, select **Remove**. Alternatively, click **Remove** on the toolbar.
3. Click **Remove** to confirm. The selected access policy is removed from the Access Policy tab. Pending action is filled with Remove. Repeat this if you want to remove more

policies. You can click **Undo** if you do not want to remove the policy that is already marked with remove.

4. Click **Apply**. The request is to be approved if it raises a workflow. Then the selected policies are removed from the role.

16.5.2.5 The Members Tab

In the Members tab, you can perform the following:

- About Members Tab
- Assigning Members to a Role
- Revoking Members from a Role
- Adding Membership Rules
- Modifying Membership Rules
- Deleting Membership Rules

16.5.2.5.1 About Members Tab

The Members tab displays the members assigned to the open role. This information is displayed in the following sections:

- **Direct Members:** This section displays the members that are statically assigned to the open role.
- **Rule Based Members:** This section displayed the members that are assigned to the open role via membership rules.
- **Indirect Members:** This section displays the members that are indirectly inherited by the role.
- **All Members:** This section displays all the members, direct and indirect, assigned to the open role.
- **Pending Members:** This section displays all the members that are pending for this role, that is the role assignment date assigned with future start date.

16.5.2.5.2 Assigning Members to a Role

To assign members to a role:

1. In the Direct Members section of the Members tab, click **Add**. The Add Members dialog box is displayed.
2. From the Search list, specify a role attribute name. Enter a search parameter in the search field, and click the search icon. The roles that match the search criteria are displayed.
3. Select the role that you want to assign, and click **Add Selected**. The selected role is added to the Selected Users table.

   To add all the roles to the Selected Users table, click **Add All**.
4. If you want to remove a role from the Selected Users table, then select the role and click Remove Selected. To remove all roles from the Selected Users table, click **Remove All**.

5. Click **Select**. Pending action is filled with Add. Repeat this if you want to add more users. You can click **Undo** if you do not want to add the user that is already marked with add.
6. Click **Apply**. The request is to be approved if it raises a workflow. Then the selected members are added to the role.

16.5.2.5.3 Revoking Members from a Role

To revoke members from a role:

1. In any section of the Members tab, select the member that you want to remove.
2. Click **Remove** on the toolbar. A message is displayed asking for confirmation.
3. Click **Remove** to confirm. Pending action is filled with Remove. Repeat this if you want to remove more users. You can click Undo if you do not want to remove the user that is already marked with remove.
4. Click **Apply**. The request is to be approved if it raises a workflow. Then the selected members are removed from the role.

16.5.2.5.4 Adding Membership Rules

In the Members tab, you can add, modify, or delete the user membership rules or create membership rules for dynamically assigning members to a role using an SQL query. You can specify simple to complex condition expressions as the user membership rule or assign members to a role using an SQL query. When you modify a user membership rule, the existing user memberships are evaluated, and then the existing role memberships that are not valid are revoked and new role memberships are granted.

To add a user membership rule:

1. In the Members tab, click **Create Membership Rule.** The Expression Builder is displayed.
2. In the left pane, verify that <ADD> is selected. This is the placeholder to specify a user attribute for the condition.
3. Under Select Operand Value, in the Attributes tab, select a user attribute, for example, **Country.**
4. Click **Add** to add the attribute to the condition in the left pane.
5. From the list of operators, select a comparator. In Build Expression, select a comparator from the list of operators. If the attribute is of type integer, then comparators, such as = (equals), > (greater than), >= (greater than equal to), < (less than), => (less than equal to), and IN, are displayed.

   If the attribute is of type String, then comparators, such as = (equals), != (not equals), Contains, Starts with, Ends with, and IN, are displayed.
6. Under Select Operand Value, in the Literals tab, specify a value in the Value field, such as `United States of America`.

   When a checkbox or lookup type UDF or default attribute is used in membership rule, then it must be treated as shown in the following example:

```
( ( ( Last Name = "Klein" ) AND ( First Name Contains "Robert" ) )
OR ( ( User Login Starts with "rob" ) AND ( Common Name Ends with "ein" ) )
OR ( ( Robert2UserUDF111DL != "Robert2UserUDF111DL" ) AND ( Robert2UserNumberDL >=
99999 )
```

```
AND ( RobertUserDateDL =< 2013-12-31 ) AND ( Robert2UserchkboxDL = "1" )
AND ( Robert2UserLookupDL IN ["RobertLookUpCode3","RobertLookUpCode9"] ) ) )
```

Here:

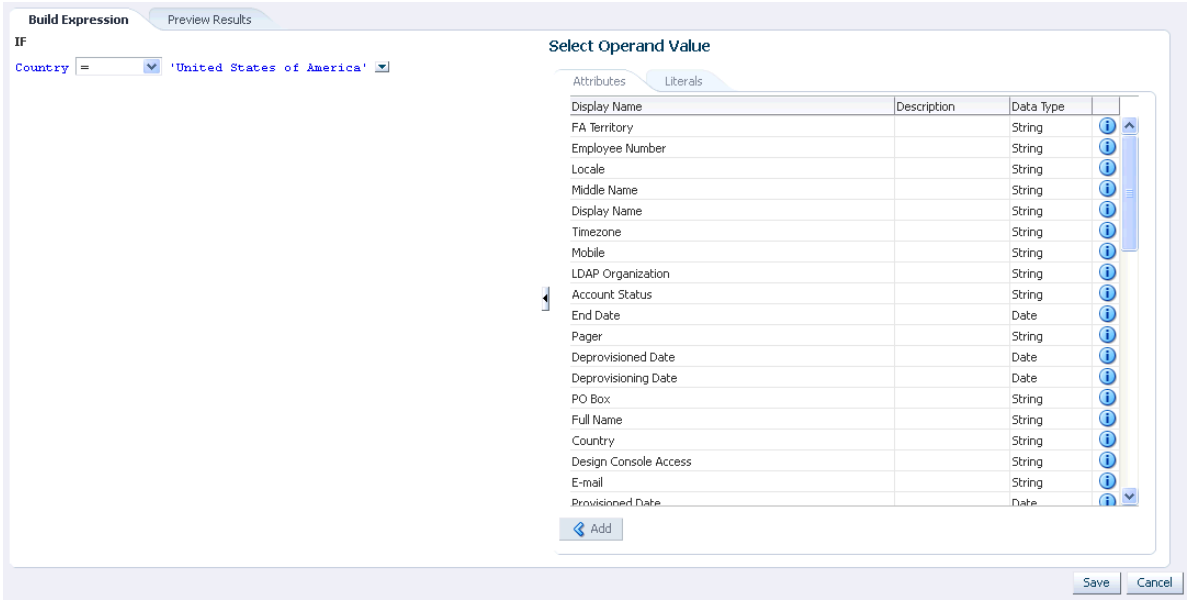
- Robert2UserchkboxDL is check box, which must be used in the rule as a string. Use "1" to check for True/yes/Selected/Checked, and use "0" to check for False/no/Unselected/unchecked.
- Robert2UserLookupDL is lookup type. In the default userprofile, "Robert2LookUpMean3" will be displayed. But you must use its code value "Robert2LookUpCode3" in the expression.
- For All type of Attributes, there is no way to check NULL or no value.

> **Note:**
>
> Checkbox fields are stored as strings in the backend. The data type for a checkbox field is a String and not Boolean. Therefore, all string operations will be displayed.

7. Click **Add** to add the specified value to the condition expression. The expression now means that users belonging to United States of America will be dynamically assigned to the open role.

   Figure 16-2 shows the expression builder with the condition.

Figure 16-2 The Expression Builder



8. If required, on the Preview Results tab, you can preview members to whom this rule will be applied.
9. Click **Save.** The expression builder closes, and the rule you defined has been saved.

10. Click **Evaluate membership rule now** to evaluates this rule against all users immediately, else you will have to run the `Refresh Role Memberships` scheduled job to evaluate rule.

To create membership rules for dynamically assigning members to a role using an SQL query:

> **Note:**
>
> - You must enable the property **RoleUserMembershipRuleSQLSupported** to view the **Create SQL Membership Rule** option. You can also enable property **RefreshRoleMembershipJob.EvaluateAllRolesForSQLMembershipRule** to evaluate all SQL membership rule when the **Refresh Role Membership** job is executed. For more information, see Default System Properties in Oracle Identity Governance.
> - If you revert these system properties, then you must first delete the **SQL Membership Rules** that is created for the Role and then revert back.

1. Click **Create SQL Membership Rule** to open the SQL User membership rules for role sample.
2. Under **SQL Query** tab, enter the SQL Query details.
3. Click the **Preview Results** tab. The role members that match the expression you specified are listed. You can use this preview for to view the role members that meet the SQL query rule criteria

   > **Note:**
   >
   > In case the SQL query is incorrect then the results are not displayed.

4. Click **Save**. The Members tab is displayed with the SQL Query added in the **User Membership Rule** section.
5. If you want the membership rule to be evaluated as soon as the role is created, then select the **Evaluate membership rule now** option.

   If you want to add/remove more role members or membership rules, then perform the procedures described in The Members Tab.
6. Click **Next**. The Organization page of the Create Role wizard is displayed.

> **Note:**
>
> After you create the Role using the **SQL Membership Rule**, if you delete the rule and want to return to **Membership Rule** for adding the role, then click **Apply** and click **Role** to add using the **Membership Rule**.

16.5.2.5.5 Modifying Membership Rules

To modify a user membership rule:

1. In the Members tab, in the User Membership Rule section, click **Edit Rule**. The expression builder is displayed.
2. Specify a condition to dynamically assign members, as described in the steps for adding membership rule.
3. If required, on the Preview Results tab, you can preview members to whom the modified rule will be applied.
4. Click **Save.** The expression builder closes, and the rule you modified has been saved. You can then click the Apply, Apply and Evaluate, and Revert buttons, as required.

16.5.2.5.6 Deleting Membership Rules

T o delete a user membership rule:

1. In the Members tab, in the User Membership Rule section, click **Delete Rule**. A dialog box asking to confirm whether you want to delete the membership rule is displayed.
2. Click **Yes.** The membership rule is deleted.

After adding, modifying, or deleting user membership rule, click **Apply**. The request is to be approved if it raises a workflow. Then the rule is added, edited, or removed from the role. Rule evaluation takes place immediately if the **Evaluate membership rule now** option is selected. Otherwise, it will be evaluated only when the `Refresh Role Memberships` scheduled job is ran.

16.5.2.6 The Organizations Tab

In the Organizations tab, you can perform the following:

- About Organizations Tab
- Publishing Roles to an Organization
- Revoking Roles From an Organization

16.5.2.6.1 About Organizations Tab

The Organizations tab allows you to assign and revoke organizations to and from the open role. By assigning an organization to the open role, you make the role available to the organization. This is called publishing the role entity to an organization.

All the organizations, to which the open role has been published, are displayed in the Organizations tab. For each organization, the **include sub-orgs** option is available for selection in the Hierarchy Aware column. Select this option if you want the open role to be available to the entire hierarchy of the organization. To make the open role available only to the organization and not its hierarchy, leave this option deselected.

16.5.2.6.2 Publishing Roles to an Organization

To publish roles to an organization:

1. In the Role details page, click the **Organizations** tab. This tab displays the organizations that are assigned to the open role.

2. From the Actions menu, select **Add**. Alternatively, click **Add** on the toolbar. The Add Organizations dialog box is displayed.
3. Search for the organizations you want to add. The organizations are displayed in the Organization Results section.
4. Select the organizations that you want to add, and click **Add Selected**. The selected organizations are added to the Selected Organizations section.
5. For each selected organization, the **Hierarchy** option is selected by default. If you want to publish the role to the suborganizations of the selected organization, then leave the **Hierarchy** option selected.

   To publish the role to the selected organization only, deselect the **Hierarchy** option.
6. Click **Select.** Pending action is filled with Add. Repeat this if you want to add more organizations. You can click **Undo** if you do not want to add the organization that is already marked with add.

> **Note:**
>
> if no organization is selected, then the role is auto published to the organization of the logged-in user and to the organizations on which the logged-in user has admin roles capabilities.

16.5.2.6.3 Revoking Roles From an Organization

To revoke a role from an organization:

1. In the Organizations tab, select the organization from which you want to revoke the role.
2. To revoke the role from sub organizations of the currently selected organization, select the **Hierarchy Aware** option, and then click **Apply**. A message is displayed. Click **Revoke**.
3. From the Actions menu, select **Remove**. Alternatively, click **Remove** on the toolbar. A message is displayed asking for confirmation.
4. Click **Remove**. Pending action is filled with Remove. Repeat this if you want to remove more organizations. You can click Undo if you do not want to remove the organizations that are already marked with remove.
5. Click **Apply**. The request is to be approved if it raises a workflow. Then the selected organizations are added or removed from the role.

16.5.2.7 The History Tab

In the History tab, you can perform the following:

- About History Tab
- Searching Role History
- Viewing Role History

16.5.2.7.1 About History Tab

The History tab is displayed only when Identity Audit is enabled in the Oracle Identity Manager deployment.

This tab displays all data about the open role that have been modified within a specified date range. Using this tab, the role administrator can track any changes to the role definition. The role administrator can enter a date range, and view the modifications that have been done within that date range to the role attributes, role hierarchy, access policies, role memberships, organizations, membership rules, and role certifications. By default, the history for the last seven days is displayed in this tab.

> **Note:**
>
> In the History tab, data is available for only the retention period for auditing that is configured in the `Remove Audit Log Entries` scheduled job, for example, six months. See "Predefined Scheduled Tasks" in the *Administering Oracle Identity Governance* for information about the `Remove Audit Log Entries` scheduled job.

16.5.2.7.2 Searching Role History

To search for role history:

1. Open the role.
2. Click the **History** tab.
3. In the Search History section, enter a date range in the two date fields. You can also click the calendar icons and select the dates.
4. Click **Search**. The role history within specified date range is populated in the subtabs of the History tab. For example, all role attribute modifications are listed in the Attributes subtab.

   You can click **Reset** to reset the date ranges mentioned.

   If you do not specify any values in the date fields and click Search, then all modifications made to the role from its creation till date are displayed in the subtabs.

   > **Note:**
   >
   > All data shown in History is read-only and can not be modified.

16.5.2.7.3 Viewing Role History

To view role history:

1. Search for role history by specifying a date range, as described in Searching Role History.

2. Click the **Attributes** tab. The modifications made to the role attributes within the specified date range are displayed in a table. The columns in the table provide information about the attributes modified, the new value of the attributes, the old value of the attributes before modification, the date on which the attribute is modified, and the user who updated the attribute.
3. Click the **Hierarchy** tab. This tab displays the modifications made in the role hierarchy of the open role in a tabular format. The columns in the table provide information about the Display Name of the parent that have been added/removed, the change action (add/modify/delete), the user who modified the role hierarchy, and the dates on which the modification have been done.
4. Click the **Access Policy** tab. This tab displays the modification made to the access policies associated with the open role in a tabular format. The columns in the table provide information about the policy names that have been added/removed, the user who modified the access policies, the change action, and the dates on which the access policies were modified.
5. Click the **Organizations** tab. This tab displays the modifications made to the organization assignment of the open role in a tabular format. The columns in the tab provide information about the organization name that have been added or removed or updated, the change action, the user who modified the organization assignment, and the dates on which the modification have been done.
6. Click the **Role Membership** tab. This tab displays the modification made to the role membership of the open role in a tabular format. The columns in the table provide information about the user names that have been added or removed, the change action, the user who modified the role membership, and the dates on which the modification have been made.
7. Click the **Membership Rules** tab. This tab displays the modifications made to the membership rules in a tabular format. The columns in the table provide information about the rule name that have been modified, the change action (add/update/remove), the user who modified the rule, and the dates on which the modification have been done.
8. Click the **Certification** tab. This tab displays the certifications performed for the open role in a tabular format. The columns in the table provide information about the certification name that have been modified, the user who certified, and the dates on which the last certification have been made.

16.5.3 Displaying Role Analytics

When Identity Audit is enabled, administrators or approvers can view the role analytics during creation/modification/track request/approval of a role, such as impact analysis on users that will be or are assigned the role, role consolidation information, and SoD violations.

This section describes the following:

- About Viewing Role Analytics
- Viewing Role Analytics

16.5.3.1 About Viewing Role Analytics

Role analytics can be viewed in the following ways:

- In the Summary page of the Create Role wizard, click **View Analytics**.

- In the role details page, if you modify any attribute or any other data, then the **View Analytics** button is available.
- In the Request Details tab of the Pending Approvals page, click **View Analytics**. This is for the request approver to compare the role with other existing roles to justify or reject the creation of the requested role.

16.5.3.2 Viewing Role Analytics

To view role analytics:

1. In the Summary page of the Role Creation wizard, or in the role details page, or in the Request Details tab of the Pending Approvals page, click **View Analytics**. The Analytic Details page for the role is displayed. This page has the following sections:
   - **Impact Analysis:** Displays the number of potential users members that will be affected when a role is created/modified/deleted. The impact analysis is based on changes to the user membership rule and/or access policy association changes. The parameter affecting the members is user membership rule. Based on the rule, the potential members can be evaluated and displayed on the approval UI. The list of user names are paginated. This section also displays the impact of adding or removing the access policies from the role. The impact displays which users will get the entitlements associated with the access policy added as well as the users that will have the entitlements revoked when an access policy is removed from the role.
   - **SoD Violations:** Displays any access policies or entitlements within and across access policies that are in SoD conflict. See Managing Identity Audit for information about configuring identity audit rules and policies.
   - **Role Consolidation:** Displays contextual information about how similar the role is to other roles in the access catalog. The similarity is based on the entitlements of the two roles. The entitlement matching percentage must be at least 50 percent to be considered as a match. When a match is found, the common memberships must be calculated. Only the top three percentage matches are displayed, if they match the 50 percent cutoff. For example, if the top three percentages are 100%, 85%, and 50%, and 10 roles match 100%, one role match 85%, and 8 roles match 50%, then all of these are displayed.

     If the percentage of entitlements matching is greater than or equal to 50%, then the percentage of users matching is also displayed along with the percentage of matching entitlements.
2. Click the down arrow in the **Impact Analysis** box.

   An overview of the impact on users and entitlements of the role is displayed. Impact Analysis is displayed in the following sections:
   - **Users:** This section provides a graphical representation of the users that have been added and deleted, and the unchanged users. It shows users that are added/revoked only via membership rules and does not show the users that are added/removed directly.
   - **Users Added:** This section contains a table that shows the usernames, user login IDs, and the email IDs of the users that have been added to the role. It has the following subsections:

  - **Users Deleted:** This section contains a table that shows the usernames, user login IDs, and the email IDs of the users that have been revoked from the role.
  - **Users Unchanged:** This section contains a table that shows the usernames, user login IDs, and the email IDs of the users that are unchanged in the role.

  To view more details about each user, you can click the user name. More information about the user is displayed in the User Details popup. It displays information about added/deleted/modified users and entitlements. Click **Cancel** to close the User Details popup.

- **Entitlements:** This section provides a graphical representation of the entitlements that have been added and deleted, and the unchanged entitlements.
- **Entitlements Added:** This section contains a table that shows the Display Name, Entitlement Name, and Description of the entitlements that have been added to the role. It contains the following subsections:
  - **Entitlements Deleted:** This section contains a table that shows the display names, entitlement names, and descriptions of the entitlements that have been revoked from the role.
  - **Entitlements Unchanged:** This section contains a table that shows the Display Name, Entitlement Name, and Description of the entitlements that are unchanged in the role.

  To view more information about each entitlement, click the entitlement name. More information about the entitlement is displayed in a popup.

3. Click the down arrow in the **SoD Violations** box. The SoD Violations box already shows the number of items that are in violation. When you activate this box, all the SoD policies that are in violation are displayed. When you click a policy, the details of the policy are displayed in the Description box. This box lists all the items that are in violation. The name and description of the items are displayed in a tabular format. On selecting each item, the severity of the violation is also shown above the table.
4. Click the down arrow in the **Role Consolidation** box. The Role Consolidation box already shows the number of roles that are similar to the open role. Similar roles are roles with matching entitlements. For these similar roles, memberships match is then computed, irrespective of whether they have any memberships or not. All roles are considered, pending, direct grants, and dynamic memberships

   The role comparison is represented as a graph, which shows the similar roles and the membership and entitlement matching percentage of the similar roles with the open role.

   > **Note:**
   >
   > Roles without members are considered for role consolidation. The similarity is only based on entitlements. After similar roles are found, then membership match for only those roles are computed. It could be 0 if the similar role has no memberships.

5. You can click **Back** to go back to the previous page.

16.5.4 Deleting Roles

Delete the roles that are not required or are not in use.

To delete a role:

1. In the Search Roles page, search for a role as described in Searching for Roles.
2. Select the role that you want to delete.
3. From the Actions menu, select **Delete**. Alternatively, click **Delete** on the toolbar.

   If the role has existing relationships, such as parent roles, access policies, members, or organizations, then a message is displayed stating that , Deleting the selected role will also delete its relationships.
4. Click **Yes** to confirm.

   If workflows are configured, then an approval task is sent to the Role Owner for approval, and the role is not deleted from the system until all approvers have approved. During the approval, the approver can see the impact of deleting the role by clicking **View Analytics**.

17

Managing Access Policies

The access policy management feature in Oracle Identity Manager allows you to understand the different features of access policy, create and manage access policy, manage provisioning multiple instances of the same resources via access policy.

It contains the following sections:

- Terminologies Used in Access Policies
- Features of Access Policies
- Creating Access Policies
- Managing Access Policies
- Deleting Access Policies
- Provisioning Multiple Instances of the Same Resource via Access Policy
- Troubleshooting Issues with Evaluate User Policy Scheduled Job

17.1 Terminologies Used in Access Policies

Important terminologies used in access policy management are Access Policy Owner, Resource, Account, Account Discriminator, and Application instance.

The following terminologies are associated with access policies:

- **Access Policy Owner**: Access policy owner does not have any special privileges, as access policy configuration UI is available in the Identity Self-Service. Also there are no authorization checks added based on access policy owners in access policy management APIs.
- **Resource:** A resource is a logical entity in Oracle Identity Manager that can be provisioned to a user or an organization in Oracle Identity Manager. For example, Microsoft Active Directory (AD), Microsoft Exchange, SAP, UNIX, and Database is modeled as a resource in Oracle Identity Manager.

  Resources are templated definitions that are associated with one or more workflows called Provisioning Process in Oracle Identity Manager, which model the lifecycle management, such as how to provision, revoke, enable, and disable.

  Resources also have entities called forms associated with them. Forms represent a collection of attributes associated with the resource. For instance, a form associated with AD server includes attributes such as SAM Account Name, Common Name, and User Principal Name. Forms also contain an attribute of type IT Resource. See the description of IT Resource Type in this section for details on IT resource type.
- **Account:** Accounts are actual instances of a resource that are created and provisioned to a user or organization in Oracle Identity Manager. For example, an e-mail account on an Exchange server is an account (instance) of resource type Exchange.

  Accounts have specific values for the attributes of the associated form.

- **Account Discriminator:** Account discriminator is a collection of attributes on a form that uniquely identifies the logical entity on which accounts are created. This term is sometimes loosely referred to as a target. For instance, for an AD server, an account discriminator can be a combination of AD server (an attribute of type IT Resource) and Organization Name.

  Attributes are marked as account discriminators by setting the Account Discriminator property of a Form field to True.

- **Application instance**: Application instance is a combination of IT resource instance (target connectivity and connector configuration) and resource object (provisioning mechanism).

17.2 Features of Access Policies

Some of the key features of managing access policy are Direct Provisioning, Revoking or Disabling the Policy, Role Hierarchy, Denying a Resource, Evaluating Policies, Evaluating Policies for Reconciled and Bulk Load-Created Accounts, Access Policy Priority, Access Policy Data, and Provisioning Multiple Instances of the Same Resource via Access Policy.

This section describes the various features offered by the access policy engine in the following sections:

- Direct Provisioning
- Revoking or Disabling the Policy
- Role Hierarchy
- Denying a Resource
- Evaluating Policies
- Evaluating Policies for Reconciled and Bulk Load-Created Accounts
- Evaluating Policies for Direct Provisioned and Request Created Accounts
- Access Policy Priority
- Access Policy Data
- Provisioning Multiple Instances of the Same Resource via Access Policy by Using Account Discriminator
- Access Policy Authorization

17.2.1 Direct Provisioning

Whenever an access policy is applied, the resources are directly provisioned/denied without any request being generated.

17.2.2 Revoking or Disabling the Policy

You must specify whether a resource in a policy must be revoked or disabled when the policy no longer applies. Based on your selection, the resources are automatically revoked from the users or disabled when the policy no longer applies to the users. Accounts and entitlements can either be revoked or disabled if policy no longer applies.

For each resource associated with an access policy, you must select any one of the following options:

- **Revoke:** Selecting this option revokes the account and the entitlements associated with the access policy when the access policy is no longer applicable.
- **Disable:** Selecting this option disables the account and revokes the entitlements associated with the access policy when the access policy is no longer applicable.
- **Keep account active if entitlement provisioned outside of Access Policy:** Selecting this option keeps the account as active when the user has entitlements provisioned outside of the Access Policies for this resource.

> **Note:**
>
> This option is not selected by default.

When the **Revoke** option or the **Disable** option is selected, entitlements are always revoked with the policy no longer applies. If the **Disable** option is selected, then the entitlements associated with the resource are revoked when the policy no longer applies because the entitlements have been originally granted because of the role grant. The entitlements are added to the resource instance when the role is granted once again.

If two policies have the same resource in the policy definition with one having the **Revoke** option selected and the other one with the **Disable** option, then the **Disable** option takes precedence over the **Revoke** option. In other words, resources are disabled (and not revoked) when policy no longer applies.

17.2.3 Role Hierarchy

Role Hierarchy support for access policies is available. To enable this feature set the system property **XL.AllowRoleHierarchicalPolicyEval** value to true. When Role Hierarchy is enabled, access policy engine considers both the direct and indirect roles during Access Policy Evaluation.

17.2.4 Denying a Resource

While creating an access policy, you can select resources to be denied along with resources to be provisioned. If you first select a resource for provisioning and then select the same resource to be denied, then error message saying resource is already added. When same resource is added in two different policies, in one policy if the resource is denied and in the other it is provisioned. And both these policies are applicable to the user, then the resource that is denied takes precedence.

> **Note:**
>
> If a resource is denied by an access policy, then the resource is always denied, even if a different policy provisions it. Denying of resources is irrespective of access policy priority. Even if an access policy with lower priority denies a resource, it takes precedence over an access policy with higher priority.

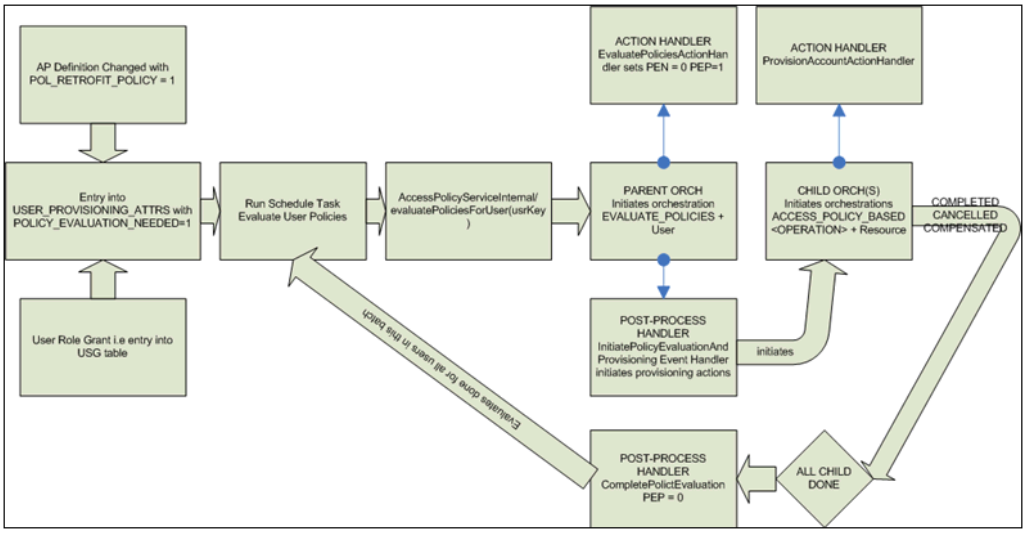
17.2.5 Evaluating Policies

Access policy evaluation works in the following manner:

1. After role grant to user or update of policy definition, the users for whom policy evaluation is needed are identified and the entry is updated or added in the USER_PROVISIONING_ATTRS table.
2. Flag stored in USER_PROVISIONING_ATTRS. POLICY_EVAL_NEEDED is used to determine users for whom policy evaluation is required.
3. The `Evaluate User Policies` scheduled job is run to invoke policy evaluation and further actions on accounts. By default, this task is enabled and scheduled to run every 10 minutes. See "Predefined Scheduled Tasks" in the *Administering Oracle Identity Governance* for information about evaluate user policies scheduled tasks.
4. The scheduled task picks distinct user records (each record in this table is for distinct user) available in USER_PROVISIONING_ATTRS in the default batch size of 500 using 20 threads, which is 25 records per thread in the ascending order of update date. A JMS message is submitted for each user for access policy evaluation.

Access policy evaluation is shown in Figure 17-1.

Figure 17-1 Access Policy Evaluation



When the policy is created with `Retrofit = true` and the policy definition is changed by one of the following manner:

- When a user is made a part of a role or removed from a role. The policy for the user is evaluated as part of the add or remove operation.
- If the retrofit flag is set for the policy. The evaluations can happen in the following scenarios:
  - Policy definition is updated. Policies are evaluated for all applicable users.
  - A role is added or removed from the policy definition. Policies are evaluated only for roles that is added or removed.

> **Note:**
>
> After the role is applicable to the user, you must run the Evaluate User Policies scheduled job to make access policy applicable.

- A resource is added, removed, or the **Revoke** or **Disable** options are changed for the resource.

  When you change the **Revoke** and **Disable** options from one to the other, the existing resource instances are not re-evaluated immediately. This policy change takes effect only the next time the policy is evaluated by the Evaluate User Policies scheduled task.

- When policy data is updated or deleted. This includes both parent and child form data. Policies are evaluated for all applicable users.

When roles are assigned to or removed from a policy, then users are immediately marked for policy evaluation irrespective of the setting for `Retrofit` flag. The `Retrofit` flag can be used only to determine if users need to be marked for policy evaluation for access policy definition changes, which involves:

- Priority of the policy changes
- Resource associated to policy changes
- The the **Revoke** or **Disable** options change
- Parent or child data changes. In this scenario, if `Retrofit` is set to `false`, then users are not marked for policy evaluation although policy definition has changed.

> **Note:**
>
> For managing the evaluation of Access Policy for users in the **Disabled** status, set the value of the system property `XL.DoNotEvaluateAPForDisableUsers`. For details, see Default System Properties in Oracle Identity Manager

17.2.6 Evaluating Policies for Reconciled and Bulk Load-Created Accounts

The access policy engine can link access policies to reconciled accounts and to accounts created by the Bulk Load Utility. The access policies are then evaluated using the `Evaluate User Policies` scheduled job. To enable this feature, ensure the following:

- Set the values of `XL.AllowAPHarvesting` and `XL.AllowAPBasedMultipleAccountProvisioning` system properties to `TRUE`.

  For more information about these system properties, see and for information about setting the value of a system property, see Creating and Managing System Properties in the *Administering Oracle Identity Governance*.

- Set the retrofit flag to ON for the policy to be linked by selecting Retrofit Access Policy.

  For information about the retrofit flag, see Creating Access Policies. For information about updating a policy definition, see Managing Access Policies.

- Populate the ITResource field in access policy defaults.

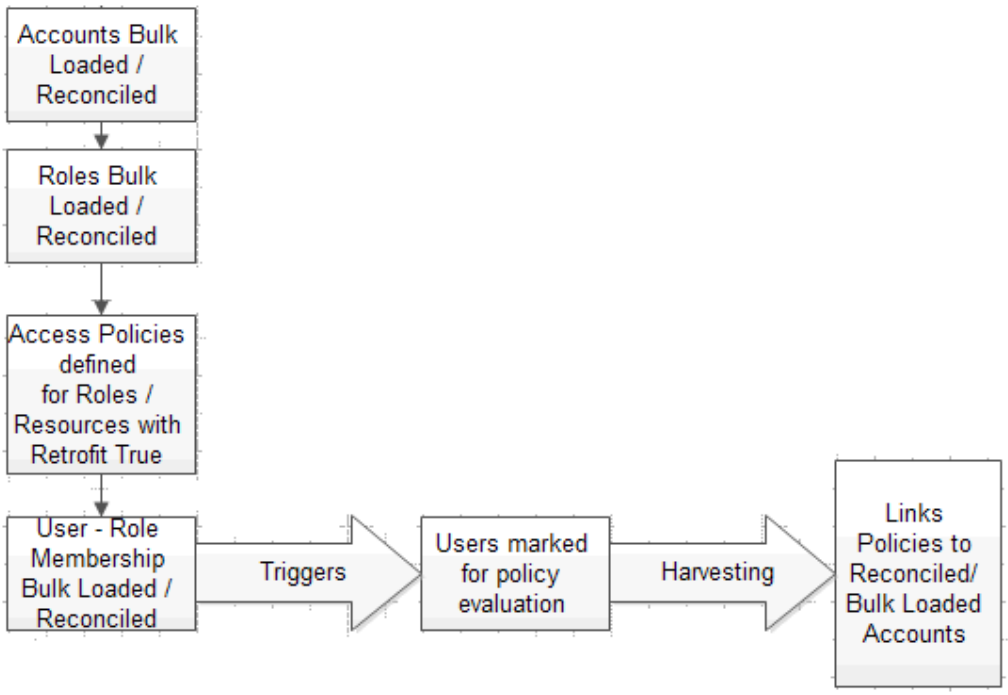
If the ITResource field is not populated, then the provisioning engine cannot determine the application instance to be associated with the account and the account will not be visible in the UI.

- Designate a field on the process form as the discriminator field and set the value of the **Account Discriminator** property to `True`. Then, populate the access policy defaults for the account discriminator field.

  For information about setting the discriminator field, see Enabling Multiple Account Provisioning.

After enabling the feature to link access policies to reconciled accounts and to accounts created by the Bulk Load Utility, the access policy harvesting flow is depicted in Figure 17-2.

Figure 17-2 Access Policy Harvesting Flow



17.2.7 Evaluating Policies for Direct Provisioned and Request Created Accounts

The access policy engine can link access policies to accounts created by request and to accounts that are provisioned directly. To enable these features, perform the steps as in enabling the Reconciled and Bulk Load-Created Accounts feature described in Evaluating Policies for Reconciled and Bulk Load-Created Accounts with the following exceptions:

- To enable linking access policies to accounts created by request, set the values of `XL.APHarvestRequestAccount`, `XL.AllowAPHarvesting`, and `XL.AllowAPBasedMultipleAccountProvisioning` system properties to `TRUE`.

- To enable linking access policies to accounts that are provisioned directly, set the values of `XL.APHarvestDirectProvisionAccount`, `XL.AllowAPHarvesting`, and `XL.AllowAPBasedMultipleAccountProvisioning` system properties to `TRUE`.
- To enable updating the account data with the policy defaults for the accounts linked to the access policies, set the values of the `XL.APHarvesting.AllowAccountDataUpdate`, `XL.AllowAPHarvesting`, `XL.APHarvestRequestAccount`, `XL.APHarvestDirectProvisionAccount`, and `XL.AllowAPBasedMultipleAccountProvisioning` system properties to `TRUE`.

For more information about these system properties, see Default System Properties in Oracle Identity Governance.

17.2.8 Access Policy Priority

Policy priority is a numeric field containing a number that is unique for each access policy you create. The lower the number, the higher is the priority of the access policy. For example, if you specify Priority =1, it means that the policy has the highest priority. When you define access policies through Oracle Identity System Administration, the value 1 is always added to the value of the current lowest priority and the resultant value is automatically populated in the Priority field. Changing this value to a different number might result in readjusting the priority of all the other access policies, thus ensuring that the priorities remain consistent. The following actions are associated with the priority number:

- If the priority number entered is less than 1, then Oracle Identity Manager will change the value to 1 (highest priority).
- If the priority number entered is greater than M, in which M is the current lowest priority, then Oracle Identity Manager will force to specify the value as less than or equal to M+1.
- Two access policies cannot have the same priority number. Therefore, assigning an already existing priority number to an access policy will lower the priority by 1 for all policies of lesser priority.

Conflicts can arise from multiple access policies being applied to the same user. Because a single instance of a resource is provisioned to the user through access policies, Oracle Identity Manager uses the highest priority policy data for a parent form. For child forms, Oracle Identity Manager uses cumulative records from all applicable policies.

If there is more than one access policy created for the same resource but granting different sets of entitlements and having different behavior when policy no longer applies, then the access policy with **Disable if no longer applies** (DLNA) option enabled has the highest priority irrespective of the access policy priorities. For example, if there is an access policy with **Revoke if no longer applies** (RLNA) option enabled and another policy with DLNA option enabled, then the policy with DLNA option enabled has higher precedence. Irrespective of the order in which the policies are applied, as long as a policy with DLNA option enabled is applied to the user, the account is always disabled when the policy no longer applies.

If a policy with Disable if no longer applies is later converted to Revoke if no longer applies, then existing accounts that are associated with the policy are not updated to RLNA. The change is effective only for accounts to be created in future.

If a policy with RLNA is later converted to DLNA, then the accounts that are already revoked are not impacted. The change is effective only for accounts currently associated with this policy or accounts to be created in the future.

17.2.9 Access Policy Data

There are multiple ways in which process form data is supplied for resources during provisioning. The following is the order of preference built into Oracle Identity Manager:

1. Default values from the form definition using Oracle Identity Manager Design Console
2. Prepopulate adapters
3. Access policy data if resource is provisioned because of a policy
4. Data updated by Process Task

If a given option is available, then the rest of the options that are at a lower order of preference are overridden. For example, if Option 4 is available, then Options 3, 2, and 1 are ignored.

> **Note:**
>
> When *XL.AllowRequestDataToPrepopAdapter* system property is set to true, then Pre-populate Adapters data takes precedence over Access Policy data. That is, provisioning access policy data will be overridden with pre-populate adapters data. For more information about this system property, see Default System Properties in Oracle Identity Governance in the *Administering Oracle Identity Governance*.

17.2.10 Provisioning Multiple Instances of the Same Resource via Access Policy by Using Account Discriminator

In earlier releases of Oracle Identity Manager, access policies can be used to manage only a single account for a resource object. In other words, if you already have resource provisioned to user (account has been created in the target system) and if another instance of the same resource is to be provisioned to the same user via access policy, then it is not possible in earlier releases of Oracle Identity Manager. To achieve the functionality of provisioning multiple instances of resource to a user, prior to access policy enhancement in Oracle Identity Manager, you must clone the connector that represents the target system in Oracle Identity Manager. Cloning of connector is error prone and need a lot of effort for testing/maintenance of the cloned resources. Access Policy enhancement done for provisioning of multiple instances of resource in Oracle Identity Manager saves the time and effort on cloning connectors.

A target system, such as UNIX server, Active Directory (AD) server, database, SAP, or JD Edwards, is the external system to Oracle Identity Manager that must be provisioned to users in Oracle Identity Manager. The target system is represented by an entity called resource in Oracle Identity Manager. The server on which target system is installed is represented by IT resource in Oracle Identity Manager. And the login credentials provided to user accessing this target system is represented by an account in Oracle Identity Manager. A user can have multiple accounts on a single target system. For example, one account can be a service (administrator) account and another a regular account. Therefore, it is mandatory to have two accounts for a same

user in a single target system. In addition, it is possible to have different instances of target system, such as multiple UNIX servers, database servers, and AD servers. As a result, it is required to create accounts on each instance of the target system for the same user. For implementation details, see Creating Separate Accounts for the Same User and Same Resource on a Single Target System.

In Oracle Identity Manager, access policies can provision multiple accounts in the same target system as well as a single account in multiple instance of the same target system. While evaluating access policies and provisioning resources to user, Oracle Identity Manager checks if the resource has already been provisioned to the user or not. This is determined by checking the resource key (OBJ_KEY) of the resource provisioned to user. To have multiple instances to be provisioned through access policy, another criteria called *account discriminator* along with OBJ_KEY is required to distinguish the multiple instances of the same resource. Therefore, access policy checks the resource key as well as account discriminator to decide if the resource has been provisioned or not.

The account discriminator is a field on a process form (account data) that distinguishes two accounts of the same user, which can be present on the same target system or different target systems. For example:

- If user Jane.Doe is to be provisioned two accounts on two different UNIX servers, then IT resource can be used as account discriminator.
- If user John.Doe is to be provisioned two accounts on the same database instance, then distinct login IDs can be used as account discriminator.

> **See Also:**
>
> Provisioning Multiple Instances of the Same Resource via Access Policy for the steps to provision data from multiple target systems

17.2.11 Access Policy Authorization

The following authorization capabilities related to access policies should be assigned to the user to get the appropriate access to access policies:

- Access Policy - Create
- Access Policy - Delete
- Access Policy - Modify
- Access Policy - View/Search

See Managing Administration Roles for information about admin roles and admin role capabilities. See Functional Capabilities for information about the different functional capabilities and their details.

17.3 Creating Access Policies

You can define an access policy for provisioning resources to users who have roles defined in the policy by using the Access Policy page.

> **Note:**
>
> - Identity Audit policies (SoD) are not evaluated during the creation of an access policy.
> - The association of a role to an access policy is done as part of role management and not via the access policy UI.

To create an access policy:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab.
3. Click the **Roles and Access Policies** box, select **Access Policies**. The Access Policy page is displayed.
4. Click **Create** to open the Create Access Policy page.
5. Enter information in the required fields indicated with an asterisk (*), such as access policy name and description.

> **Note:**
>
> The following special characters are not allowed in the access policy name:
>
> Semicolon (;)
>
> Hash (#)
>
> Percentage (%)
>
> Equal to (=)
>
> Bar (|)
>
> Plus (+)
>
> Comma (,)
>
> Forward slash (/)
>
> Back slash (\)
>
> Single quote (')
>
> Double quote (")
>
> Less than (<)
>
> Greater than (>)

6. From the Owner list, select **USER** or **ROLE** as the policy owner type. Based on your selection, click the lookup icon and select a user or role as the policy owner.

   If you do no select a policy owner type, then the access policy is created with the default policy owner type as USER and the logged in User as Owner.

   If you select a policy owner type and do not select a policy owner value, which is USER or ROLE, and click **Next**, then a validation error is displayed that does not allow you to proceed to the next screen.

7. Select **Retrofit** to retrofit this access policy when it is created.

   If you set the **Retrofit** option, then any changes to access policy data will be updated to existing users. For information about assigning access policies to roles, see The Access Policies Tab.

   If you do not select this option, then existing role memberships are not taken into consideration.

8. Enter appropriate **Priority Level**.

9. Click **Next**. The Application page is displayed.

10. Click **Add** in the Provisioned Applications panel to select the application instance that needs to be provisioned. Add Application Instance window is displayed.

    Select the application instance by using the filter search menu.

    - Select the name of the application instance from the results table, and then click **Add Selected**.

      > **Note:**
      >
      > If a child application is dependent on other application , adding child application instance will automatically add its parent application instance. Removing parent application instance is not permitted as long as child application instance is added. Duplicate Child Form records are not allowed and will be automatically removed on clicking **Save**.

    - The names of the desired application instance to provision appear in the Selected list.
    - To unassign the selected application instance, select the application instance in the Selected list and click **Remove**.

11. Click **Select**.

12. For each application instance listed in the page, select any one of the following options:

    - **Revoke:** Selecting this option revokes the account and the entitlements associated with the access policy when the access policy is no longer applicable.
    - **Disable:** Selecting this option disables the account and revokes the entitlements associated with the access policy when the access policy is no longer applicable.

    See Revoking or Disabling the Policy and Evaluating Policies for more information about revoking or disabling accounts and entitlements when access policies no longer apply.

13. For the selected Application Instance, to provide additional information like parent data and child data, click on the Display name link of the selected application instance. Create Access Policy - General Attributes page opens.

Enter the required information and click **Save**.

14. Click **Add**, from the Denied Applications panel to select the application instance that needs to be denied. Add Application Instance window is displayed.

    Select the application instance by using the filter search menu.

    - Select the name of the application instance from the results table, and then click **Add Selected**.
    - The names of the desired application instance to deny appear in the Selected list.
    - To unassign the selected application instance, select the application instance in the Selected list and click **Remove**.

15. Click **Finish** to create the access policy.

    A success message is displayed with the access policy name.

17.4 Managing Access Policies

You can modify information of existing access policies from the Access Policy page.

To manage access policies:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab.
3. Click the **Roles and Access Policies** box, select **Access Policies**. The Access Policies page is displayed.
4. Search for the Access Policy you want to modify. Enter the Name or Description and click Search icon.
5. Select the Access Policy you want to modify and click **Open** on the toolbar.

   Access Policy page is displayed with three tabs, Attribute, Applications, and Roles. You can modify the Attributes and the Applications details, but Roles information can not be modified.

17.5 Deleting Access Policies

Delete the access policy that are not required or are not in use.

To delete an Access Policy:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab.
3. Click the **Roles and Access Policies** box, select **Access Policies**. The Access Policies page is displayed.
4. Search for the Access Policy you want to delete. Enter the Name or Description and click Search icon.
5. Select the Access Policy you want to delete and click **Delete** on the toolbar.

> **Note:**
>
> Access Policy can be deleted only if it is not associated with any Role. Ensure to remove all dependencies before deleting any access policy.

17.6 Provisioning Multiple Instances of the Same Resource via Access Policy

Provisioning multiple instances of the same resource via access policy by using account discriminator involves enabling multiple account provisioning, creating separate accounts for the same user and same resource on a single target system, provisioning multiple instances of a resource to multiple target systems, and limitation of provisioning multiple instances of a resource via access policy.

This section contains the following topics:

- Enabling Multiple Account Provisioning
- Creating Separate Accounts for the Same User and Same Resource on a Single Target System
- Provisioning Multiple Instances of a Resource to Multiple Target Systems
- Limitation of Provisioning Multiple Instances of a Resource via Access Policy

17.6.1 Enabling Multiple Account Provisioning

By default, Oracle Identity Manager does not support multiple account provisioning. To enable multiple account provisioning:

Set the value of the XL.AllowAPBasedMultipleAccountProvisioning system property to `TRUE`. For more information about this system property, see Creating and Managing System Properties in *Administering Oracle Identity Governance*.

When multiple account provisioning is enabled, you must define the appropriate account discriminator attributes. To do so:

1. Log in to the Design Console.
2. Update the process form as follows:
   a. Expand Development Tools, and then double-click **Form Designer**.
   b. Search and open the process form.
   c. On the Form Designer tab, click **Create New Version**.
   d. In the Create a New Version dialog box, enter a label in the Label field, and then click **Save**.
   e. From the Current Version list, select the version that you created.
   f. On the Properties tab, select the field that you want to designate as the discriminator field, and then click **Add Property**.
   g. In the Add Property dialog box, select **Account Discriminator** as the property name, enter `True` in the Property Value field, and then click **Save**.

h. Click **Make Version Active**, and then click **OK**.

i. Click **Save**.

17.6.2 Creating Separate Accounts for the Same User and Same Resource on a Single Target System

Two distinct accounts can be created for the same user and same resource on a single target system via access policy. For example, it is required to create two accounts, a user account and service account on a single AD instance. The Active Directory target system is represented by the AD User resource in Oracle Identity Manager. This is implemented in the following way:

1. Create a AD User resource.
2. Create the user, such as JohnD.
3. In the process form, mark UD_ADUSER_ORGNAME as the discriminator field so that two distinct accounts have different login IDs.
4. Create two access policies as follows:
   - **For regular account:**

     Access policy name: AP1

     Associated to role: Role1

     Resource to provision: AD User

     Process form having Discriminator field: User ID (UD_ADUSER_ORGNAME)

     Default value in access policy: Account1
   - **For service account:**

     Access policy name: AP2

     Associated to role: Role2

     Resource to provision: AD User

     Process form having Discriminator field: User ID (UD_ADUSER_ORGNAME)

     Default value in access policy: Account2

   > **Note:**
   >
   > You must create a prepopulate adapter associated with the process form to generate the values for User ID so that unique values are generated for this field.

5. Assign Role1 and Role2 to JohnD. Note that you will not see the resource provisioned right after completion of role assignment. You must either wait for the Evaluate User Policies scheduled task to run automatically or you run this scheduled task manually.

   When Role1 is assigned to JohnD, the Account1 account is created in the AD User target system via the AP1 access policy. When Role2 is assigned to JohnD, Account2 is created in AD User via AP2. Therefore, two distinct accounts can be

created for the same user and same resource on a single target system via access policy.

17.6.3 Provisioning Multiple Instances of a Resource to Multiple Target Systems

The following are the broad-level steps to provision multiple instances of a resource object to multiple target systems via access policy:

1. Create an IT resource type by using the IT Resources Type Definition Form in the Oracle Identity Manager Design Console. For information about using this form, see IT Resources Type Definition Form in *Developing and Customizing Applications for Oracle Identity Governance*.
2. Create multiple IT resource instances of the IT resource type that you created in step 1. For information about creating IT resources, see Creating IT Resources in *Administering Oracle Identity Governance*.

   Here, IT resource instance is the account discriminator. See Provisioning Multiple Instances of the Same Resource via Access Policy by Using Account Discriminator for information about account discriminator.

   > **Note:**
   >
   > Display the process form default for IT Resource. It is mandatory to display it. By doing so, you can successfully provision an application instance via access policy.

3. Create a process form with a field of type that you created in step 1.
4. Create a resource object.
5. Create a process definition, and associate the resource object and process form. For information about creating a process definition, see Creating a Process Definition in *Developing and Customizing Applications for Oracle Identity Governance*.
6. Create access policies associating a role and resource object. See Creating Access Policies for details.

17.6.4 Limitation of Provisioning Multiple Instances of a Resource via Access Policy

Provisioning multiple instances of a resource via access policy has the following limitations:

- A single access policy cannot provision multiple instances of a resource to a user. Multiple access policies must be created to provision multiple instances of resource. You must create the same number of access policies as that of instances of same resource that is to be provisioned.
- If a resource object has a process form that has fields marked as account discriminator fields, then the value of these fields must be specified in any access policy that provisions that resource. Otherwise, issues might be encountered, such as multiple accounts might be provisioned when the policies are evaluated next time.

- If a resource object has a process form that has fields marked as account discriminator fields and if you use the access policy engine to provision this resource to one or more users, then the values of the account discriminator fields must remain constant throughout the lifecycle of the account. In other words, the values of the account discriminator fields must not be changed. This is because the access policy engine uses the resource object key and the account discriminator values to decide whether or not to provision a new account to the user.

  By modifying account discriminator values, you modify the basis on which the provisioning decision had been taken. and the behavior of the access policy engine cannot be determined. Therefore, it is recommended that you do not modify account discriminator values. And the process form values of the account discriminator fields must not be changed.
- If access policies are configured with different account discriminator values, they provision different accounts to the user.

> **Note:**
>
> Account discriminator values that are different only in casing (for example, abc and aBc) are also treated as different values. With this data, two accounts are provisioned to the end user.

17.7 Troubleshooting Issues with Evaluate User Policy Scheduled Job

In some cases, the Evaluate User Policy scheduled task may not trigger, process users, or process only a few users.

Any of the following could be the reasons:

- The Evaluate User Policy scheduled task ran, but there are no users marked for policy evaluation.
- Users were marked for policy evaluation, however the users are not active.
- Policy evaluation was done, however provisioning operations failed.

  In this case, the event handlers related to provisioning will be in CANCELLED state. Therefore, no accounts or entitlements are provisioned to the users.
- The Evaluate User Policy scheduled task is not triggered due to an issue with the scheduler.

  In this case, the scheduler issue needs to be troubleshooted separately.

To identify if the issue is with access policy, provisioning, or scheduler, perform the steps mentioned in the MetaLink note 1563379.1.

18
Managing Organizations

The organization management feature in Oracle Identity Manager allows you to view and manage organizations. Some of the organization management tasks include creating, viewing, modifying, and deleting organizations.
The tasks are described in the following sections:

- About Organization Entity
- Searching Organizations
- Creating an Organization
- Viewing and Modifying Organizations
- Creating a User Member
- Creating a Sub-Organization
- Disabling and Enabling Organizations
- Deleting an Organization

18.1 About Organization Entity

An organization entity represents a logical container of entities such as users and other organizations in Oracle Identity Manager. Organization in Oracle Identity Manager is used only for security purposes.

Organizations allow you to:

- Logically and securely manage user accounts and administrators
- Limit access to users, applications, roles, and entitlements

Customers can setup delegated administration by creating organizations and assigning users to various locations in an organizational hierarchy. Organizations that contain one or more other organizations are called parent organizations.

All Oracle Identity Manager users (including administrators) are statically assigned to one organization. Users also can be dynamically assigned to additional organizations. Oracle Identity Manager administrators are additionally assigned to control organizations.

18.2 Searching Organizations

Use the Organization page to perform simple and advanced search for organization.

To search for organizations you can perform one of the following:

- Performing Basic Search for Organization
- Performing Advanced Search for Organization

18.2.1 Performing Basic Search for Organization

1. Log in to Identity Self Service.
2. Click **Manage**. Click **Organizations** box. The Organization page is displayed.
3. To perform basic search, select any one of the following search criteria from the Search drop-down and click **Search** icon:
   - Organization Name
   - Type
   - Organization Status
   - Parent Organization Name
   - Certifier User Login

   The search results table displays the organization name, parent organization name, organization type, and organization status.

18.2.2 Performing Advanced Search for Organization

1. Log in to Identity Self Service.
2. Click Manage and click **Organizations** box. The Organization page is displayed.
3. Click **Advance** link. Advance Organization search page opens.
4. Select any one of the following **Match** options:
   - **All:** Search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.
   - **Any:** Search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.
5. In the Organization Name field, enter the organization name search attribute that you want to search. To do so, select a search comparator. The default search comparator is Starts With. The Equals comparator is available in the list as an alternative.

   You can use wildcard characters to specify the organization name.
6. From the Type list, select the organization type. The organization type can be Branch, Company, or Department.
7. To add a field in your search:
   a. Click **Add Fields,** and select a field, such as Organization Status.
   b. Enter value for the search attribute that you added. In this example, from the Organization Status list, select the organization status, which can be Active, Deleted, or Disabled.

      If you want to remove a field that you added in the search, then click the cross icon next to the field.
8. Click **Search**. The results are displayed in the search results table.

   The search results table displays the organization name, parent organization name, organization type, and organization status.

18.3 Creating an Organization

Using the Create Organization page, you can create an organization of type branch, company or department, control password behavior, and select applicable password policy for the organization.

To create an organization:

> **Note:**
>
> Organizations are persisted in the Oracle Identity Manager database regardless of whether the users and groups are stored in a Directory or the Oracle Identity Manager database.

1. In Identity Self Service, click **Manage** to open the Home Page. Click **Organizations**. The Search Organizations page is displayed.
2. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Organization page is displayed.
3. In the Organization Name field, enter the name of the organization.
4. From the Type list, select the type of the organization, such as Branch, Company, or Department.
5. Specify the parent organization to which the newly created organization will belong. To do so:
   a. Click the search icon next to the Parent Organization field. The Search Organizations dialog box is displayed.
   b. Search and select the organization that you want to specify as the parent organization.
   c. Click **Select**. The selected organization is added as the parent organization.
6. (Optional) Select a user in the Certifier User Login field to specify the selected user as the organization certifier of the organization being created.

   See Setting User Manager and Organization Certifier, for information about organization certifier.
7. Organization can control password behavior of the users entering into it by using home organization modification of the user. If the Home Organization of a user gets changed from one organization to other, and the password policies attached to these two organizations are different, then the Enforce password policy flag of the new home organization will determine if the user has to change the password as per the password policy of the new home organization at the next logon or user can continue using the same password.

   Select the Enforce password policy on reassignment from the drop down. Options are, Inherit from Parent Org, No, or Yes. Default value is Yes.

   - If Enforce password policy on reassignment is Yes, then the user has to change password as per the password policy of the new home organization at the first login after home organization is changed.

> **Note:**
>
> In case, challenge policy is enabled in the password policy of new home organization, then new password and challenge question has to be set at the first login.

- If Enforce password policy on reassignment is No, then user can continue using the existing password.
- If Enforce password policy on reassignment is Inherit from Parent Org, then value Yes or No is inherited from its nearest parent where it is set.

8. Specify a password policy name that you want to associate with the organization. To do so:
   a. Click the search icon next to the Password Policy Name field. The Search Password Policy Name dialog box is displayed.
   b. Search and select the password policy that you want to associate with the organization. To list all password policies, you can click the search icon, and then you can select the password policy from the search results.

      For information on how to create a new password policy see, Managing Password Policies.
   c. Click **Add**. The selected password policy name is added to the Password Policy Name field.
9. Click **Save** to create the organization.

18.4 Viewing and Modifying Organizations

You can perform administrative organization modifications in the organization details page. The modification is divided across the different sections of the organization details page, which means that modifications done in each section are independent of each other and must be saved individually.

. The modification for each section is described in the following sections:

- Opening Organization Details
- Modifying Organization Attributes
- Managing Child Organizations
- Viewing Organization Membership
- Managing Dynamic Organization Membership
- Managing Admin Roles
- Viewing Available Accounts
- Viewing Provisioned Accounts
- Viewing Available Entitlements

18.4.1 Opening Organization Details

You can view details of an organization in the organization details page.

To open the details of an organization:

1. In Identity Self Service, click **Manage** to open the Home Page. Click **Organizations**. The Search Organizations page is displayed.
2. Search and select the organization whose details you want to display.
3. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar. The details of the selected organization is displayed in a new page.

18.4.2 Modifying Organization Attributes

The Attributes tab of the organization details page displays attributes of the organization. You can modify the organization attributes if you have the appropriate authorization.

If you are authorized to modify the organization profile as determined by authorization policy, then the organization details page opens in editable mode, and you can modify organization information. You can modify the values for the attributes, and then click **Apply** to save the changes.

Whether or not the logged-in user is allowed to modify the organization is controlled by authorization policies. If you are not allowed to modify the organization, then the organization details page is displayed in read-only mode with no editable fields.

> **Note:**
>
> The Status attribute in the organization details page is read-only.

18.4.3 Managing Child Organizations

The Children tab displays a list of child organizations that the open organization has. You can create new child organization, view, delete and enable or disable a child organization.

For each child organization in the list, the organization name, organization type, and organization status are displayed. The Children tab enables you to perform the following:

- Creating a Child Organization
- Deleting a Child Organization
- Disabling a Child Organization
- Enabling a Child Organization
- Opening a Child Organization

18.4.3.1 Creating a Child Organization

In the Children tab, you can create a child organization or suborganization of the open organization by selecting **Create Sub-org** from the Actions menu. Alternatively, click **Create**

Sub-org on the toolbar. The Create organization page is displayed. Perform the steps described in Creating an Organization to complete creating the child organization.

18.4.3.2 Deleting a Child Organization

To delete a child organization:

1. In the Children tab, select the organization you want to delete.
2. From the Actions menu, select **Delete**. Alternatively, click **Delete** on the toolbar. A message is displayed asking for confirmation.
3. Click **Delete** to confirm. The selected child organization is deleted.

18.4.3.3 Disabling a Child Organization

To disable a child organization:

1. In the Children tab, select the organization you want to disable.
2. From the Actions menu, select **Disable**. Alternatively, click **Disable** on the toolbar. A message is displayed asking for confirmation.
3. Click **Disable** to confirm. The selected child organization is disabled.

18.4.3.4 Enabling a Child Organization

To enable a child organization:

1. In the Children tab, select the organization you want to enable.
2. From the Actions menu, select **Enable**. Alternatively, click **Enable** on the toolbar. A message is displayed asking for confirmation.
3. Click **Enable** to confirm. The selected child organization is enabled.

18.4.3.5 Opening a Child Organization

To open a child organization:

1. In the Children tab, select the organization you want to open.
2. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar, or click the name of the organization.

   The organization details page for the selected organization is displayed, by using which you can modify the details of that organization.

18.4.4 Viewing Organization Membership

The Members tab displays a list of users in the open organization.

For each user in the list, the following are displayed:

- User Login
- Display Name

- First Name
- Last Name
- E-mail
- Relationship Type

> **Tip:**
>
> You can add or remove users to and from organizations by using the Attributes tab of the user details page.

The Relationship Type column displays the type of relationship that the user member has with the organization. This is described in detail in Managing Dynamic Organization Membership.

18.4.5 Managing Dynamic Organization Membership

You can dynamically assign users to organizations based on user-membership rules, which you can define in the Members tab of the organization details page. You can create new dynamic membership rule, view and modify existing rules, or delete rules from the Members tab.

Managing dynamic user-organization memberships is described in the following sections:

- About Dynamic Organization Membership Rule
- Creating a Dynamic Organization Membership Rule
- Modifying a Dynamic Organization Membership Rule
- Deleting a Dynamic Organization Membership Rule

18.4.5.1 About Dynamic Organization Membership Rule

Users are assigned to organizations by specifying an organization name in the Organization attribute of the user details. This is called a static membership. In addition, you can dynamically assign users to organizations based on user-membership rules, which you can define in the Members tab of the organization details page. All users that satisfy the user-membership rule are dynamically associated with the organization irrespective of which organization hierarchy the users statically belong to.

Each organization can have one user-membership rule that enables a user to be a member of multiple organizations at a time, and thereby view and request for additional resources.

The dynamic memberships can be revoked by changing the user-membership rules.

18.4.5.2 Creating a Dynamic Organization Membership Rule

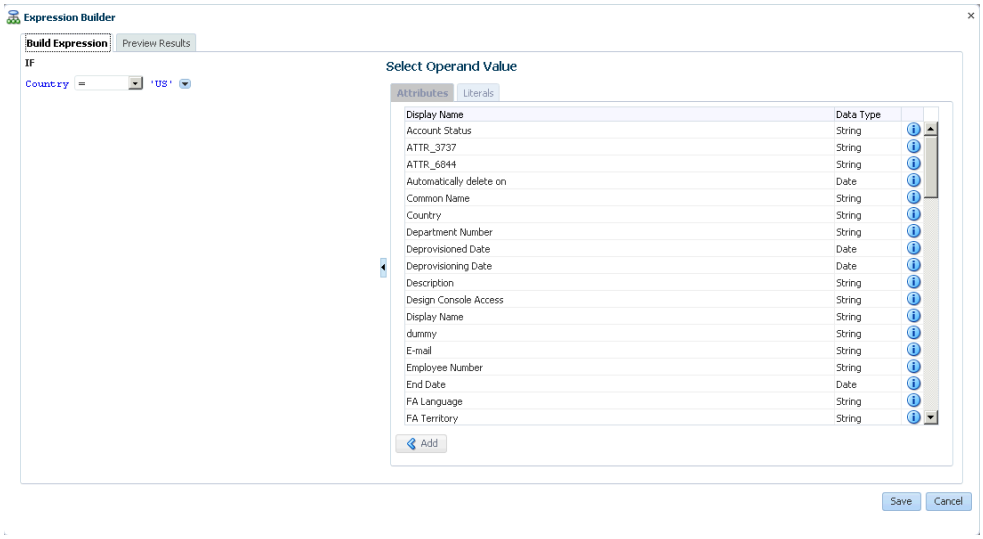
To create dynamic membership rule for an organization:

1. In the Members tab of the organization details page, click **Add Rule**. The Expression Builder is displayed.

2. In the Attributes tab, select an attribute, such as Country, and then click **Add**. The attribute is added to the expression builder for which you can specify a value. In addition, the Literals tab is displayed.
3. In the Value field, enter a value for the selected attribute, such as US, and then click **Add**. The value is added to the expression builder. The expression for the membership rule specifies that users with Country as US will be members of the selected organization.

   Figure 18-1 shows the Expression Builder with a sample dynamic organization membership rule.

Figure 18-1 Dynamic Organization Membership Rule



4. Click the **Preview Results** tab. This tab displays all the users that match the specified membership rule and will be assigned to the selected organization.
5. Click **Save**. The Members tab is displayed with the membership rule added in the User Membership Rule section.
6. Click any one of the following:
   - **Apply:** Clicking this button saves the membership rule for later evaluation. The users matching the rule criteria will be assigned to the selected organization when you run the Refresh Organization Memberships scheduled job. This scheduled job evaluates the changes in user-organization membership rules since the last job run and assigns users to organizations based on the rules. For more information about this scheduled job, see "Predefined Scheduled Tasks" in the *Administering Oracle Identity Governance*.
   - **Apply and Evaluate:** Clicking this button saves the membership rule and evaluates it against all users. As a result, the users that match the rule criteria are displayed in the list of members of the selected organization. The Relationship Type column for such users display Dynamic Member because these users are assigned to the selected organization based on the membership rule.
   - **Revert:** Clicking this button reverts the changes done after saving.

> **WARNING:**
>
> The membership rule will be lost if you close the organization details page without clicking any one of the Apply or Apply and Evaluate buttons.

18.4.5.3 Modifying a Dynamic Organization Membership Rule

To modify a user-membership rule:

1. In the User Membership Rule section of the Members tab, click **Edit Rule**. The Expression Builder is displayed with the user-membership rule.
2. If you want to change the attribute in the existing user-membership rule, then click the attribute to select it, and select another attribute in the Attributes tab. When finished, click **Add**.

   Similarly, you can click the value to change it and specify a different value.
3. To add more criteria to the user-membership rule, click the down arrow and select any operator, such as AND or OR. To remove the rule, select REMOVE. You can specify complex criteria by building an expression as required.
4. Click the **Preview Results** tab. This tab displays all the users that match the specified membership rule and will be assigned to the selected organization.
5. Click **Save**. The Members tab is displayed with the modified membership rule in the User Membership Rule section.

18.4.5.4 Deleting a Dynamic Organization Membership Rule

To delete a user-membership rule:

1. In the User Membership Rule section of the Members tab, click **Delete Rule**. A warning message is displayed asking for confirmation.
2. Click **Yes** to confirm the deletion.

After confirming the rule deletion, all the organization memberships are deleted immediately in the post-process. There is no offline evaluation for organization membership rule deletion.

18.4.6 Managing Admin Roles

You can view the admin roles that are assigned to the organization, assign admin roles to a user or revoke admin roles of a user.

In the Admin Roles tab, you can perform the following:

- About Admin Role in Organization Details
- Granting an Admin Role
- Revoking an Admin Role

18.4.6.1 About Admin Role in Organization Details

You can view the admin roles that are assigned to an organization by clicking the **Admin Roles** tab of the organization details page. The admin roles and their corresponding description are listed in this tab. When you select an admin role, the users who have the selected admin role are displayed in the User Members section. This tab also allows you to grant and revoke admin roles available to the open organization to users.

18.4.6.2 Granting an Admin Role

To grant an admin role to a user:

1. In the organization details page, click the **Admin Roles** tab. A list of admin roles assigned to the open organization is displayed.
2. Select the admin role that you want to grant to a user.
3. From the Actions menu, select **Assign**. Alternatively, click **Assign** on the toolbar. The Advanced Search for Target Users dialog box is displayed.
4. Search for the target users to whom you want to grant the selected admin role. You can select the **Just show my directs** option to list only your direct reports.
5. In the User Results section, select the user that you want to grant the admin role.
6. Click **Add Selected** to move the selected user to the Selected Users section. Alternatively, you can click **Add All** to move all the users from the User Results section to the Selected Users section.
7. Click **Select**. The admin roles is granted to the selected user. When you click the admin role in the Admin Roles tab, the selected user's record is displayed in the User Members section.
8. In the User Members section, select the user record. Select the **include sub-orgs** option to grant the admin role to the user's organization and its suborganizations. If you want to grant the admin role to the user's organization only, then do not select this option.

18.4.6.3 Revoking an Admin Role

To revoke an admin role from a user:

1. In the Admin Roles tab, select an admin role from which you want to revoke the user.
2. In the User Members section, select the user from whom you want to revoke the admin roles.
3. From the Actions menu, select **Revoke.** Alternatively, click **Revoke** on the toolbar. A message is displayed asking for confirmation.
4. Click **Revoke** to confirm. The user record is no longer displayed when you select the admin role.

   To revoke user from suborganizations of the currently opened organization, select the **include sub-orgs** option, and click **Apply** in the User Members section.

18.4.7 Viewing Available Accounts

The accounts available to an organization are the accounts that have been published to the organization. This means that the accounts are available for requesting by the users of the organization. The Available Accounts tab shows the accounts provisioned to users in the organization.

18.4.8 Viewing Provisioned Accounts

The Provisioned Accounts tab displays the accounts that have been provisioned to the open organization. You can provision a resource, revoke a resource, view the details of a provisioned resource, enable or disable a provisioned resource, or view the action history of a provisioned resource from the Provisioned Accounts tab.

In the Provisioned Accounts tab, you can perform the following:

- Provisioning a Resource
- Revoking a Resource
- Viewing the Details of a Provisioned Resource
- Disabling a Provisioned Resource
- Enabling a Provisioned Resource
- Viewing Resource History

18.4.8.1 Provisioning a Resource

To provision a resource to an organization:

1. In the Provisioned Accounts tab, from the Actions menu, select **Provision**. Alternatively, you can click **Provision** on the toolbar. The Provision Resource to Organization window is displayed.
2. In the Select Resource tab, search for the resource by Resource Name. Select the Resource from the Search Result table, and then click **Next**. The Provide Process Data tab is displayed.

> **Note:**
>
> In any search result in the Identity Self Service, you might not be able to select a control field or option, such as a row or a radio button, by pressing the `Tab` or `Space bar` keys. This is because some fields in a page are not accessible through the keys. Therefore, to pass accessibility test, run the JAWS tool, press the `Insert + F3` keys and select the control field. Then, you can select the rows or radio buttons from your key board.

3. In the Provide Process Data tab, select the required details and then click **Next**. The Review Summary tab is displayed.
4. You can review the summary, and then click **Finish**. Provisioning has been initiated message is displayed.

18.4.8.2 Revoking a Resource

To revoke a resource from an organization:

1. In the Provisioned Accounts tab, select the account that you want to revoke.
2. From the Actions menu, select **Revoke**. Alternatively, you can click **Revoke** on the toolbar.

   A message is displayed asking for confirmation.
3. Click **Yes**.

18.4.8.3 Viewing the Details of a Provisioned Resource

To view the details of a provisioned resource:

1. In the Provisioned Accounts tab, select the account you want to open.
2. From the Actions menu, select **Open**. Alternatively, you can click **Open** on the toolbar.

   The details of the account is displayed in a new page.

18.4.8.4 Disabling a Provisioned Resource

To disable a provisioned resource:

1. In the Provisioned Accounts tab, select the account you want to disable.
2. From the Actions menu, select **Disable**. Alternatively, you can click **Disable** on the toolbar.

   A message is displayed stating that the provisioned account has been successfully disabled.

18.4.8.5 Enabling a Provisioned Resource

To enable a resource provisioned to the organization:

1. In the Provisioned Accounts tab, select the resource you want to enable.
2. From the Actions menu, select **Enable**. Alternatively, you can click **Enable** on the toolbar.

   A message is displayed stating that the provisioned account has been successfully enabled.

18.4.8.6 Viewing Resource History

In the Provisioned Accounts tab of the organization details page, you can view the action history of a provisioned resource.

To view resource history:

1. In the Provisioned Accounts tab, select the resource for which you want to view the resource history.
2. From the Actions menu, select Resource History. Alternatively, click Resource History on the toolbar.

   The Resource History is displayed in a new window with the details of the provisioning tasks for the selected resource. It shows the task name, task status, date assigned, and the user to whom the resource is assigned to.
3. (Optional) To add a task to the resource history, click Add Task, select the radio button corresponding to the task name you want to add, and click **Add**.

> **Note:**
>
> By default, the first row of the table is selected, but the radio button on the row is not selected. Keep pressing `Shift + Tab` to navigate to the last row of the table. The radio button in the last row is now selected. Use the space bar to switch the radio button and Up /Down arrow keys to select the rows.

18.4.9 Viewing Available Entitlements

You can view the entitlements published to the open organization in the Available Entitlement tab.

For each entitlement, the following information is displayed:

- Entitlements name
- Resource associated with the entitlement
- Account name associated with the entitlement
- Organization name

18.5 Creating a User Member

You can create a user for the organization using the Create User option available on the organization details page.

The organization name is pre-filled in read only format on this create user page. The password policy of this organization is applicable when creating user and not the default password policy.

To create user:

1. In the organization details page, click **Create User** on the toolbar. Create user page is displayed.
2. Enter the required details. For description of the different fields see, Creating a User.
3. Click **Submit**.

18.6 Creating a Sub-Organization

Using the Create Organization page, you can create a sub-organization of type branch, company or department, control password behavior, and select applicable password policy for the organization.

To create a sub-organization for the open organization:

1. In the organization details page, click **Create Sub-org** on the toolbar. The Create Organization page is displayed. The open organization name is populated by default as the parent organization name.
2. Enter the organization attribute values, as described in Creating an Organization.
3. From the Enforce password policy on reassignment list, select a value to specify whether or not to enforce password policy on reassignment, or to inherit the password policy of the parent organization.
4. Click **Save**.

18.7 Disabling and Enabling Organizations

You can disable or enable an organization from the Search Organization page.

This section describes how to enable and disable organizations in the following topics:

- Disabling an Organization
- Enabling an Organization

> **Note:**
>
> You cannot disable organizations with child organizations or users. You can force disable it only by setting the value of the ORG.DisableDeleteActionEnabled system property to `true`. After you set this property, the users and suborganizations will be disabled while disabling the parent organization.

18.7.1 Disabling an Organization

To disable an organization with enabled state:

1. In the search result for organizations in the Search Organization page, select the organization that you want to disable.
2. From the Actions menu, select **Disable**. Alternatively, click **Disable** on the toolbar, or open the organization details page and click **Disable**.

   A message is displayed asking for confirmation.
3. Click **Disable** to confirm.

18.7.2 Enabling an Organization

To enable an organization with disabled state:

1. In the search result for organizations in the Search Organization page, select the organization that you want to enable.
2. From the Actions menu, select **Enable**. Alternatively, click **Enable** on the toolbar, or open the organization details page and click **Enable**.

   A message is displayed asking for confirmation.
3. Click **Enable** to confirm.

18.8 Deleting an Organization

Delete the organization that are not required or are not in use.

> **Note:**
>
> - You cannot delete organizations with child orgs or users. You can force delete it only by setting the value of the ORG.DisableDeleteActionEnabled system property to `true`. Once you set the property, the users and sub orgs will be deleted while deleting the parent org.
> - You can delete an organization only if you have the "Delete" permission for that organization.
> - The deleted record would still exist in the database, marked deleted.

To delete an organization:

1. In the search result for organizations in the Organization page, select the organization that you want to delete.
2. From the Actions menu, select **Delete**. Alternatively, click **Delete** on the toolbar, or click **Delete** on top of the organization details page.

   A message is displayed asking for confirmation.
3. Click **Delete** to confirm.

19

Managing Administration Roles

Managing administration roles involves understanding the administration roles feature supported by Oracle Identity Manager, understanding the admin role attributes, managing and configuring administration roles.

In this release, to control the actions that users can perform on others, administrators can use the Custom Administration Roles feature.

This chapter describes about the Administration Roles feature in the following sections:

- About Administration Roles in Oracle Identity Governance
- Introducing Admin Roles
- Understanding the Admin Role Attributes
- Searching Admin Role
- Creating an Admin Role
- Viewing and Modifying Admin Role
- Deleting Admin Role
- Controlling End User Actions

19.1 About Administration Roles in Oracle Identity Governance

Administration Roles feature of Oracle Identity Governance is used to control the actions that users can perform on other Oracle Identity Governance objects.

The authorization engine embedded in Oracle Identity Governance with the help of authorization policies facilitates this control. The purpose of authorization policies is to control user's access to Oracle Identity Governance application, which includes data, UI, and API. The authorization policies determine at runtime whether or not a particular action is allowed. Authorization policies can be defined that satisfy the authorization requirements within Oracle Identity Governance.

In Oracle Identity Governance, authorization policy management is centralized as an administrative feature. The Managing Admin Role feature of Oracle Identity Governance provides flexibility to create new admin roles and select the capabilities for the admin roles. You can select multiple capabilities from different entities. Oracle Identity Governance will hold the mapping of capabilities to admin roles. You can also define membership rule on user-assignment to admin roles.

> **Note:**
>
> Admin Roles should not be confused with roles, which are used to control user's access to external resources.

System Administrator having capability to manage admin roles will be allowed to publish the admin roles. They would publish the admin roles to organization and then the users from those organizations or having the manage-admin-roles capability on those organizations would be able to manage the admin roles.

19.2 Introducing Admin Roles

An Admin Role defines the actions, also known as functional capabilities, that can be performed and the scope of control (the scope of control refers to the set of organizations managed by the admin role).

Multiple admin roles can be assigned to a single administrator. This enables an administrator to have one set of capabilities in one scope of control, and a different set of capabilities in another scope of control. For example, one admin role might grant the administrator the right to create and edit users for the controlled organizations specified in that admin role. A second admin role assigned to the same administrator, might grant only the change user passwords right in a separate set of controlled organizations as defined in that admin role.

Admin roles enable the reuse of capabilities and scope-of-control pairings. Admin roles also simplify the management of administrator privileges across a large number of users. Instead of directly assigning capabilities and controlled organizations to individual users, admin roles should be used to grant administrator privileges.

There are two predefined admin roles in Oracle Identity Manager:

- System Administrator, that is the Oracle Identity Manager System Administrator role with all privileges.
- Catalog System Administrator, that is the role with privileges to manage all catalog items.

> **Note:**
>
> Role catalog attributes can be edited from the Roles page only and requires additional privilege.

19.3 Understanding the Admin Role Attributes

The Admin Role Capability, Scope of Control, and Publication are the attributes that are configured for an admin role.

This section describes about admin role attributes in the following topics:

- About Admin Role Capability
- About Admin Role Scope of Control
- About Admin Role Publication

19.3.1 About Admin Role Capability

Capabilities represent administrative functions with Oracle Identity Manager. Capabilities are collections of fine-grained actions. For example, the Create User

capability consists of two actions - Create User and View/Search User. Capabilities cannot be created and they cannot be assigned directly to users. Users are assigned capabilities using Admin Roles. Multiple capabilities can be assigned to an admin-role and capabilities can be selected from multiple entities. Capabilities will control on what a person is allowed to do or request for themselves and others.

> **Tip:**
>
> See Table B-1 for list of default capabilities which can be used while creating Admin Roles.

Oracle Identity Manager supports an additional level of granularity while granting the ability to modify or view users and their profiles through Denied Attributes. Administrators can specify which attributes cannot be modified or seen as part of assigning the Modify User or View/ Search User capability.

> **Note:**
>
> If an attribute is marked as denied for View/Search, it should also be marked as denied for the Modify User capability.
>
> Mandatory attributes and System generated attributes like Status, Display name, User Login and so on cannot be included in denied attributes list.

Users will not be allowed to perform any operation on behalf of home organization peers, such as, viewing user account or entitlements, request for roles or accounts and so on. Users need to be granted specific admin roles capabilities so that they can do any of the admin operations.

19.3.2 About Admin Role Scope of Control

Oracle Identity Manager allows you to control which users are within an admin's scope of control. Using Scope of Control, administrator can specify organizations that the members of the admin role can manage.

19.3.3 About Admin Role Publication

Oracle Identity Manager allows you to make the Admin Role available to organizations. Once the admin role has been published to these organizations, the organization administrators can grant them to other users. This helps in standardizing delegated administration and encourages reuse of admin roles.

19.4 Searching Admin Role

Use the Admin Roles page to perform simple and advanced search for admin roles.

To search for Admin Role you can perform one of the following:

- Performing Basic Search for Admin Role

- Performing Advanced Search for Admin Role

19.4.1 Performing Basic Search for Admin Role

To perform basic search:

1. Log in to Identity Self Service.
2. Click the **Manage** tab, click **Administration Roles** box. The Admin Roles page is displayed.
3. To perform basic search, select any one of the following search criteria from the **Search** drop-down and click **Search Admin Role** icon:
   - Display Name
   - Description
   - Name

   It lists the Admin Roles that match the selected Search Criteria.

19.4.2 Performing Advanced Search for Admin Role

To perform advanced search:

1. Log in to Identity Self Service.
2. Click the **Manage** tab, click **Administration Roles** box. The Admin Roles page is displayed.
3. Click **Advanced** link. Advance Admin Roles search page is displayed.
4. Select any one of the following **Match** options:
   - **All**: Search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.
   - **Any**: Search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.
5. In the **Display Name** field, enter the display name search attribute that you want to search. To do so, select a search comparator. The default search comparator is Starts With. Equals, Ends with, Does not equal, Contains, and Does not contain comparators are available in the list as an alternative.
6. In the **Description** and **Name** field, enter the appropriate values and the comparators required.
7. To add a field in your search:
   a. Click **Add Fields**, and select a field, such as Description or Name.
   b. Enter value for the search attribute that you added.

   If you want to remove a field that you added in the search, then click the cross icon next to the field.
8. To reorder the search element list, click **Reorder**. A Reorder Search Fields tab opens. Select the search element that has to be reordered and rearrange it using the arrow keys. Click **OK**.

   The order in which search elements are listed is modified accordingly.
9. Click **Search**. The results are displayed in the search results table.

19.5 Creating an Admin Role

Oracle Identity Manager provides flexibility to create new admin roles and select the capabilities for the admin roles. You can select multiple capabilities from different entities.

To create an Admin Role:

1. In Identity Self Service, click the **Manage** tab, click **Administration Roles** box. The Admin Roles Search page is displayed.
2. From the **Actions** menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Admin Role page is displayed.
3. In the **Basic Information** tab, enter Name, Display Name, and Description details and click **Next**. The **Capabilities** tab is displayed.

   Name is the only mandatory field and admin role name should have only alphabets and should not have numbers and space.
4. In the **Capabilities** tab, click **Add Capabilities**. Add Capabilities panel is displayed.

   To add Capabilities:

   a. Search for Capabilities by using search criteria as Display Name, Description, or Entity Name and click the Search icon. The search operator can be combined with wildcard characters to specify a search condition. The percentage sign (%) character is used as a wildcard character.

      Capabilities matching the search criteria are listed. The list has Name of capability, Description, and Attribute.

      > **Note:**
      >
      > - If the capability is a User Modify or View Search capability, then attribute column will show a link. To set an attribute as denied attribute, click this link. Attribute panel is displayed. From the list of attributes, select the attributes to be marked as denied attributes and click **OK**.
      > - For managing proxy users, if we create a custom admin role to manager the proxies, then apart form the above capabilities we need to explicitly add the **User - View / Search** capability to the admin role. This ensures the admin user can view and search for the users he wants to set as proxy.
      >
      > Mandatory attributes and System generated attributes like Status, Display name, User Login and so on cannot be included in denied attributes list.

   b. From the list of Capabilities, select the required capability and click **Add Selected** or to add all the listed capabilities click **Add All**.

   c. If you want to deselect any capabilities from Selected Capabilities list click **Remove Selected** or **Remove All** options.

   d. Click **Select**. Assign Capabilities Panel lists the Capabilities selected in Add Capability.

   Click **Next**. The Members tab is displayed.

5. In the Members tab, you can assign users (static assignment) and create membership rules (dynamically assignment).

> **Note:**
>
> For member assignment, scope of control is mandatory.

To create membership rules:

a. Click **Create Membership Rule** to open the User membership rules for role tab.

b. In the Expression Builder tab, under Attributes tab, select an attribute, such as Country, and then click **Add**. The attribute is added to the expression builder for which you can specify a value. In addition, the Literals tab is displayed.

c. In the Value field, enter a value for the selected attribute, such as US, and then click **Add**. The value is added to the expression builder. The expression for the membership rule specifies that users with Country as US will be members of the selected admin role.

d. Click **Save**. The Members tab is displayed with the membership rule added in the User Membership Rule section.

   Member Assignment tab displays the list of members matching the membership rule.

   Direct Members: This section displays the members that are statically assigned to the open role.

   Rule Based Members: This section displayed the members that are assigned to the open role via membership rules.

   All Members: This section displays all the members, direct and rule based which are assigned to the open role.

e. In case you want to evaluate the rule later, select **Evaluate Rule Later** check box. The rule can be evaluated later by running the *Refresh Admin-Role Memberships* scheduled task. If **Evaluate Rule Later** check box is not selected then, the rule is evaluated when the Admin Role is created.

To assign static users:

a. Click **Assign**. The Assign Users search dialog box is displayed.

b. Search for Users by using appropriate search criteria and click the Search icon. The search operator can be combined with wildcard characters to specify a search condition. The percentage sign (%) character is used as a wildcard character.

   Users matching the search criteria are listed.

c. From the list of users select the required user and click **Add Selected** or to add all the listed users click **Add All**.

   If you want to deselect any capabilities from Selected users list click **Remove Selected** or **Remove All** options.

d. Click **Select**. The Members tab is displayed with the assigned users in the Member Assignment section.

Click **Next**.The Scope of Control tab is displayed.

6. You can specify the organizations that this admin role can manage.

   To do so, click **Add Organizations**. Add Organization tab is displayed.

   a. Search for Organizations by using search criteria as Organization Name, Type, Organizations Status, or Parent Organization Name and click the Search icon.

      The search operator can be combined with wildcard characters to specify a search condition. The percentage sign (%) character is used as a wildcard character. Organizations matching the search criteria are listed.

   b. From the list of Organizations, select the required organization and click **Add Selected** or to add all the listed organizations click **Add All**.

      If you want to deselect any organization from Selected Organization list click **Remove Selected** or **Remove All** options.

   c. Click **Select**. The Scope of Control tab is displayed with the organizations in the Scope of Control section.

   Click **Next**. The Organizations tab is displayed.

7. You can publish the admin role to one or more organizations.

   To do so, click **Add Organizations**. Add Organization tab is displayed.

   a. Search for Organizations by using search criteria as Organization Name, Type, Organizations Status, or Parent Organization Name and click the Search icon.

      The search operator can be combined with wildcard characters to specify a search condition. The percentage sign (%) character is used as a wildcard character. Organizations matching the search criteria are listed.

   b. From the list of Organizations, select the required organization and click **Add Selected** or to add all the listed organizations click **Add All**.

      If you want to deselect any organization from Selected Organization list click **Remove Selected** or **Remove All** options.

   c. Click **Select**. The Organizations tab is displayed with the organizations in the Organizations section.

   Click **Next**.The Summary tab is displayed.

8. Summary tab lists all the information entered in the previous steps. Click **Finish**. This creates the new Admin Role.

19.6 Viewing and Modifying Admin Role

You can open the details of an admin role and edit the basic information, the capabilities, the members, the scope of control, and, the organizations.

To open the details of a role and modify it, perform one of the following:

1. In the Search Admin Roles page, search and select the admin role that you want to edit. From the Actions menu, select **Open**. Alternatively, click Open on the toolbar.
2. In the search results table of the Search Admin Roles page, click the Open Admin Role icon beside admin role name.
3. The details of the Admin role is displayed in a new page. Modify Admin role information in the following tabs of this page:

a. **Basic Information Tab**

   The Basic Information tab displays the Admin role attributes. Except for the Admin Role Name field (which is a read-only field), the rest of the fields in this tab are same as available in the Create Admin Role page. Other fields that can be modified in this tab are Display Name and Description.

   To modify the Admin role attributes, change the values in the fields, and click **Apply**.

b. **Capabilities Tab**

   The Capabilities tab displays the Capabilities the Admin role is assigned. You can add new capabilities or remove capabilities from the existing list.

   To add new Capabilities, click **Add**. Add Capabilities page is displayed. For adding capabilities refer to steps in Creating an Admin Role.

   To remove an existing Capability, select the capability in the list and click **Remove**. Click **Apply**.

c. **Members** Tab

   The Members tab displays the User Membership Rules and Member assignment for the Admin role.

   To edit Rule, click **Edit Rule**. For steps refer to Creating an Admin Role .

   To delete rule, click **Delete Rule**.

   To add new Users, click **Assign**. For steps refer to Creating an Admin Role.

   Click **Apply**.

d. **Scope of Control** Tab

   The Scope of Control tab allows you to specify the organizations that this admin role can manage.

   To assign more Organization, click **Assign**. For steps refer to Creating an Admin Role.

   To remove an organization from the list, select the organization and click **Revoke**. Click **Apply**.

e. **Organizations** Tab

   The Organization tab allows you to publish the admin role to one or more organizations.

   To assign more Organization, click **Assign**. For steps refer to Creating an Admin Role.

   To remove an organization from the list, select the organization and click **Revoke**. Click **Apply**.

19.7 Deleting Admin Role

Delete the admin roles that are not required or are not in use.

To delete an Admin Role:

1. In the Search Admin Roles page, search and select the admin role that you want to Delete.

2. From the **Actions** menu, select **Delete**. Alternatively, click **Delete** on the toolbar. A warning message is displayed to confirm deletion of the Admin Role. Click **Delete.**

19.8 Controlling End User Actions

Admin Roles are used to control the actions that a user can perform on other users and objects. To control the actions that an end-user can perform on themselves, administrators need to configure Self Service Capabilities.

For more information on Self Service Capabilities, see "Managing Self Service Capability Policy" in the *Administering Oracle Identity Governance*.

20
Managing Password Policies

You can specify different password policies for different organizations, allowing granular control of passwords and challenge questions.
This chapter describes about the password policy management in the following sections:

- About Password Policies
- Searching Password Policies
- Creating a Password Policy
- Understanding Password Policy Rules
- Evaluating Password Policies
- Setting Challenge Options
- Deleting a Password Policy
- Associating Password Policies with Organization

20.1 About Password Policies

The Oracle Identity Manager provides a common password policy management framework between Oracle Identity Manager and Oracle Access Manager (OAM). It also introduces the concept of a challenge policy, which allows you to specify whether challenge questions are system-defined or end-user defined (or a combination of both).

Organization administrators can associate a password policy to an organization. The organization administrators can select a relevant password policy from the password policies created by system administrators. A password policy set for an organization is applicable for that organization and all its suborganizations. If the suborganization-level administrator sets a different password policy for that organization, then the parent organization password policy is overridden by the new one, and is applicable to all suborganizations under this organization. If a user is a member of multiple organizations, then the user's password policy depends on the home organization and the home organization hierarchy.

In addition, password policy priority determines which password policy is applicable for a user if the user is a member of multiple organizations. If the organizations are in hierarchy, then the password policy of the organization that is closest to the user is applicable even if the password policy associated with the parent organization has higher priority.During user creation, Oracle Identity Manager validates the password provided manually or autogenerated against the default password policy which is attached to the Top organization. When a user logs in for the first time and changes the password, the password policy with the highest priority that is applicable to the user's organization is applied.

20.2 Searching Password Policies

Use the Password Policy page to perform simple and advanced search for password policy.

To search for Password Policies you can perform one of the following:

- Performing Basic Search for Password Policies
- Performing Advanced Search for Password Policies

20.2.1 Performing Basic Search for Password Policies

To search for password policies:

1. Login to Identity Self Service.
2. Click **Manage**. Place your mouse pointer on the **Policies** box, and click **Password Policies**. The Password Policy page is displayed.
3. In the Policy Name field, enter the policy name you want to search.
4. Click **Search**. The password policies that match search condition **Policy Name** is displayed.

20.2.2 Performing Advanced Search for Password Policies

To perform advanced search:

1. Log in to Identity Self Service.
2. Click **Manage**. Place your mouse pointer on the **Policies** box, and click **Password Policies**. The Password Policy page is displayed.
3. Click **Advance** link. Advance Password Policies search page is displayed.
4. Select a search comparator. The default search comparator is Starts With. Other options are Equals, Ends with, Does not equal, and Contains.

   You can use wildcard characters to specify the Password Policy name.
5. To add a field to your search:
   a. Click **Add Fields**, and select Policy Name.
   b. Enter value for the search attribute that you added.

   This option is useful to create complex conditions such as Policy Name starts with *Test* and Policy Name ends with *User*. In this case two fields have to be included.

   If you want to remove a field that you added in the search, then click the cross icon next to the field.
6. To reorder the search element list, click **Reorder**. A Reorder Search Fields tab opens. Select the search element that has to be reordered and rearrange it using the arrow keys. Click **OK**.

   The order in which search elements are listed is modified accordingly.
7. Click **Search**. The results are displayed in the search results table.

20.3 Creating a Password Policy

Creating a password policy involves setting password restrictions, challenge question restrictions, and rules that are associated with a password policy.

By creating password policies, you can:

- Set password restrictions, for example, define the minimum and maximum length of passwords

- Set challenge question restrictions
- See rules that are associated with a password policy

> **Note:**
>
> In an environment in which LDAP synchronization is enabled, you must ensure one of the following:
>
> - Password policies set on Oracle Identity Manager must be more restrictive than password policies set on the LDAP server.
> - Password policies set on Oracle Identity Manager must match the password policies set on the LDAP server.

To create a password policy:

1. In the Password Policy page, from the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar.
2. In the Policy Name field, enter the name of the password policy.
3. In the Description field, enter a short description of the password policy.
4. In the Policy Rules tab, specify value to set the rules for the password policy. For a description of each field in the Policy Rules tab, see Understanding Password Policy Rules.

   > **Note:**
   >
   > You can leave the fields blank in the Policy Rules tab, and click **Apply** to save the password policy. You can later open the password policy and set the policy rules by following the instructions in Understanding Password Policy Rules.

5. In the Challenge Options section, select **Enable Challenge Policy Support** to enable configuring challenge policy options. For a description of each field in the Challenge Options section, see Setting Challenge Options.
6. Click **Apply**.

> **Note:**
>
> A password policy is not applied during the creation of an Oracle Identity Manager user through trusted source reconciliation.

20.4 Understanding Password Policy Rules

Setting password policy rules involves specifying criteria for your password policy in the Policy Rules section of the password policy details page.

This section describes the password policy rules in the following topics:

- Password Policy Rules
- Setting Password Policy Rules

20.4.1 Password Policy Rules

Setting password policy rules involves specifying criteria for your password policy, for example, the minimum and maximum length of passwords.

You can use either or both of the following methods to set password restrictions:

- Enter information in the appropriate fields, or select the required check boxes. For example, to indicate that a password must have a minimum length of four characters, enter **4** in the Minimum Length field.
- In the Password File field, enter the directory path and name of the password policy file (for example, c:\Xellerate\userlimits.txt). This file contains predefined words that you do not want to be used as passwords. The delimiter specified in the File Delimiter field separates these words. The predefined words in the file cannot be used as passwords. For example, if the file contains the word welcome, then welcome, Welcome, and welcome123 are invalid passwords.

20.4.2 Setting Password Policy Rules

To set the rules for a password policy:

1. In the Password Policy page, search and select the password policy that you want to open.
2. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar. The password policy details page is displayed.

> **Note:**
>
> You can also set the password policy rules at the time of creating the password policy.

3. In the Policy Rules tab, enter values in the fields, as listed in Table 20-1:

> **Note:**
>
> If a data field of the policy is empty, a password conforming to this policy does not have to meet the criteria of that field for the password to be valid. For example, when the Minimum Numeric Characters field is blank, Oracle Identity Manager will accept a password, regardless of the number of characters included in it.

Table 20-1 Fields in the Policy Rules Section

Field Name	Description
Minimum Length	The minimum number of characters that a password must contain for the password to be valid. For example, if you enter **4** in the Minimum Length field, then the password must contain at least four characters. This field accepts values from 0 to 999.
Minimum Password Age (Days)	The minimum duration in days for which users can use a password. For example, if you enter **2** in the Minimum Password Age (Days) field, then the user cannot change the password before 2 days of creating the password. The value of this field must be less than the value of the Expires After (Days) field. For example, if you enter 30 in the Expires After (Days) field and 31 in the Minimum Password Age (Days) field, then an error is displayed.
Warn After (Days)	The number of days that must pass before a user is notified that the user's password will expire on a designated date. For example, you enter **30** in the Expires After (Days) field, and **20** in the Warn After (Days) field, and the password is created on November 1. On November 21, the user will be informed that the password will expire on December 1. This field accepts values from 0 to 999.
Disallow Past Passwords	The frequency at which old passwords can be reused. This policy ensures that users do not change back and forth among a set of common passwords. For example, if you enter **10** in the Disallow Past Passwords field, then users are allowed to reuse a password only after using 10 unique passwords. This field accepts values from 0 to 24.
Expires After (Days)	The maximum duration in days for which users can use a password. For example, if you enter **30** in the Expires After Days field, then users must change their passwords by the thirtieth day from when it was created or last modified. This field accepts values from 0 to 999. **Note:** After the number of days specified in the Expires After Days field passes, a message is displayed asking the user to change the password.

4. You can configure either a default complex password policy or a custom password policy. If you select the **Complex Password** option, then you cannot use the Custom Policy option setup, and passwords will be evaluated against the complex password criteria.

   - **Complex Password:** Selecting this option sets the following complex password criteria:
     - The password is at least six characters long.
     - The password contains characters from at least three of the following five categories:

       - English Uppercase Characters (A - Z)

       - English Lowercase Characters (a - z)

       - Base 10 digits (0 - 9)

- Non-alphanumeric characters (for example: !, $, #, or ^)

- Unicode characters

– The password does not contain any of User ID, first name, or last name when their length is larger than 2.

  The names are parsed for delimiters: commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs. If any of these delimiters are found, then the names are split and all sections are verified not to be included in the password. For example, if the user name is john-d, then d will not be checked in the password because its length is less than 2. Similarly, if the name is John Richard Doe, then the password cannot contain john, richard, or doe.

  When checking against the user's full name, characters such as commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs are treated as delimiters that separate the name into individual character sets. Each character set that has three or more characters is searched in the password. If the character set is present in the password, the password change is rejected. For example, the name John Richard-Doe is split into three character sets: John, Richard, and Doe. This user cannot have a password that consists of three continuous characters from either John or Richard or Doe anywhere in the password. However, the password can contain the substring d-D because the hyphen (-) is treated as the delimiter between the substrings Richard and Doe. In addition, the search for character sets in the password is not case-sensitive.

  > **Note:**
  >
  > After applying Oracle Identity Governance Bundle Patch 12.2.1.4.200624, a new system property is available with name `OIM Complex Password Policy compatible with Active Directory` and keyword `OIM.ADPasswordPolicyCompatibilityEnabled`. If you want to replace the last rule (inclusion of user ID, first name, or last name in password) of the OIG complex password policy with the Active Directory (AD) password policy (inclusion of Display Name and User Login in password), then set the value of the `OIM Complex Password Policy compatible with Active Directory` system property to `TRUE`. This property is applicable to all complex password policies. See Default System Properties in Oracle Identity Governance in *Administering Oracle Identity Governance* for more information about this system property.

> **Note:**
>
> If the user's full name is less than three characters in length, the password is not checked against it because the rate at which passwords will be rejected is too high.

- **Custom Policy:** If you select the **Custom Policy** option, you can set a custom password policy by using the fields listed in Table 20-2.

Table 20-2 Fields in Custom Policy Section

Field Name	Description
Maximum Length	The maximum number of characters that a password can contain. For example, if you enter **8** in the Maximum Length field, then a password is not accepted if it has more than eight characters. This field accepts values from 1 to 999.
Maximum Repeated Characters	The maximum number of times a character can be repeated in a password. For example, if you enter **2** in the Maximum Repeated Characters field, then a password is not accepted if any character is repeated more than two times. For example, RL112211 would not be a valid password because the character `1` is repeated three times. **Note:** In this example, there are four occurrences of the character `1`, which means that it is repeated three times. This field accepts values from 1 to 999.
Minimum Numeric Characters	The minimum number of digits that a password must contain. For example, if you enter **1** in the Minimum Numeric Characters field, then a password must contain at least one digit. This field accepts values from 0 to 999.
Minimum Alphanumeric Characters	The minimum number of letters or digits that a password must contain. For example, if you enter **6** in the Minimum Alphanumeric Characters field, then a password must contain at least six letters or numbers. This field accepts values from 0 to 999.
Minimum Unique Characters	The minimum number of nonrepeating characters that a password must contain. For example, if you enter **1** in the Minimum Unique Characters field, then a password is accepted if at least one character in the password is not repeated. For example, 1a23321 would be a valid password because the character `a` in the password is not repeated although the remaining characters are repeated. This field accepts values from 0 to 999.
Minimum Alphabet Characters	The minimum number of letters that a password must contain. For example, if you enter **2** in the Minimum Alphabet Characters field, then the password is not accepted if it has less than two letters. This field accepts values from 0 to 999.
Minimum Uppercase Characters	The minimum number of uppercase letters that a password must contain. For example, if you enter **8** in the Uppercase Characters: Minimum field, then a password is not accepted if it contains less than eight uppercase letters. This field accepts values from 0 to 999.
Minimum Lowercase Characters	The minimum number of lowercase letters that a password must contain. For example, if you enter **8** in the Minimum Lowercase Characters field, then a password is not accepted if it has less than eight lowercase letters. This field accepts values from 0 to 999.

Table 20-2 (Cont.) Fields in Custom Policy Section

Field Name	Description
Special Characters: Min	The minimum number of special characters that a password must contain. For example, if you enter **2** in the Special Characters: Min field, then the password is not accepted if it has less than two special characters. The field accepts values from 0 to 999.
Special Characters: Max	The maximum number of special characters that a password can contain. For example, if you enter **5** in the Special Characters: Max field, then a password is not accepted if it has more than five special characters. This field accepts values from 1 to 999.
Unicode Characters: Min	The minimum number of Unicode characters that a password must contain. For example, if you enter **3** in the Unicode Characters: Minimum field, then the password is not accepted if it has less than three Unicode characters. This field accepts values from 0 to 999.
Unicode Characters: Max	The maximum number of Unicode characters that a password can contain. For example, if you enter **8** in the Unicode Characters: Maximum field, then a password is not accepted if it has more than eight Unicode characters. This field accepts values from 1 to 999.
Password File	The path and name of a file that contains predefined terms, which are not allowed as passwords. The file must be stored on the same host on which Oracle Identity Manager is deployed. **Note:** The settings on the Policy Rules tab get precedence over the specifications in the password file. For example, a disallowed term of the password file is used in the policy when no disallowed term is specified in the Policy Rules tab.
File Delimiter	The delimiter character used to separate terms in the password file. For example, if a comma (,) is entered in the Password File Delimiter field, then the terms in the password file will be separated by commas. **Note:** There are no escape characters defined to be used in password policies.

Table 20-2 (Cont.) Fields in Custom Policy Section

Field Name	Description
Characters Required	The characters that a password must contain. For example, if you enter **x** in the Characters Required field, then a password is accepted only if it contains the character x. The character you specify in the Characters Required field, must be mentioned in the Characters Allowed field. If you enter a character in the Characters Required field that is not mentioned in the Characters Allowed field, then an error is displayed stating that the required characters must be in the list of allowed characters, and required characters must not be in the list of not allowed characters. In addition, if you specify more than one character, then do not provide delimiters. Commas and white spaces are also considered as characters in this field. For example, if you specify characters such as a,x,c, then the password is not accepted unless it contains comma. **Note:** Characters specified and case-sensitive.
Characters Allowed	The characters that a password can contain. For example, if you enter the percent sign (%) in the Characters Allowed field, then a password is accepted if it contains a percent sign, given that all other criteria are met. **Note:** If any character is used in the password and that character is not in the Characters Allowed field, then the password will be rejected. For example, if the Characters Allowed field has "abc" and the password is "dad", then the password is rejected because "d" is not in the Characters Allowed field. If you specify the same character in the Characters Allowed and Characters Not Allowed fields, then an error message is returned when you create the password policy. **Note:** Characters specified and case-sensitive.
Characters Not Allowed	The characters that a password must not contain. For example, if you enter an exclamation point (!) in the Characters Not Allowed field, then a password is not accepted if it contains an exclamation point. **Note:** Characters specified and case-sensitive.
Substrings Not Allowed	A series of consecutive alphanumeric characters that a password must not contain. For example, if you enter **oracle** in the Substrings Not Allowed field, then a password is not accepted if it contains the letters o, r, a, c, l, and e, in successive order.
Maximum Incorrect Login attempts counter	The maximum number of incorrect login attempt is allowed for a user. After the maximum number of attempts is failed, user is locked. You can set if the user is locked permanently or for a time duration. When a value is entered in this field it enables **Permanent Lockout** and **Lock Duration**.
Permanent Lockout	If an user exceeds maximum incorrect login attempt, then the user can be permanently lockout. To enabled this select this check box. If this option is enabled then you will not be allowed to set Lock Duration time. Note: Only Admin can unlock the user if this option is enabled.

Table 20-2 (Cont.) Fields in Custom Policy Section

Field Name	Description
Lock Duration	If an user exceeds maximum incorrect login attempt, then the user can be locked for a certain period of time. The duration for which the user is locked is set in minutes. For example, if lock duration is set to 5 minutes, user will get unlocked after 5 minutes of the user being locked. If Permanent Lockout is enabled then this field is not applicable.
Start with Alphabet	Whether or not the password must begin with a letter. For example, if you select this option, then the password 123welcome is not accepted because the password does not begin with a letter. However, if you do not select this option, then the password can begin with a letter, numeric digit, or special character.
Disallow First Name	This check box specifies if the user's first name will be accepted as the whole password or as part of the password. When this check box is selected, a password will not be valid if the user's first name is entered in the Password field. In addition, the password is not valid is the first name is entered as a part of the password. If you deselect this check box, then the password will be accepted, even if it contains the user's first name.
Disallow User ID	This check box specifies if the user ID will be accepted as the whole password or as part of the password. When this check box is selected, a password will not be valid if the user ID is entered in the Password field. In addition, the password is not valid if the user ID occurs as a part of the password specified in the Password field. If you deselect this check box, the password will be accepted, even if it contains the user ID.
Disallow Last Name	This check box specifies if the user's last name will be accepted as the whole password or as part of the password. When this check box is selected, a password will not be valid if the user's last name is entered in the **Password** field. In addition, the password is not valid is the last name is entered as a part of the password. If you deselect this check box, then the password is accepted, even if it contains the user's last name.
Disallow White Space	This check box specifies whether or not the password can include a white space. When this check box is selected, a password will not be valid if it contains a white space. If you deselect this check box, then the password with a white space will be accepted. **Note:** This field is unchecked by default, unless the value for **Characters not allowed** field has a white space included.

5. Click **Apply** to save the password policy.

> **Note:**
>
> After creating a password policy, you must associate the policy with an organization. The rules of the policy will be applied for the users of that organization and its suborganizations. For information see, Evaluating Password Policies.

20.5 Evaluating Password Policies

Oracle Identity Manager evaluates the password policy that is applicable to a user when user registers to Oracle Identity Manager or when user resets forgotten password.

In Oracle Identity Manager, password policies are evaluated in the following scenarios:

- When users register themselves to Oracle Identity Manager to perform certain tasks in Identity Self Service or Oracle Identity System Administration.
- When users reset their password using the Forgot Password? link.
- When users change their enterprise password or target system account password from the Change Password section of the My Information page.
- When an administrator sets or changes the password of a user manually.

The following is the order in which a user's effective password policy is evaluated:

1. The password policy (if available) set for the user's home organization is applicable for the user.
2. If no password policy is set for the user's home organization, then the policy of the organization at the next level in the organization hierarchy of the user's home organization is picked. This procedure of identifying an organization at the next level in the hierarchy of the user's home organization continues until an organization associated with a password policy is determined. This password policy is applicable to the user.
3. If none of the organizations in the hierarchy has password policies set, then the password policy attached to the Top organization is applicable. If no password policy is attached to the Top organization, then the default password policy of the XellerateUsers resource is applicable.

20.6 Setting Challenge Options

Oracle Identity Manager allows administrator to configure the set of challenge question that is shown to the user to validate the user's identity before resetting forgotten password.

To set the Challenge question options for a password policy:

1. In the Password Policy page, search and select the password policy that you want to open.
2. From the Actions menu, select **Open**. Alternatively, click **Open** on the toolbar. The password policy details page is displayed.

> **Note:**
>
> You can also set the Challenge option at the time of creating the password policy.

3. In the Challenge Options section, if **Enable Challenge Policy support** is enabled then the fields listed in Table 20-3 can be configured:

Table 20-3 Fields in the Challenge Option Section

Field Name	Description
Allowed Challenges	This field allows you to select which set of challenge question is shown to the user. The options are: User Defined, Admin Defined, or User or Admin Defined. If User Defined is selected, then the challenge questions is set by the user. If Admin Defined is selected, then the challenge questions is selected from the list provided by the admin. If User or Admin Defined is selected, then the combination of questions is admin defined and user customized.
Total Questions To Be Collected	This determines the total number of challenge questions a user needs to provide at login.
Minimum Correct Answers When Challenged	The minimum number of correct answers the user needs to provide when he is asked the challenge questions.
Allow Duplicate Responses	This allows you to select if duplicate responses are allowed or not.
Minimum Answer Length	The minimum length of answer for the challenge questions.
Lock User After Attempts	The number of attempts before the user is locked if he provided wrong answers to the challenge questions.

4. When Allowed Challenges is set to Admin Defined or User or Admin Defined, challenge questions have to be added. The number of challenge question is determined by **Total Questions To Be Collected** field.

   To add questions:

   a. Under Challenge Questions section, click **Add**.

   b. Enter the challenge question in the Questions table. To include more questions, click **Add**.

   c. To delete a question, select the question and click **Delete**.

> **Note:**
>
> If you have customized the challenge questions, then modify the `customResources` properties under the *IDM_HOME*/server/customResources/ directory to add your local messages.

5. Click **Apply** to save the password policy changes.

20.7 Deleting a Password Policy

Delete the password policy that are not required or are not in use.

To delete a password policy:

1. In the Password Policy page, search and select a password policy that you want to delete.
2. From the Actions menu, select **Delete**. Alternatively, click **Delete** on the toolbar. A message is displayed asking for confirmation.
3. Click **Yes** to confirm the deletion.

20.8 Associating Password Policies with Organization

To associate the password policy with an organization and use the password policy to manage the passwords of Oracle Identity Manager users, see Creating an Organization.

To associate the password policy with a resource, see "Configuring Password Policies for Application Instances" in the *Administering Oracle Identity Governance*.

21
Managing Application Onboarding

Use the application onboarding capability in Oracle Identity Self Service to create and manage applications, templates, flat file configuration for applications, instances of applications, manage jobs, upgrade the applications, and to clone applications.

This chapter contains the following sections:

- About Application Onboarding
- Searching Applications
- Creating Applications
- Creating Templates
- Modifying Applications
- Cloning Applications
- Creating Instance Applications
- Creating Applications in Bulk
- Configuring Flat Files
- Managing Flat File Configurations
- Managing Jobs
- Upgrading Connector Applications
- Deleting Applications
- About Customizing Groovy Scripts
- Troubleshooting Application Onboarding

> **Note:**
>
> The Design Console has been deprecated in this release. Use the new Applications page in Identity Self Service to do any of the following:
>
> - Application template-based install process should be used in ICF-based connector install package.
> - Install the template-based 12c connectors.
> - Manage IT resource instances for template-based applications.

21.1 About Application Onboarding

This section describes the following concepts:

- What Is Application Onboarding?

- Application Onboarding Concepts

21.1.1 What Is Application Onboarding?

Application onboarding is the process of registering or associating an application with Oracle Identity Governance so that Oracle Identity Governance can provision or reconcile user information in or from that application.

Oracle Identity Governance provides a quick and convenient way to onboard applications by using the Applications option on the Manage tab in Identity Self Service. You can perform all the necessary configurations to onboard an application from a single console.

This simplified solution has the following benefits:

- You can configure new or existing applications by using a single user interface: Identity Self Service.
- You can export configurations as application templates and configure applications by using these templates, instead of Oracle Identity Governance.

21.1.2 Application Onboarding Concepts

Some of the key concepts related to the Application onboarding are application authorization, types of application, application templates, disconnected connector applications, instance creation, cloning of applications, validation and transformation of provisioning and reconciliation attributes, and application template elements.

The concepts related to application onboarding are described in the following sections.

- Application Authorization
- Application Types
- Application Templates
- Disconnected Applications
- Instance Creation
- Cloning Applications
- Validation and Transformation of Provisioning and Reconciliation Attributes
- Important Elements in the Application Template XML

21.1.2.1 Application Authorization

Users can access the Application option in Identity Self Service if they have the following authorizations:

- Any user with the **Application Instance Administrator** or **System Administrator** admin role can manage the application using the Application option.
- Any user with the **Application Instance Administrator** admin role can manage the entire life cycle of the applications published within the user's home organization and in the organizations that are within the scope of control of the admin role.

21.1.2.2 Application Types

You can create two types of applications:

- **Target Application**: A target application allows user requests for provisioning accounts through the access request catalog. The target application can be either connected or disconnected. The disconnected applications must be manually provisioned.
- **Authoritative Application**: For an authoritative application, Oracle Identity Governance manages accounts and represents them as users across different reconciliation jobs. Authoritative applications cannot be requested through the access request catalog. Therefore, Oracle Identity Governance pulls data and represents the applications as users, and then grants different target applications through requests or access policies. For example, the HRMS applications that are managed entirely by an HR department. The HRMS applications involve user account creation. Oracle Identity Governance pulls data from the HRMS application and represents these as user accounts. These user accounts are granted to various target applications through requests and approvals.

The application onboarding capability in Identity Self Service allows you to create applications in two ways:

- **From a connector package**: Oracle Identity Governance provides predefined connectors with default templates, which includes all the target system-specific details, such as provisioning and reconciliation mappings, reconciliation actions, and reconciliation matching rules.

  > **Note:**
  >
  > You can install the predefined connectors for which default templates are not available by using the **Manage Connector** option on the Provisioning Configuration tab in the Identity System Administration interface.

- **Using application templates**: If saved application templates are present in the system, then you can create new applications by using these templates.

21.1.2.3 Application Templates

An application template is an XML representation of all the configurations that are relevant to an application instance. It contains all the information required for provisioning to a target system and reconciliation from a target system. In addition, it contains other details, such as publication information, connectivity details, and other advanced configurations that are specific to a target system. You can save an application configuration as a template and use it later to create an application. Application templates must be placed in a folder.

You can create application templates in the following ways:

- Create a template by clicking the **Save as Template** option in the Create Application page. See Creating Applications.
- Run the Application Template Generation Job scheduled task to generate the template. The folder in which this template is to be saved is passed as a parameter to the job. This may be useful for applications that are created by using the Connector Installer before or after an upgrade. By default, templates are not generated for these applications.

See Predefined Scheduled Tasks in *Administering Oracle Identity Governance* for information about this scheduled task.

- Import templates by using the Import option in the Deployment Manager. See Importing Deployments in *Administering Oracle Identity Governance* for information about importing entities by using the Deployment Manager.
- Create a template manually by using the sample template.

> **Note:**
>
> - For authoritative applications, create an application instance by using the `ApplicationInstanceService.addApplicationInstance(ApplicationInstance appInst)` API, and then run the Application Template Generation Job to generate the template. See Java API Reference for Oracle Identity Governance for information about this API.
> - The applications that are created through the **Create Application** option contains the schema attributes related to all the values present in the lookup. These schema attributes might include attributes that are previously derived attributes, such as `_NAME_`. When a new UI form is created, these attributes must be removed. To remove these attributes, customize the form by using a sandbox.
>
>   See Managing Forms in *Administering Oracle Identity Governance* for more information on customizing forms by using sandboxes.

21.1.2.4 Disconnected Applications

Disconnected resources are targets for which there are no connectors. Therefore, you must provision these resources manually. You can create applications for disconnected resources from the Applications page in the Identity Self Service.

See Managing Disconnected Resources in *Administering Oracle Identity Governance* for information about disconnected resources and disconnected application instances.

21.1.2.5 Instance Creation

You can create an instance of an application that shares the configurations of the base application but includes different connectivity options.

The following configurations are shared between the base and instance applications:

- Advanced configuration
- Schema configuration
- Provisioning configuration
- Reconciliation configuration

An instance application has its own attributes and configurations for:

- Application Name
- Application Display Name

- Application Description
- Basic Configurations
- Catalog attributes
- Organization publication

> **Note:**
>
> Configurations that are shared with the base application cannot be modified by editing an application from the Applications page.

21.1.2.6 Cloning Applications

When an application is cloned, all the configurations of the base application are copied into the cloned application.

21.1.2.7 Validation and Transformation of Provisioning and Reconciliation Attributes

When you create an application from the Identity Self Service, you can apply, validate, and transform provisioning attributes before passing the attributes to the target system. Application onboarding capability in Identity Self Service lets you write Groovy script-based validation and transformation logic. See Creating a Target Application or Creating an Authoritative Application for more information on how to include these scripts.

Suppose you want to manage accounts on an Oracle Database target through Oracle Identity Governance. This situation has the following requirements:

- The account fields are User ID, Organization, First Name, and Last Name.
- The User ID field cannot be null.
- The user ID must end with *@example.com*. For example, if the user ID is test, then during the request it must be transformed to *test@example.com* on the target.
- If the user does not provide organization details, then the default value must be set to Server Technology.

To meet these requirements, you can create the following validation script and transformation script while creating the application.

Validation Groovy Script:

```
def errors = "";
if(User_Id == null || User_Id ==""){
errors = errors+" User Id cannot be null";
}
return errors;
```

Transformation Groovy Script:

```
if(Organization == null || Organization == "")
{
```

```
    Organization = "Server Technology";
}
User_Id = User_Id.toString()+"@example.com";
```

Validation Groovy Script for Resource Exclusion:

In the validation script, you can specify a list of user IDs for accounts that must be excluded from reconciliation and provisioning operations. The following is a sample script to do so:

```
def errors = "";
def excludedUsers = ['user01','user02'];
def regexStr = /^[a-zA-Z0-9_]+/;
if(!User_Id.matches(regexStr)) errors = errors+" Invalid UserId";
if(excludedUsers.contains(User_Id)) errors = errors+" User Id lies in
excluded list";
return errors;
```

See About Customizing Groovy Scripts for more sample scripts and information about transformation of attributes.

21.1.2.8 Important Elements in the Application Template XML

Some important elements and structures of the application template XML file are:

- `applicationName`: The application name. It must be unique and cannot be more than 200 characters.
- `applicationDisplayName`: Display Name of the application.
- `connectorDisplayName`: The connector display name is used for locating the connector bundle and is a read-only field for the user. The value is included with the default template in the connector bundle.
- `connectorVersion`: The connector version is used for locating the connector bundle and is a read-only field for the user. The value is included with the default template in the connector bundle.
- `basicConfigurations`: The connectivity details for a target system, such as host and port. The list of parameters varies from target to target.
- `advanceConfigurations`: The target specific configurations, which are used by the bundle while performing provisioning or reconciliation to or from the target system. The list of parameters varies from target to target.
- `objectClass`: Each template has at least one object class that represents the object on the target system to be provisioned or reconciled.
  - `provisioningConfig`: Provisioning related configurations:
    - `validationScript`: Groovy validation scripts that are executed before provisioning on the target system.
    - `transformationScript`: Groovy transformation scripts that are executed before provisioning the data.
    - `capabilities`: A list of operations supported by the bundle on the target system.

- `reconConfig`: Reconciliation related configurations:
  - `reconJobDetails`: A list of jobs that reconcile the data into Oracle Identity Governance.
  - `identityCorrelationRule`: The rule for owner matching. This rule is defined between the target attribute and the Oracle Identity Governance user attribute.
  - `situationResponses`: A list of situations and their corresponding responses. For example, for an Authoritative Application, in a situation of *No Matches Found*, the response may be *Create User*.

    For a Target Application, in a situation of *No Matches Found*, the response may be *Establish Link*.
  - `validationScript`: Groovy validation scripts that are executed before reconciling the data into Oracle Identity Governance.
  - `transformationScript`: Groovy transformation scripts that are executed before reconciling the data into Oracle Identity Governance.
- `form`: Specifies one parent form per `objectClass`.
  - `schemaAttributes`: The schema configuration for `objectClass`. Each schema attribute has the following attributes:
    - `name`: The name of the attribute on the target system.
    - `dataType`: The data type of the attribute. For example, String.
    - `displayName`: The name of the attribute in Oracle Identity Governance.
    - `length`: The length of data that can be stored in the attribute. If this attribute is not supplied in the template, then it is configured with the default length. However, this attribute is not exposed in the interface.

      > **Note:**
      >
      > While creating an application, you can provide any value for this attribute. But while updating the application, the new length must be equal to or greater than the existing length.

    - `identityAttribute`: The name of the user attribute. Changes to this name forces the corresponding account attribute to be updated on the target system.

      > **Note:**
      >
      > The list of `schemaAttributes` does not include the user password. If you want to add this capability, then select the capability in the Settings tab, from the provisioning options.

    - `keyField`: Defines the reconciliation account matching rule.
    - `keyFieldCaseInsensitive`: Defines whether the reconcilication account matching rule is case insensitive or not.
    - `required`: Indicates whether or not the attribute is required.

* `fieldType`: Displays the type of schema attribute. This attribute is for legacy purposes and is not exposed to the user. If the type is not specified in the template, then this attribute is configured with the default type.
* `entitlement`: Marks the schema attribute as an entitlement. This property is inherited by child schema attributes.
* `reconcileable`: Indicates whether or not the attribute can be reconciled.
* `provisionable`: Indicates whether or not the attribute can be provisioned. This property is inherited from parent schema attributes.
* `encrypted`: Indicates whether or not the attribute is encrypted.
* `advanceFlags`: Advanced flags, such as Lookup, Date, and WriteBack.
  * `Lookup`: Use `Lookup` if the tilde character (~) must be removed from the attribute value before the value is sent to the target.
  * `Date`: Use `Date` if the `datatype` attribute matches the date on the target.
  * `WriteBack`: Use `WriteBack` if the attribute must be populated from the target after provisioning.
* `Account Discriminator`: Set the schema attribute as the discriminator for the accounts. You can select multiple provisionable fields as account discriminators. See Terminologies Used in Access Policies for more information about account discriminators.
* `listOfValues`: The name of the Lookup attribute that lists the value for the attribute.
* `defaultValue`: The value to be used during reconciliation when no value for the attribute is available on the target system.
* `provideOldValueOnUpdate`: Set to true if the old value of this attribute must propagate to the target during the update.
* `dependentAttribute`: The value of this attribute is supplied to the target application during the update of this attribute.

> **Note:**
>
> Both `provideOldValueOnUpdate` and `dependentAttribute` attributes are not supported at the same time. Either the old value is passed to the target or the dependent attribute is passed to the target during the attribute update.

* `form`: Specifies the child form (or forms) for the parent or root form. It corresponds to a multi-valued attribute.
  * `Use Bulk`: Select this option to configure the *Update Child Table Values Bulk* adapter for all child table-related operations.

    Some targets support only bulk updates of child values for all operations, including adding a new child, updating an existing child,

and removing a child. For these targets, the *Use Bulk* option must be selected for each child form.

- `catalogAttributes`: List of catalog attributes.
  - `Audit Objective`: A text field that provides any relevant value or description for Oracle Identity Analytics (OIA) certification.
  - `Risk Level`: Level of risk for the entity. The values supported are Low Risk, Medium Risk, and High Risk.
  - `User Defined Tags`: A value that describes the catalog item and that can be used for searching the entity.
  - `Approver User`: User who can approve the catalog item. This is used at the time of processing the request for the catalog item or during attestation.
  - `Approver Role`: Role that can approve the catalog item.
  - `Certifier User`: User who can certify the catalog item.
  - `Certifier Role`: Role that can certify the catalog item.
  - `Fulfillment User`: User who can complete or fulfill the request for the catalog item.
  - `Fulfillment Role`: Role that can complete or fulfill the request for the catalog item.
  - `Certifiable`: Specifies whether or not a catalog item is certifiable.
- `organizations`: The list of organizations to which the application is published.
- `parentApplicationName`: The name of the application on which the current application has a dependency. For example, if AD Exchange application has a dependency on the AD application, then `parentApplicationName` is set to the AD application.

21.2 Searching Applications

On the Applications page, you can search for applications based on the application name, display name, connector name, and base application.

To search for applications:

1. Login to Identity Self Service.
2. Click the **Manage** tab, and then click the **Applications** box to open the Applications page.
3. In the search list, select any one of the following:
   - Name: Search by application name.
   - Display Name: Search by display name.
   - Connector Name: Search by connector name.
   - Base Application: Search by base application name.
4. In the Search box, enter your search criterion.
5. Click the Search icon.

   The search results table displays the application name, display name, connector name, and application.

21.3 Creating Applications

You can use the Create Application option to create a target application or an authoritative application

Creating applications is described in the following sections:

- Creating a Target Application
- Creating an Authoritative Application

21.3.1 Creating a Target Application

Creating a Target Application includes steps such as, providing basic information, updating schema attributes, reviewing and updating settings for default attributes, and verifying the application information.

To navigate to the Create Application Wizard, login to Identity Self Service, go to the Manage tab and click the **Applications** box to open the Applications page. From the **Actions** menu, click **Create**, and then select **Target**. Alternatively, click **Create** on the toolbar, and select **Target** to open the Create Application wizard.

From this point onward, page-wise instructions are provided in the following sections:

- Providing Basic Information for Target Application
- Providing Schema Information for Target Application
- Providing Settings Information for Target Application
- Verifying the Target Application Details

21.3.1.1 Providing Basic Information for Target Application

On the Basic Information page, select the application you wish to onboard. To do so:

1. If you want to onboard a disconnected application using the default disconnected template, then select the **Disconnected** checkbox.

   > **Note:**
   >
   > To create a disconnected application for any custom template, do not select the **Disconnected** checkbox. Go to step 3.

2. If you want to create the application from a connector package, then select **Connector Package**. Select the connector from the **Select Bundle** list. By default, the Select Bundle drop-down shows the list of templates from the connector bundles present in the `OIM_HOME/server/ConnectorDefaultDirectory/` directory.

   To load a template from connector bundles at an alternate location, provide the path in the **Alternate Connector Directory** field, and click the **Reload connector list from alternate directory** icon next to the **Alternate Connector Directory**.

3. Alternatively, if you want to create the application by using a template, then select **Template**. Select **Select Template**.

4. Enter values in the Application Name, Display Name, and Description fields for the application. Application Name and Display Name are mandatory fields. The application name cannot include a space. Display name is the name that is used to represent the application in the request catalog.
5. Depending on the selected bundle or template, Basic Configuration and Advanced Settings for the connector may appear.

> **Note:**
>
> The parameters in the Basic Configuration and Advanced Settings section will vary based on the connector you have selected. For more information about these parameters, refer to the corresponding Connector documentation available on the Oracle Help Center website at the following URL:
>
> https://docs.oracle.com/en/middleware/idm/identity-governance-connectors/12.2.1.3/index.html

- The Advanced Settings section allows you to add new attributes. To add an attribute:
  a. Click **Add Attribute**. The New Attribute window is displayed.
  b. Enter the values for the Name, Value, Category, and Display Name fields, and click **OK**.

     The new attribute is displayed in the Custom section.
- If you have selected a flat file connector from the Select Bundle list, then in Advanced Settings, you have to provide the flat file location in the **flatFileLocation** field.

  Click **Parse Headers** to list the flat file schema properties from the CSV file mentioned in the flatFileLocation field.

  You can update the flat file attributes information and also add new fields. Click **Add Field** to add a new field.

  a. Enter the display name of the flat file attribute in the **Attribute** field.
  b. Select **MVA** if the attribute is a multivalued attribute.
  c. Click **Add Attribute** to create the complex multivalued attribute and specify the Sub Field names.
  d. Select the data type for the attribute.
  e. Select **Name** if the attribute has to be mapped to _Name_.
  f. Select **UID** if the attribute has to be mapped to _UID_.
  g. Select **Status** if the attribute has to be mapped to status.
  h. Select **Mandatory** if it is mandatory to get the value of this field from the target system. This option is selected when Name or UID is selected.

Update the required Basic Configuration parameters. Check if the connection between the target system and the server is fine by clicking the **Test Connection** button.

6. Click **Next** to navigate to the Schema page.

21.3.1.2 Providing Schema Information for Target Application

On the Schema page, you can manage the account and entitlement schema attributes. You can edit or delete existing attributes from the schema. After you perform all required actions in the Schema page, click **Next** to go to the Settings page.

> **Note:**
>
> If the connector is a Database Application Tables (DBAT) connector, then you can use the auto-discovery feature to fetch the target schema. If the Test Connection option on the Basic Information page is successful, then click **Discover** on the Schema page to fetch the target schema. If you are using this feature for editing an application, then the current configurations are overridden and you must do the attribute mapping on this page again.

Adding attributes and child form is described in the following sections:

- Adding Attributes
- Adding Child Forms

21.3.1.2.1 Adding Attributes

To add new attributes:

1. Click **Add Attribute** to add a new row to the table. Provide the following Application Attribute details:
   - **Identity Attribute**: Select an attribute from the list of user attributes. This attribute is used for user trigger process, that is, to propagate the user attribute changes to the user resource account. For example, if the *FirstName* of a user is modified, the changes should be pushed down to *fname* of the user account on the target, then select *FirstName* in the Identity Attribute list and select *fname* in the corresponding **Target Attribute** list.

     See Process Definition Form in *Developing and Customizing Applications for Oracle Identity Governance* for more information on user triggered process.
   - **Display Name**: Enter the display name for the attribute in Oracle Identity Governance.
   - **Target Attribute**: Enter the target attribute name. For connectors that support schema discovery, if the correct connectivity details are provided in the Basic Configuration section, then all the attributes on the target are listed in the Target Attribute drop-down. Select the target attribute name from the list.
   - **Data Type**: Select the data type from the list.
2. Provide the following Provisioning Property descriptions:
   - **Mandatory**: Select if the attribute is mandatory for target provisioning.
   - **Provision Field**: Select if the attribute must be present on the provisioning form.
3. Provide the following Reconciliation Properties descriptions:

- **Recon Field**: Select if the reconciliation process needs to pull this attribute value.
- **Key Field**: Select if the attribute is used for entity matching during reconciliation.
- **Case Insensitive**: Select if the account matching rule is case-insensitive.

4. To add additional properties to the attribute, click icon. The Advanced Settings window is displayed. Provide the following advanced settings:
   - **Account Discriminator**: Select to mark this attribute as one of the Account Discriminator fields. The collection of all such attributes in the form uniquely identifies the logical entity on which accounts are created. See Terminologies Used in Access Policies for more information about Account Discriminator.
   - **Lookup**: Select to indicate that the value of this attribute is set to a Lookup field. In the **List Of Values** field, enter the name of a lookup that contains a list of allowed values for this attribute. While provisioning, the value of this attribute can be set to one of the values from this list. If the lookup name provided does not exist, then a new lookup is created with an empty list of value. This is applicable only when the Data Type of the attribute is String.
   - **Date**: Select if the data type of the attribute is Date on the target and must be mapped to a String type attribute in Oracle Identity Governance.
   - **WriteBack**: Select to set the attribute as WriteBack for provisioning use case. When account provisioning is done, the value of this attribute in Oracle Identity Manager will get updated with the value in target. For example, __UID__ field is of type WriteBack. The value for UID is generated on the target and is written back into the Oracle Identity Manager account after provisioning.
   - **Provide old value on update**: Select if the update operation of the attribute on target requires the old value to be propagated to the target along with the new value. For example, to change the account password, you must provide the old password value along with the new password.
   - **Dependent Attribute**: Enter or select the name of the Oracle Identity Governance attribute on which the update operation of this attribute on target is dependent.
5. If you want to remove any attribute, then click the icon that is associated with the attribute.

21.3.1.2.2 Adding Child Forms

To add child forms:

1. Click **Add Child Form**. The Add Child Form window is displayed.
2. Enter the Form name, and click **OK**. The new child form is created.
3. Enter the attribute details. This is similar to the attribute details in Adding Attributes.
4. Provide the following application attribute details: **Display Name**, **Target Attribute**, and **Data Type**.
5. Provide the following Provisioning Property: **Mandatory**
6. Provide the following Reconciliation Properties: **Recon Field**, **Key Field**, and **Case Insensitive**.

7. To add additional properties to the attribute, click the icon. The Advanced Settings window is displayed. Provide the following advanced settings: **Lookup**, **Date**, **WriteBack**, and **Entitlement** (Select if this attribute must be marked as an entitlement).
8. For targets that support only bulk update of child values, select the **Use Bulk** option.
9. Click **Delete Form** to remove the child form.

21.3.1.3 Providing Settings Information for Target Application

On the Settings page, you can review and customize the default settings related to provisioning, reconciliation, catalog, and organization publications. After you perform all required actions on the Settings page, click **Next** to go to the Finish page.

Expand the **Preview Settings** tab and perform the following:

- Updating the Provisioning Configuration
- Updating the Reconciliation Configuration
- Updating the Organization Configuration
- Updating the Catalog Configuration

21.3.1.3.1 Updating the Provisioning Configuration

In the Provisioning tab, perform the following steps to update provisioning configurations:

1. In the Global Configuration section, review and if required, update the predefined provisioning configurations:
   - **Validation Script**: Click to review the validation script or to include a script. The Validation Script editor is displayed. If the script is present, you can edit the validation script or compile the script.
   - **Transformation Script**: Click to review the transformation script or to include a script. The Transformation Script editor is displayed. If the script is present, you can edit the transformation script or compile the script.
   - **Account Name**: Select the attribute to uniquely identify the account from the list. This list consists of all the schema attributes that can be set as account name.

   See About Customizing Groovy Scripts for information about how to write validation and transformation scripts.
2. In the Capabilities section, you can review and if required, update pre and post action scripts for the provisioning operations that are associated with this application. Provisioning operations include Create, Enable, Disable, Update (Bulk), Delete, and Change User Password.

> **Note:**
>
> If script execution is not supported for a particular provisioning operation in a connector, then the **Action Scrip** button is disabled.

To update pre and post action scripts for the provisioning operations:

a. Select the capabilities you want to review, edit, or add pre and post action script for, and click **Action Script** associated with that capability. The Action Script editor opens.

b. You can configure to run the script before or after provisioning operations. Use the pane where Trigger Time is set to **Before** to configure the script that must run before the provisioning operation and the pane where Trigger Time is set to **After** to configure the script that must run after the provisioning operation.

c. Enter the **Language** in which the script is written. For example, Shell.

> **Note:**
>
> For more information on the languages supported and whether the script execution for a particular action is supported by the connector type, refer to the corresponding connector documentation.

d. Enter value of the **Target** field to specify where the script has to be executed. For example, if the Target is set to Resource, then the script is executed on the computer where the target system is running. If the Target is set to Connector, then the script is executed on the Oracle Identity Governance server or the connector server (if configured).

e. Enter the script and click **Compile** to check if the script is valid.

f. Click **Save**.

> **Note:**
>
> You cannot add or manage scripts for the applications that are created through Connector Installer. However, the Java-based transformation and validation provided by the Design Console continue to work.

21.3.1.3.2 Updating the Reconciliation Configuration

On the Reconciliation tab, you can review or customize the required predefined matching rules, situations and responses, and reconciliation jobs.

Perform the following to update the reconciliation configuration:

- Updating Identity Correlation Rule
- Updating Situations And Responses
- Updating Validation and Transformation Scripts
- Updating Reconciliation Jobs

21.3.1.3.2.1 Updating Identity Correlation Rules

In the Identity Correlation Rule section, you can review and if required, edit or add simple or complex correlation rules. To add a rule:

1. If you want to add a simple rule, then select the **Simple Correlation Rule** option, and set the rule conditions. If the rule is based on more than one condition, then click **Add Rule**

Element to include a new rule element. Each rule element matches one target attribute to a user or identity attribute. These rule elements are separated by the AND or OR operators.

2. Otherwise, if you want to add a complex rule, then select the **Complex Correlation Rule** option, and enter the rule equation in JSON format. To validate the rule, click **Validate JSON Syntax**.

   Complex correlation rules are used when:

   - The rule has nested rules. The following is an example of a nested rule:

```
{
          "ruleOperator": "AND",
          "ruleElement": [
              {
                    "targetAttribute": "__NAME__",
                    "userAttribute": "User Login",
                    "elementOperator":
"Equals",
                    "transformName": "NONE"
              },
      ],
      "identityCorrelationRule": [
       {
           "ruleOperator": "OR",
           "ruleElement": [
              {
                     "targetAttribute": "Mid Name",
                     "userAttribute": "Middle Name",
                     "elementOperator": "Equals",
                     "transformName": "NONE"
              },
              {
                     "targetAttribute": "Last Name",
                     "userAttribute": "Last Name",
                     "elementOperator": "Equals",
                     "transformName": "NONE",
                     "caseSensitive": true
              }
           ]
        },
        {
           "ruleOperator": "OR",
           "ruleElement": [
               {

                     "targetAttribute": "First Name",
                     "userAttribute": "First Name",
                     "elementOperator": "Equals",
                     "transformName": "NONE",
               }
           ]
        }
   ]
 }
```

- When the target system must be configured to match part of the data value of a target attribute to the identity or user attribute value, some transformation can be specified in the rule. For example, to match a SubString of the target FirstName to the Oracle Identity Governance User FirstName. The supported transformations are:
  - Substring, for example start point or end point
  - Endstring, for example end point
  - Tokenize, for example Delimiters, Token Number, or Space Delimiter

  The following is an example for a rule that has transformName set to Tokenize and the rule maps target attribute _NAME_ to Oracle Identity Governance attribute User Login.

```
{
       "ruleOperator": "AND",
       "ruleElement": [
            {
                "targetAttribute": "__NAME__",
                "userAttribute": "User Login",
                "elementOperator": "Equals",
                "transformName": "Tokenize",
                "transformParams": [
                    {
                        "name": "Space Delimiter",
                        "value": "FALSE"
                    },
                    {
                        "name": "Token Number",
                        "value": "1"
                    },
                    {
                       "name": "Delimiters",
                       "value": "'@'"
                    }
               ]
            }
       ]
 }
```

21.3.1.3.2.2 Updating Situations and Responses

In the Situations And Responses section, you can review, and if required, update or add new situations and responses. To do so:

1. To add a new situation and response, click **Add**.
2. Select the situation from the **Situation** list, for example No matches found or One entity match found.
3. Select an appropriate response for the situation from the list of possible Response. See the following options:
   a. Create User
   b. Establish Link
   c. None

As part of AOB, OIM 12cPS4 the following responses are replaced by NONE.

- Assign To Administrator With Least Load
- Assign To Authorizer With Least Load
- Assign To Authorizer With Highest Priority

21.3.1.3.2.3 Updating Validation and Transformation Scripts

In the Validation & Transformation section, review and if required, update or add new validation and transformation logic based on groovy scripts. Click **Validation Script** or click **Transformation Script** to open the editor to include scripts.

> **Note:**
>
> - You cannot add or manage scripts for the applications that are created through the Connector Installer. However, the Java- based transformation and validation provided by the Design Console continue to work.
> - You can access any provisioning attribute value in the Groovy script with its display name as defined in the schema section. To do this, replace spaces in the display name with underscore characters (_).

21.3.1.3.2.4 Updating Reconciliation Jobs

On the Reconciliation Jobs section, you can review and if required, update or add new reconciliation jobs. To add a job:

1. Click **Add Job** to open the New Job window.
2. Enter values for the Job Name field and other required parameters, and click **OK**. You can add parameters to the existing jobs by clicking **Add Parameter**. This opens the Select Parameter Type window. Select the parameter type from the list, and click **OK**. Enter the required details, and click **OK**.

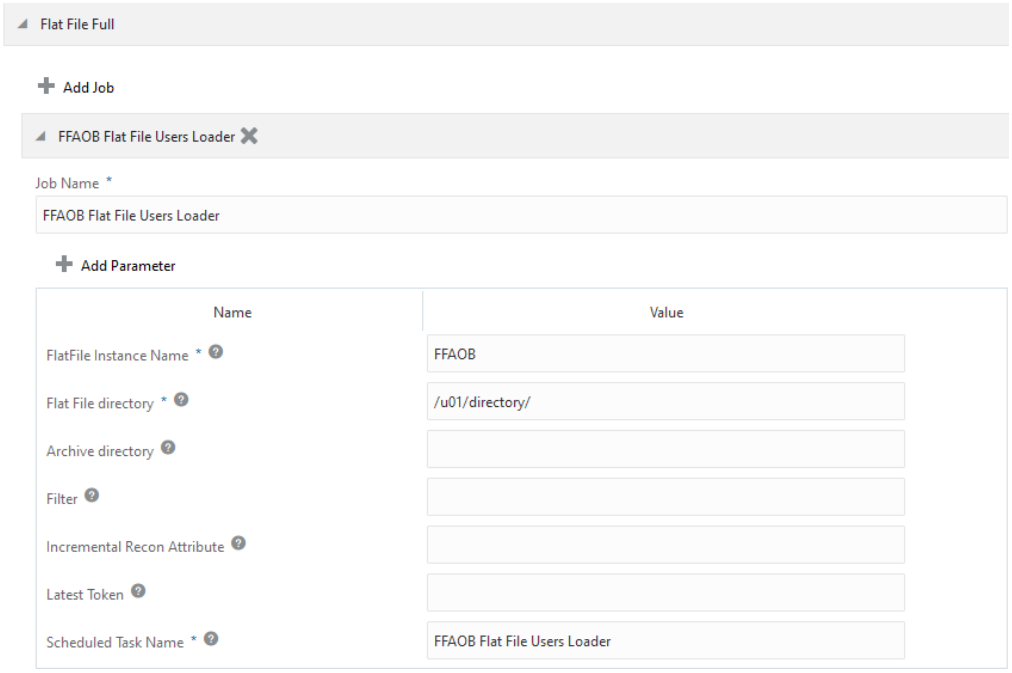
   The following reconciliation jobs can be set:

   - **Full**: This is used to reconcile all existing user records from the target system into Oracle Identity Governance.
   - **Incremental**: This is used to reconcile only records created or modified after the last reconciliation run.
   - **Delete**: This is used for reconciliation of deleted records.
   - **Entitlement**: This is used for lookup field synchronization.

   For flat file connectors, the following reconciliation jobs can be set:

   - **Flat File Full**: This is used to reconcile all existing user records from the target system into Oracle Identity Governance.

Figure 21-1 Flat File Full



- **Flat File Diff Sync**: This is used to perform diff-based reconciliation.
- **Flat File Delete Sync**: This is used to perform a delete reconciliation run.
- **Flat File Delete**: This is used for reconciliation of deleted records.
- **Flat File Entitlement**: This is used for lookup field synchronization.

When you create an authoritative Application for Flat File connector, under **Applications** ensure to fill up the **Reconciliation Jobs** section within Reconciliation located in **Settings** tab. Enter the values for the mandatory parameters (marked by the asterisk (*) symbol) for all the reconciliation jobs and then click **Apply**.

The mandatory parameters are:

- Job Name
- FlatFile Instance Name
- Flat File directory
- Scheduled Task Name
- Previous Flat File directory or Current Flat File directory.

A successful message is displayed stating that the flat file configuration is created successfully.

> **Note:**
>
> For information about the default set of reconciliation jobs for a given connector, refer to the corresponding Connector documentation available on the Oracle Help Center website at the following URL: https://docs.oracle.com/en/middleware/idm/identity-governance-connectors/12.2.1.3/index.html

21.3.1.3.3 Updating the Organization Configuration

On the Organization tab, select the organizations to which this application will be published. By default, the application is configured to be published to the Top organization. To add organizations:

1. Click **Add** to open the Add Organization window.
2. Search for the organization. Select the required organization from the search result table, and click **Select**.
3. Select **Hierarchy Aware** if you want to publish this application to the organization and its child organizations.

21.3.1.3.4 Updating the Catalog Configuration

In the Catalog tab, you can set various configuration-related Catalog metadata.

You can update the following attributes:

- **Category**: Enter the category for the application.
- **User Defined Tags**: Enter the user defined tag for this attribute.
- **Audit Objective**: Enter the objective of the audit.
- **Auditable**: Select **Yes** if the application is auditable or **No** if it is not.
- **Requestable**: Select **Yes** if the application is requestable or **No** if it is not. The following fields are enabled if Requestable is set to Yes:
  - **Fulfillment Role**: Click the Search icon to search and select the fulfillment role.
  - **Approver User**: Click the Search icon to search and select the user.
  - **Approver Role**: Click the Search icon to search and select approver role.
  - **Fulfillment User**: Click the Search icon to search and select the fulfillment user.
- **Certifiable**: Select **Yes** if the attribute is certifiable or **No** if it is not. The following fields are enabled if Certifiable is set to Yes:
  - **Certifier User**: Click the Search icon to search and select the certifier user.
  - **Certifier Role**: Click the Search icon to search and select the certifier role.
- **Risk Level**: Select the risk levels, which are High Risk, Medium Risk, or Low Risk.

21.3.1.4 Verifying the Target Application Details

On the Finish page, review the details used to create the application. If anything needs to be changed, click **Back** and make the required changes. If the details are fine, then click **Finish** to create an application.

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

If you choose to create a default request form, then 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, you must create a new one. To view the new default form, you must log in again to Oracle Identity Self Service. However, other users can view the default form as soon as it is created.

If you want to perform any sandbox- related changes after you create an application, then you must log out from the current Oracle Identity Self Service session and log in again.

21.3.2 Creating an Authoritative Application

Creating an Authoritative Application includes steps such as, providing basic information, updating schema attributes, reviewing and updating settings for default attributes, and verifying the application information.

To navigate to the Create Application Wizard, login to Identity Self Service, go to the Manage tab and click the **Applications** box to open the Applications page. From the **Actions** menu, click **Create**, and then select **Authoritative**. Alternatively, click **Create** on the toolbar, and select **Authoritative** to open the Create Application wizard.

From this point onward, page-wise instructions are provided in the following sections:

- Providing Basic Information for Authoritative Applications
- Providing Schema Information for Authoritative Application
- Providing Settings Information for Authoritative Application
- Verifying the Authoritative Application Details

21.3.2.1 Providing Basic Information for Authoritative Applications

On the Basic Information page, select the application you wish to onboard. To do so:

1. If you want to create the application from a connector package, then select **Connector Package**. Select the connector from the **Select Bundle** list. By default, the Select Bundle drop-down shows the list of templates from the connector bundles present in the `OIM_HOME/server/ConnectorDefaultDirectory` directory.

   To load a template from the connector bundles at an alternate location, provide the path in the **Alternate Connector Directory** field, and click the **Reload connector list from alternate directory** icon next to the **Alternate Connector Directory** field.
2. Alternatively, if you want to create the application by using a template, then select **Template**. Select **Select Template**.
3. Enter the **Application Name**, **Display Name**, and **Description** for the application. Application Name and Display Name are mandatory fields. Application Name cannot include a space. Display name is the name that is used to represent the application in the request catalog.

4. Depending on the selected bundle or template, Basic Configuration and Advanced Settings for the connector may appear.

> **Note:**
>
> The parameters in the Basic Configuration and Advanced Settings section varies based on the connector you select. For more information about these parameters, refer to the corresponding Connector documentation available on the Oracle Help Center website at the following URL:
> https://docs.oracle.com/en/middleware/idm/identity-governance-connectors/12.2.1.3/index.html

Update the required Basic Configuration parameters. Check if the connection between the target system and the server is fine by clicking **Test Connection**.

If you have selected a flat file connector from the Select Bundle list, then in Advanced Settings, provide the flat file location in the **flatFileLocation** field.

Click **Parse Headers** to list the flat file schema properties from the CSV file mentioned in flatFileLocation field.

You can update the flat file attributes information and also add new fields. Click **Add Field** to add a new field.

a. Enter the display name of the flat file attribute in the **Attribute** field.
b. Select **MVA** if the attribute is a multivalued attribute.
c. Click **Add Attribute** to create the complex multivalued attribute, and specify the Sub Field names.
d. Select the data type for the attribute.
e. Select **Name** if the attribute has to be mapped to _Name_.
f. Select **UID** if the attribute has to be mapped to _UID_.
g. Select **Status** if the attribute has to be mapped to status.
h. Select **Mandatory** if it is mandatory to get the value of this field from the target system. This option is selected when Name or UID is selected.

5. Click **Next** to open the Schema page.

21.3.2.2 Providing Schema Information for Authoritative Application

On the Schema page, you can manage the account and entitlement schema attributes. You can edit or delete existing attributes from the schema. After you perform all required actions in Schema page, click **Next** to go to the Settings page. To add new attributes:

> **Note:**
>
> If the connector is a DBAT connector, then you can use the auto-discovery feature. If the Test Connection option on the Basic Information page is successful, then click **Discover** in the Schema page to fetch the target schema. If you are using this feature for editing an application, then the current configurations are overridden and you must do the attribute mapping on this page again.

1. Click Add Attribute to add a new row to the table. Provide the following Application Attribute details:
   - **Identity Display Name**: Select the display name for the attribute.
   - **Target Attribute**: Enter the target attribute name or select the attribute name from the list.
   - **Data Type**: Select the data type from the list.
2. Provide the following Reconciliation Properties descriptions:
   - **Mandatory**: Select if the attribute is mandatory for target provisioning.
   - **Key Field**: Select if the attribute is used for entity matching during reconciliation.
3. To add additional properties to the attribute, click . The Advanced Settings window is displayed. Provide the default value and click **OK**.

21.3.2.3 Providing Settings Information for Authoritative Application

On the Settings page, you can review and customize the default settings related to reconciliation and organization publications. After you perform all required actions in the Settings page, click **Next** to go to the Finish page.

- Updating the Reconciliation Configuration
- Updating the Organization Configuration

21.3.2.3.1 Updating the Reconciliation Configuration

On the Reconciliation tab, you can review or customize the required predefined matching rules, situations and responses, and reconciliation jobs.

Perform the following to update the reconciliation configuration:

- Updating Identity Correlation Rule
- Updating Situations And Responses
- Updating Validation and Transformation Scripts
- Updating Reconciliation Jobs

21.3.2.3.1.1 Updating Identity Correlation Rules

In the Identity Correlation Rule section, you can review and if required, edit or add simple or complex correlation rules. To add a rule:

1. If you want to add a simple rule, then select the **Simple Correlation Rule** option, and set the rule conditions. If the rule is based on more than one condition, then click **Add Rule Element** to include a new rule element. Each rule element matches one target attribute

to a user or identity attribute. These rule elements are separated by the AND or OR operators.

2. Otherwise, if you want to add a complex rule, then select the **Complex Correlation Rule** option, and enter the rule equation in JSON format. To validate the rule, click **Validate JSON Syntax**.

   Complex correlation rules are used when:

   - The rule has nested rules. The following is an example of a nested rule:

```
{
          "ruleOperator": "AND",
          "ruleElement": [
              {
                    "targetAttribute": "__NAME__",
                    "userAttribute": "User Login",
                    "elementOperator":
"Equals",
                    "transformName": "NONE"
              },
      ],
      "identityCorrelationRule": [
       {
           "ruleOperator": "OR",
           "ruleElement": [
              {
                     "targetAttribute": "Mid Name",
                     "userAttribute": "Middle Name",
                     "elementOperator": "Equals",
                     "transformName": "NONE"
              },
              {
                     "targetAttribute": "Last Name",
                     "userAttribute": "Last Name",
                     "elementOperator": "Equals",
                     "transformName": "NONE",
                     "caseSensitive": true
              }
           ]
        },
        {
           "ruleOperator": "OR",
           "ruleElement": [
               {

                     "targetAttribute": "First Name",
                     "userAttribute": "First Name",
                     "elementOperator": "Equals",
                     "transformName": "NONE",
               }
           ]
        }
    ]
 }
```

- When the target system must be configured to match part of the data value of a target attribute to the identity or user attribute value, some transformation can be specified in the rule. For example, to match a SubString of the target FirstName to the Oracle Identity Governance User FirstName. The supported transformations are:
  - Substring, for example start point or end point
  - Endstring, for example end point
  - Tokenize, for example Delimiters, Token Number, or Space Delimiter

  The following is an example for a rule that has transformName set to Tokenize and the rule maps target attribute _NAME_ to Oracle Identity Governance attribute User Login.

```
{
       "ruleOperator": "AND",
       "ruleElement": [
            {
                "targetAttribute": "__NAME__",
                "userAttribute": "User Login",
                "elementOperator": "Equals",
                "transformName": "Tokenize",
                "transformParams": [
                    {
                        "name": "Space Delimiter",
                        "value": "FALSE"
                    },
                    {
                        "name": "Token Number",
                        "value": "1"
                    },
                    {
                       "name": "Delimiters",
                       "value": "'@'"
                    }
               ]
            }
       ]
 }
```

21.3.2.3.1.2 Updating Situations and Responses

In the Situations And Responses section, you can review, and if required, update or add new situations and responses. To do so:

1. To add a new situation and response, click **Add**.
2. Select the situation from the **Situation** list, for example No matches found or One entity match found.
3. Select an appropriate response for the situation from the list of possible Response. See the following options:
   a. Create User
   b. Establish Link
   c. None

As part of AOB, OIM 12cPS4 the following responses are replaced by NONE.

- Assign To Administrator With Least Load
- Assign To Authorizer With Least Load
- Assign To Authorizer With Highest Priority

21.3.2.3.1.3 Updating Validation and Transformation Scripts

In the Validation & Transformation section, review and if required, update or add new validation and transformation logic based on groovy scripts. Click **Validation Script** or click **Transformation Script** to open the editor to include scripts.

> **Note:**
>
> - You cannot add or manage scripts for the applications that are created through the Connector Installer. However, the Java- based transformation and validation provided by the Design Console continue to work.
> - You can access any provisioning attribute value in the Groovy script with its display name as defined in the schema section. To do this, replace spaces in the display name with underscore characters (_).

21.3.2.3.1.4 Updating Reconciliation Jobs

On the Reconciliation Jobs section, you can review and if required, update or add new reconciliation jobs. To add a job:

1. Click **Add Job** to open the New Job window.
2. Enter values for the Job Name fields and other required parameters, and click **OK**. You can add parameters to the existing jobs by clicking **Add Parameter**. This opens the Select Parameter Type window. Select the parameter type from the list, and click **OK**. Enter the required details, and click **OK**.

   The following reconciliation jobs can be set:

   - **Full**: This is used to reconcile all existing user records from the target system into Oracle Identity Governance.
   - **Incremental**: This is used to reconcile only records created or modified after the last reconciliation run.
   - **Delete**: This is used for reconciliation of deleted records.

   For flat file connectors, the following reconciliation jobs can be set:

   - **Flat File Full**: This is used to reconcile all existing user records from the target system into Oracle Identity Governance.
   - **Flat File Diff Sync**: This is used to perform diff-based reconciliation.
   - **Flat File Delete Sync**: This is used to perform a delete reconciliation run.
   - **Flat File Delete**: This is used for reconciliation of deleted records.
   - **Flat File Entitlement**: This is used for lookup field synchronization.

> **Note:**
>
> For information about the default set of reconciliation jobs for a given connector, refer to the corresponding Connector documentation available on the Oracle Help Center website at the following URL: https://docs.oracle.com/en/middleware/idm/identity-governance-connectors/12.2.1.3/index.html

21.3.2.3.2 Updating the Organization Configuration

On the Organization tab, select the organizations to which this application will be published. By default, the application is configured to be published to the Top organization. To add organizations:

1. Click **Add** to open the Add Organization window.
2. Search for the organization. Select the required organization from the search result table, and click **Select**.
3. Select **Hierarchy Aware** if you want to publish this application to the organization and its child organizations.

21.3.2.4 Verifying the Authoritative Application Details

On the Finish page, review the details used to create the application. If anything needs to be changed, click **Back** and make the required changes. If the details are fine, then click **Finish** to create an application.

21.4 Creating Templates

You can use the Create Application option to create a target template or an authoritative template and save it in the database for future use.

Creating templates is described in the following sections:

- Creating an Authoritative Template
- Creating a Target Template

21.4.1 Creating an Authoritative Template

To create an authoritative template:

1. Perform all the steps described in the Creating an Authoritative Application till you open the Finish page of the Create Authoritative Application wizard.
2. In the Finish page:
   a. Click **Save as Template** to create a template. The Save as Template window is displayed.
   b. Enter **Template Name** and **Description**, and click **OK**.

21.4.2 Creating a Target Template

To create a target template:

1. Perform all the steps described in the Creating a Target Application till you open the Finish page of the Create Target Application wizard.
2. In the Finish page:
   a. Click **Save as Template** to create a template. The Save as Template window is displayed.
   b. Enter **Template Name** and **Description**, and click **OK**.

21.5 Modifying Applications

You can edit applications that were created by using the Connector Installation Wizard or applications that were created by using the Create Application option.

The following sections describe how to edit applications:

- Editing an Application That Was Created by Using the Connector Installation Wizard
- Editing Applications
- Editing Templates

21.5.1 Editing an Application That Was Created by Using the Connector Installation Wizard

When an authoritative application is created by using the Connector Installation wizard, no default application instance is created. Therefore, the application cannot be edited on the Applications page of the Identity Self Service. To edit an authoritative application that was created by using the Connector Installation wizard, follow these steps:

1. Create an application instance for this application by using the `ApplicationInstanceService.addApplicationInstance(ApplicationInstance appInst)` API. See Java API Reference for Oracle Identity Governance for information about this API.
2. After the application instance is created, run the Application Template Generation Job scheduled task that creates a template for the application.

> **Note:**
>
> You cannot add or manage scripts for applications that are created through Connector Installer. However, the Java-based transformation and validation that the Design Console provides continues to work.

21.5.2 Editing Applications

To edit an application:

1. Log in to Oracle Identity Self Service.
2. Click the **Manage** tab. Click the **Applications** box to open the Applications page.
3. Select the application.
4. In the **Action** menu, select **Edit**. Alternatively, click **Edit** on the toolbar.

> **Note:**
>
> In the table that lists the applications, the application name is a hyperlink. Clicking this hyperlink opens a page that contains the details of the application. You can edit the details on this page.
>
> The Base Application field in the table indicates whether the application is a base application or instance. The configurations that are shared with the base application cannot be modified by using the edit option.

5. On the application detail page, change the values of the attributes on the Basic Information, Schema, or Settings tabs as required.

> **Note:**
>
> When you edit an application, if you are adding a new provisionable schema attribute or updating the display name of an existing provisionable schema attribute, then make sure to run the Form Upgrade Job scheduled job before you update an existing account for the application.

6. Click **Apply**.

21.5.3 Editing Templates

You can modify a template by using the **Create Application** option. On the Basic Information tab, use the Template option to select the template. Make the changes, and use the **Save as Template** option to save them to the template.

21.6 Cloning Applications

When you clone an application, all the configurations of the base application are copied into the cloned application.

To clone an application:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab. Click the **Applications** box to open the Applications page.
3. Select the application.

4. From the **Actions** menu, select **Clone**. Alternatively, click **Clone** on the toolbar to open the Clone Application page.
5. On the Clone Application page:
   a. Enter the Application Name, Display Name, and Description for the clone application. Application Name and Display Name are mandatory fields. Application Name cannot include space. Display name is the name that is used to represent the application in the request catalog.
   b. Change the values of the attributes in the Basic Information, Schema, and Settings pages as required.

> **Note:**
>
> For security reasons, the values of the encrypted basic attributes are not copied from the parent application. Make sure to enter these values.

6. Click **Apply**.

   If you are cloning a target application, then you are asked whether you want to create a default request form. Click **Yes** or **No**.

   If you choose to create a default request form, then the default form is created with the same name as the application. Default form cannot be modified later. Therefore, create a new form if you want to customize it. You have to re-login to the Identity Self Service to view the created default form. However, other users can view the default form once it is created.

   If you want to perform any sandbox-related changes after creating an application, then logout from the current Identity Self Service session and re-login.

21.7 Creating Instance Applications

You can create an application instance that has the same configurations as the base application.

> **Note:**
>
> The following configurations are shared between instance and base application:
>
> - Advance configurations
> - Schema configurations
> - Provisioning configuration
> - Reconciliation configuration

To create an instance application:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab. Click the **Applications** box to open the Applications page.

3. Select the application.
4. From the **Actions** menu, select **Create Instance**. Alternatively, click **Create Instance** on the toolbar to open the Create Instance Application page.
5. On the Basic Information tab:
   a. Enter the Application Name, Display Name, and Description for the instance application. Application Name and Display Name are mandatory fields. Application Name cannot include space. Display name is the name that is used to represent the application in the request catalog.

      The **Base Application** field displays the application for which you are creating an instance.

   b. Depending on the base application that is selected, Basic Configuration for the connector is displayed. Update the required parameters and check if the connection between the target system and the server is fine by clicking **Test Connection**.

> **Note:**
>
> For security reasons, the values of the encrypted basic attributes are not copied from the parent application. Make sure to enter these values.

6. Depending on the base application that is selected, the Settings tab might include information that can be updated. If the base application is a target application, then the Organization and Catalog tabs are displayed. If the base application is an authoritative application, then the Organization tab is displayed. Change the values of the attributes as required.
7. Click **Reconciliation Jobs** section, to copy, update, or add new reconciliation jobs.

   Copy Base Application Jobs: Select this option to copy the job for the Instance Application from the base application.

> **Note:**
>
> This selection is available after applying the bundle patch version 12.2.1.4.2110XX.

8. Click **Apply**.

21.8 Creating Applications in Bulk

You can load base applications and instance applications in bulk by using the Application Bulk Create scheduled task.

See Predefined Scheduled Tasks in *Administering Oracle Identity Governance* for information about this scheduled task.

The templates are processed in the following way:

- The templates that do not contain a base application name are processed first, and new applications are created synchronously.
- The templates that do contain a base application name are used to create instance applications. These templates are processed asynchronously.

See Application Template for more information about templates and how they are created.

> **Note:**
>
> When you create applications by using a job run of the Application Bulk Create scheduled task, use a sandbox to create the UI form from Identity System Administration.

21.9 Configuring Flat Files

For connected applications, you can configure flat files by loading data from CSV files.

Configuring flat files involve providing basic information, loading data from a CSV file for a connected system, auto-discovery of schema from the source, and updating the reconciliation jobs for predefined job modes.

To create a flat file configuration for a connector application, login to Identity Self Service, go to the Manage tab and click the **Applications** box to open the Applications page. Use the search option to search for the application or click the search icon to list all the connector applications. Select the application for which you want to create a flat file configuration.

From the **Actions** menu, select **Flat File**, **Configure**. Alternatively, click **Flat File** on the toolbar, and select **Configure** to open the Configure Application using Flat File page.

From this point onward, page-wise instructions are provided in the following sections:

- Providing Basic Information for Flat Files
- Providing Settings Information for Flat Files
- Adding a New Field to the Schema for a Disconnected Application

21.9.1 Providing Basic Information for Flat Files

On the Basic Information page, perform the following:

1. Enter the **Configuration Name**, **Display Name**, and **Description** for the application. Configuration Name and Display Name are mandatory fields. Configuration Name cannot include a space.
2. In the Basic Configuration and the Advanced Settings for the flat file, you can update the following:
   a. In the Basic Configuration section, you can select the Connector Server from the list. Click **Test Connection** to check if the connection between the target system and the server is fine.
   b. In the Advanced Setting section, enter the flat file location in the **flatFileLocation** field. Click **Parse Headers** to list the flat file schema fields from the CSV file mentioned in the flatFileLocation field.

      You can change the configurations of the following existing properties:

i. If the attribute is a multivalued attribute, select **MVA**. The Add Attribute option is enabled. Click **Add Attribute** to create complex multivalued attribute. Enter the subfield details, and then click **OK**.

ii. Change the data type of the field from the **Data Type** list.

iii. Select **Name** if the attribute is to be mapped to _Name_.

iv. Select **UID** if the attribute is to be mapped to _UID_.

v. Select **Status** if the attribute is to be mapped to _ENABLE_.

vi. If Name or UID option is selected, then Mandatory field is enabled. Select **Mandatory** to always get the value of this field from the target system.

> **Note:**
>
> For a disconnected application, you can add new fields to the schema, as described in Adding a New Field to the Schema for a Disconnected Application.

3. Click **Settings** tab to open the Settings page.

21.9.2 Providing Settings Information for Flat Files

In the settings tab, under the User panel, click **Preview Settings**. In the Reconciliation Jobs section, you can review and if required, update or add new reconciliation jobs.

The following reconciliation job modes are supported:

- **Flat File Full**: This is used to reconcile all existing user records from the target system into Oracle Identity Governance.
- **Flat File Diff Sync**: This is used to perform difference-based reconciliation.
- **Flat File Delete Sync**: This is used to perform a delete reconciliation run based on given Delete Attribute and Delete Attribute value.
- **Flat File Delete**: This is used for reconciliation of deleted records.
- **Flat File Entitlement**: This is used for lookup field synchronization.

To add a job:

1. Click **Add Job** to open the New Job window.
2. Enter values for the Job Name field and other required parameters, and click **OK**.

   You can add parameters to the existing jobs by clicking **Add Parameter**. This opens the Select Parameter Type window. Select the parameter type from the list, and click **OK**.

Click **Apply** to complete the flat file configuration.

21.9.3 Adding a New Field to the Schema for a Disconnected Application

For a disconnected application, you can add new fields to the schema. To do so:

1. In the Flat File Schema Properties section, click **Add Field**.

   A new row is added below the existing list.

2. In the Attributes field, enter the name of the flat file.
3. If the attribute is a multi-valued attribute, select **MVA**. The **Add Attribute** button is enabled. Click **Add Attribute** to create complex multivalued attribute. Enter the subfield details, and then click **OK**.
4. From the Data Type list, select the data type of the field.
5. Select **Name** if the attribute has to be mapped to _Name_.
6. Select **UID** if the attribute has to be mapped to _UID_.
7. Select **Status** if the attribute has to be mapped to status.
8. If Name or UID option is selected, then the Mandatory option is enabled. Select **Mandatory** to always get the value of this field from the target system.

21.10 Managing Flat File Configurations

You can edit the flat file configurations created for an application or you can manage jobs for the flat file configurations.

To manage a flat file configuration:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab. Click the **Applications** box to open the Applications page.
3. Use the Search option to search for the application or click the search icon to list all the connector applications. Select the application using which flat file configuration needs to be created.
4. From the **Actions** menu, select **Flat File**, and then select **Manage**. Alternatively, click **Flat File** on the toolbar, and select **Manage**. The Manage Configurations page for the selected application is displayed.
5. In the Manage Configurations page, use the search option to search and list the flat file configurations.

   You can edit the flat file configurations or mange jobs for the flat file configurations from this page.

   To edit flat file configurations:

   a. Select the flat file configurations you want to update, and click **Edit**. The Flat File Configuration details page is displayed.

      In the search result table, name is a hyperlink. Alternatively, click this hyperlink to open Flat File Configuration details page.

   b. In the Flat File Configuration details page, change the values of the attributes on the Basic Information or Settings tab as required. Click **Apply**.

   To manage jobs for the flat file configurations:

   a. Select the flat file configurations you want to manage jobs for, and click **Manage Jobs**. The Manage jobs page is displayed. For more information on Manage Jobs, see Managing Jobs.

21.11 Managing Jobs

You can add, update, and run the reconciliation jobs for applications from Identity Self Service.

To manage jobs for an application:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab. Click the **Applications** box to open the Applications page.
3. Use the Search option to search for the application or click the search icon to list all the connector applications. Select the application for which you want to manage jobs.
4. From the **Actions** menu, click **Manage Jobs**. Alternatively, click **Manage Jobs** on the toolbar. The Manage Jobs page for the selected application is displayed.
5. The Manage jobs page lists all the reconciliation job modes based on the type of application. You can add jobs, edit jobs, enable or disable jobs, run jobs, stop jobs, and delete jobs from this page.

   To add a job:

   a. Expand the job mode for which you want to add a new job.
   b. Click **Add Job** to open the New Job section.
   c. Enter values for the Job Name field and other required parameters, and click **Save**.
   d. You can add parameters to the job by clicking **Add Parameter**. This opens the Select Parameter Type window. Select the parameter type from the list, and click **OK**.

   > **Note:**
   >
   > To save and immediately run the job, click **Save and Run**.

   To update a job:

   a. Expand the job mode for which you want to edit the details.
   b. Select the Job you want to edit. Update details or add new parameters. Click **Apply**.

   To enable a job:

   a. Expand the job mode for which you want to edit the details.
   b. Select the job you want to enable. Click **Enable**.

   > **Note:**
   >
   > You can disable, run, stop, or delete jobs by clicking the respective options.

6. You can view the job history, such as job details, error details, milestones for the job, and job report in the Job History section.

21.12 Upgrading Connector Applications

You can use the **Upgrade** option to upgrade the applications and the application instances created through application onboarding, and view the upgrade process status.

This section contains the following topics:

- About Upgrading Applications
- Upgrading Applications
- Viewing the Upgrade Status

21.12.1 About Upgrading Applications

You can upgrade the applications that are created through application onboarding.

Before starting the upgrade, replace the old connector package with the new connector package in the Connector Default Directory, which is *MW_HOME*`/idm/server/ConnectorDefaultDirectory/`. During the upgrade process, the available upgrade files are listed based on the version comparison with the master template, which is the default template that is shipped with the connector package, and the template present in the Connector Default Directory.

The upgrade process lists the difference between the old template and the new template. This allows you to accept or reject the upgraded parameters or attributes in basic configurations, advanced configurations, schema attributes, child forms, reconciliation jobs, and capabilities.

> **Note:**
>
> - The difference in the `Pre-config.xml` file is not shown here.
> - The templates created by using the **Save as Template** option in the Create Application page cannot be upgraded by using this Upgrade option.

21.12.2 Upgrading Applications

You can upgrade the applications that are created through application onboarding by using the **Upgrade** option on the Applications page.

To upgrade an application:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab. Click the **Applications** box to open the Applications page.
3. From the **Actions** menu, select **Upgrade**, and then select **New**. Alternatively, click **Upgrade** on the toolbar, and select **New**. The Upgrade page is displayed.

4. In the **Bundle Select** tab, from the Select Bundle list, select the connectors available for upgrade. A message is displayed showing the current version of the connector and to which version it is being upgraded to.

   Click **Next**. The Target Application tab is displayed.

   > **Note:**
   >
   > This tab is disabled if there are no Target Applications available in the system for upgrade.

5. In the Target Application tab:

   a. In the Basic Information tab, the changed properties are listed under two sections, Added and Removed.

      i. The Added section lists properties that are new and not present in the older version. Select **Remove** corresponding to the property to exclude it.

      ii. The Remove section lists properties that are not present in the new version but are in the older version. Select **Keep** corresponding to the property to retain it.

   b. In the Schema tab, the changed schema attributes are listed under two sections, Added and Removed.

      i. The Added section lists the attributes that are new and not present in the older version. Select **Remove** corresponding to the attribute to exclude it.

      ii. The Remove section lists the attributes that are not present in the new version but are in the older version. Select **Keep** corresponding to the attribute to retain it.

   c. In the Settings tab, the changed Reconciliation and the Provisioning Jobs attributes are listed.

      Under the Reconciliation section, you can see Added Jobs and Removed Jobs.

      i. The Added Jobs section lists the jobs that are new and not present in the older version. Select **Remove** corresponding to the job to exclude it.

      ii. The Remove Jobs section lists the jobs that are not present in the new version but are in the older version. Select **Keep** corresponding to the job to retain it.

      Under the Provisioning section, you can see the list of capabilities in two sections, Added and Removed.

      i. The Added section lists the capabilities that are new and not present in the older version. Select **Remove** corresponding to the capability to exclude it.

      ii. The Remove section lists the capabilities that are not present in the new version but are in the older version. Select **Keep** corresponding to the capability to retain it.

   d. Click **Next**. The Authoritative Application tab is displayed.

      > **Note:**
      >
      > This tab is disabled if there are no Authoritative Applications available in the system for upgrade.

6. In the Authoritative Application tab:
   a. In the Basic Information tab, the changed properties are listed under two sections, Added and Removed.
      i. The Added section lists properties that are new and not present in the older version. Select **Remove** corresponding to the property to exclude it.
      ii. The Remove section lists properties that are not present in the new version but are in the older version. Select **Keep** corresponding to the property to retain it.
   b. In the Schema tab, the changed schema attributes are listed under two sections, Added and Removed.
      i. The Added section lists the attributes that are new and not present in the older version. Select **Remove** corresponding to the attribute to exclude it.
      ii. The Remove section lists the attributes that are not present in the new version but are in the older version. Select **Keep** corresponding to the attribute to retain it.
   c. In the Settings tab, the changed Reconciliation Job attributes are listed.

      Under the Reconciliation section, you can see Added Jobs and Removed Jobs.
      i. The Added Jobs section lists the jobs that are new and not present in the older version. Select **Remove** corresponding to the job to exclude it.
      ii. The Remove Jobs section lists the jobs that are not present in the new version but are in the older version. Select **Keep** corresponding to the job to retain it.
   d. Click **Next**. The Summary page is displayed.
7. In the Summary page, you can review the options selected in the previous tabs and the list of applications that will be part of the upgrade. Click **Upgrade**. The Status for Connector Upgrade page is displayed. You can check the upgrade status and take further action.

   The Upgrade process status can be one of the following:

   - **Initiated**: This indicates connector upgrade is initiated and applications are being merged and validated.
   - **Intermediate**: This indicates that there is an error in either merging or validating one of the applications, and upgrade is halted.

     If the status is **Intermediate**, then the upgrade process can be re-initiated. To do so, click **Retry**.
   - **Success**: This indicates that the connector upgrade is successful and all the applications have been successfully upgraded.
   - **Failure**: This indicates that the merge and validation of applications are complete with no error, but there is an error in upgrading the applications.

     If the status is **Failure**, then some of the applications have corrupted, and the database has to be restored.

   The Upgrade status for the application can be one of the following:

   - **Merge-Initiated**: This indicates that the merging of the application with the delta has initiated.

- **Merge-Failed**: This indicates that the merging of the application has failed and error can be seen against that application.
- **Merge-Completed**: This indicates that the merging of the application has completed.
- **Validation-Completed**: This indicates that the validation of the application has completed.
- **Validation-Failed**: This indicates that the validation of the application has failed and error can be seen against that application.
- **Upgraded**: This indicates that the application has upgraded successfully.
- **Upgrade-Failed**: This indicates that the upgrade of the application has failed, and an error can be seen against that application.

> **Note:**
>
> - If there are changes to the application schema during upgrade, then UI form must be manually changed. See Modifying Forms in *Administering Oracle Identity Governance* for information about modifying forms.
> - After upgrade, Transformation and Validation Scripts must be manually changed for each application by editing the application. See Modifying Applications.

21.12.3 Viewing the Upgrade Status

You can view the status of overall connector upgrade and the upgrade status of all the applications.

To view the upgrade status:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab. Click the **Applications** box to open the Applications page.
3. From the **Actions** menu, select **Upgrade**, **Status**. Alternatively, click **Upgrade** on the toolbar, and select **Status**. The Upgrade Status page is displayed.

   The upgrade process status can be one of the following:

   - **Initiated**: This indicates connector upgrade is initiated and applications are being merged and validated.
   - **Intermediate**: This indicates that there is an error in either merging or validating one of the applications, and upgrade is halted.
   - **Success**: This indicates that the connector upgrade is successful and all the applications have been successfully upgraded.
   - **Failure**: This indicates that the merge and validation of applications are complete with no error, but there is an error in upgrading the applications.

   The upgrade status for the application can be one of the following:

   - **Merge-Initiated**: This indicates that the merging of the application with the delta has initiated.

- **Merge-Failed**: This indicates that the merging of the application has failed, and error can be seen against that application.
- **Merge-Completed**: This indicates that the merging of the application has completed.
- **Validation-Completed**: This indicates that the validation of the application has completed.
- **Validation-Failed**: This indicates that the validation of the application has failed, and an error can be seen against that application.
- **Upgraded**: This indicates that the application is upgraded successfully.
- **Upgrade-Failed**: This indicates that the upgrade of the application has failed, and an error can be seen against that application.

21.13 Deleting Applications

You cannot delete applications from Oracle Identity Self Service.

In some situations, such as when the application creation process fails, the system may contain partially committed applications. To remove partially committed applications from the system, run the connector uninstall utility, as described in Uninstalling Connectors in *Administering Oracle Identity Governance*.

21.14 About Customizing Groovy Scripts

The Groovy Helper in Oracle Identity Governance provides options for transforming and validating data during reconciliation or provisioning operations.

The following options are available:

- **Provisioning Mechanism Information**: Call the `context.provisionMechanism` method to get the following provisioning mechanism information from the Groovy Helper.
  - REQUEST
  - ADMIN
  - POLICY

  These values are case-sensitive.
- **Operation Information**: Call the `context.operationType` method to get the following types of operations from the Groovy Helper.
  - create
  - modify

  These values are case-sensitive.
- **Common Data Container Information:** This includes the following:
  - **Requester Information**: Call the `context.requester` method to identify the requester information (for the user initiating the provisioning request) from the Groovy Helper. The user object from which any user attribute can be obtained is returned. For example, `context.requester.getAttribute("User Login")` returns the user ID of the requester.

- **Requester Manager Information**: Call the `context.requesterManager` method to identify the requester's manager information (for the manager of the user initiating the provisioning request) from the Groovy Helper. The user object from which any user attribute can be obtained is returned. For example, `context.requesterManager.getAttribute("User Login")` returns the user ID of the requester's manager.
- **Beneficiary Information**: Call the `context.beneficiary` method to identify the beneficiary information (for the user for whom the provisioning request is initiated) from the Groovy Helper. The user object from which any user attribute can be obtained is returned. For example, `context.beneficiary.getAttribute("User Login")` returns the user ID of the beneficiary.
- **Beneficiary Manager Information**: Call the `context.beneficiaryManager` method to identify the beneficiary's manager information (manager of the user for whom the provisioning request is initiated) from the Groovy Helper. The user object from which any user attribute can be obtained is returned. For example, `context.beneficiaryManager.getAttribute("User Login")` returns the user ID of the beneficiary's manager.
- **Beneficiary Password Information**: Call the `context.beneficiaryPassword` method to identify the beneficiary's password from the Groovy Helper.

> **Note:**
>
> For more information on how to access user attributes, see the User Management APIs.

You can use the Groovy Helper methods in the following way:

- **Derived attributes**: You can form attributes that are dependent on two or more other attributes. For example, the full name attribute is a combination of the first name, middle name, and last name attributes.

```
User_Id = context.beneficiary.getAttribute("User Login");
First_Name = context.beneficiary.getAttribute("First Name");
Last_Name = context.beneficiary.getAttribute("Last Name");
Middle_Name = context.beneficiary.getAttribute("Middle Name");
Full_Name = First_Name  + ". " + Middle_Name + ". " + Last_Name;
```

- **Default value attributes**: You can form attributes whose default value must be populated. For example, if the user does not provide organization details, then the default value is set to Server Technology.

```
If (Organization == null || Organization == "")
{
        Organization = "Server Technology";
}
```

- **Transformed attributes**: You can form attributes whose value is transformed. For example,`@example.com` is appended to the User ID attribute.

```
User_Id = User_Id.toString()+"@example.com";
```

In the following sample script, based on the type of provisioning, such as REQUEST, POLICY, or ADMIN, and on the type of operation being performed, such as creation or modification, data is transformed. All the variable values are initialized and available for provisioning and reconciliation operations, except `resultList`, which is defined and declared in the script itself.

```
def resultList;
if (binding.variables.containsKey("context"))
{
  if(context.operationType.equals("create"))
  {
     if(context.provisionMechanism.equals("POLICY"))
     {
         User_Id = context.beneficiary.getAttribute("User Login");
         First_Name = context.beneficiary.getAttribute("First Name");
         Last_Name = context.beneficiary.getAttribute("Last Name");
         Middle_Name = context.beneficiary.getAttribute("Middle Name");
         Full_Name = First_Name  + ". " + Middle_Name + ". " +
Last_Name;
         Common_Name = Full_Name;
         Password = context.beneficiaryPassword;
      }
      else if(context.provisionMechanism.equals("REQUEST") ||
context.provisionMechanism.equals("ADMIN"))
      {
         Full_Name = First_Name  + ". " + Middle_Name + ". " +
Last_Name;
         Common_Name = Full_Name;
      }
      if(Organization_Name != null && Organization_Name.indexOf("~") !
= -1)
      {
         resultList = Organization_Name.tokenize("~");
         User_Full_DN = "CN=" + Common_Name + "," + resultList[1];
      }
  }
  else if(context.operationType.equals("modify"))
  {
      Full_Name = First_Name  + ". " + Middle_Name + ". " + Last_Name;
      Common_Name = Full_Name;
      if(Organization_Name != null && Organization_Name.indexOf("~")  !
=  -1)
      {
         resultList = Organization_Name.tokenize("~");
         User_Full_DN = "CN=" + Common_Name + "," + resultList[1];
      }
   }
}
```

The following is a sample **Validation Groovy Script** that displays an error message if the User ID is not provided.

```
def effors = "";
if(User_Id == null || User_Id =="")
```

```
{
   errors = errors+" User Id cannot be null";
}
return errors;
```

In the validation script, you can specify a list of accounts that are excluded from reconciliation and provisioning operations. Accounts, whose user IDs are specified in the exclusion list, are not affected by reconciliation and provisioning operations.

The following is a sample **Validation Groovy Script for Resource Exclusion** script:

```
def errors = "";
def excludedUsers = ['user01','user02'];
def regexStr = /^[a-zA-Z0-9_]$/;
   if(!User_Id.matches(regexStr)) errors = errors+" Invalid UserId";
   if(excludedUsers.contains(User_Id)) errors = errors+" User Id lies in
excluded list";
return errors;
```

Action scripts are configured to run before or after create, update, enable, disable, change user password, and delete provisioning operations. For example, you can configure a script to run before a user is created.

The following action script creates a text file on the target system with a given name. You can configure this script for the Active Directory Connector.

```
echo create >> C:\%givenName%.txt
```

21.15 Troubleshooting Application Onboarding

Problems that you encounter while performing application onboarding may be related to authorization or may reflect issues with template creation.

This section describes the troubleshooting procedures to follow as you resolve issues during application onboarding.

Problem

A user who is a member of an organization other than the default organization cannot create an application.

Solution

Make sure that the user has the correct administration roles. Only users who have the `ApplicationInstanceAdministrator` administration role can perform the following actions from the Applications page of Identity Self Service:

- Create, modify, delete, or search applications within organizations that are defined under the scope of control of the administration roles.
- Create, modify, delete, or search applications within the parent organization.

For more information on administration roles, see Managing Administration Roles.

Problem

You can generate a template for applications that were created through Connector Installer before or after you upgraded the applications by running the Application Template Generation Job scheduled job.

Solution

`Lookup.AOB.Certified.Bundles` must have an entry for the bundle of the application for which the template is being generated. `Lookup.AOB.Certified.Bundles` must be updated with the following inputs:

- **Key**: The name of the bundle that contains advanced configuration information.
- **Value**: The connector display name. The *`CONNECTOR_NAME`*`-CI.xml` file must be present in the configuration folder.

  The connector display name and the connector version are set in the generated template. If it is not possible to identify the unique connector display name for a given bundle name, then the value in Lookup is set to `Unidentified`, and the connector display name and connector version are not set when the template is generated. It is the Application Administrator's responsibility to set the correct connector display name and version.

> **Note:**
>
> Only certified bundles are part of this lookup.

Problem

The resource history for a provisioned account shows additional process tasks for field updates.

Solution

This is expected. Process tasks are created for all fields in the schema attribute except for Writeback and SoD fields. These process tasks are for single updates of fields. In some cases, such as when a derived attribute and its value are updated as a part of a transformation script, the process task is triggered. In this case, the resource history for a provisioned account may show additional process tasks for derived attributes.

Problem

Logging of application onboarding with the package `oracle.iam.application` is enabled, but log for the entire flow is not available.

Solution

Application onboarding relies on the existing provisioning, reconciliation, scheduler, and catalog engines. To enable logging for application onboarding, logging of all the underlying engines should be enabled.

Problem

When you try to manage an application, which is created from the Applications page in Identity Self Service, from the Design Console, it shows unexpected behavior.

Solution

Applications that are created from the Applications page in Identity Self Service must not be managed from the Design Console.

22

Managing the Scheduler

This content applies only to OIG Bundle Patch 12.2.1.4.221004 and later releases.

Managing the scheduler involves understanding scheduled tasks and scheduled jobs, configuring the oim-config.xml file, starting and stopping the scheduler, understanding the predefined scheduled tasks, managing scheduled jobs, and diagnosing scheduled jobs.

This chapter describes about the Scheduler in Oracle Identity Manager. This chapter contains the following sections:

- About Scheduler
- Review Dashboard
- Configuring the oim-config.xml File
- Scheduled Tasks
- Managing Jobs
- Diagnosing Scheduled Jobs

22.1 About Scheduler

The scheduler enables you to schedule jobs that automatically run predefined scheduled tasks at the specified time.

This is illustrated by the following example:

To meet the security policies of an organization, employees may be required to change their product application password every 60 days. For this purpose, the system administrator has to ensure that an email is sent to all employees whose passwords for the respective product applications have expired. One approach would be to identify the set of users whose passwords have expired and send email to each employee manually. Alternatively, the system administrator can use a service, such as scheduler. In Oracle Identity Manager, there is a predefined scheduled task called Password Warning Task. The system administrator can use this scheduled task to create a scheduled job with the intended schedule.

> **See Also:**
>
> Predefined Scheduled Tasks for information about the Password Warning Task scheduled task

Scheduler also enables you to create your own scheduled tasks that can be run by a job at a set time.

A **scheduled task** configures the metadata for a job, which is to be run, and the parameters required for execution of that task. This metadata is predefined for the predefined tasks. A new task can be added by the user, which will have the new metadata or the existing tasks can be updated to add/update the parameters for other configuration details. A **job** can be scheduled to run at the specified interval. You can create multiple jobs scheduled to run at different time intervals. A **job run** is a specific execution of a job. Each job run includes information such as the start time, stop time, exceptions and status of the execution.

22.2 Configuring the oim-config.xml File

The oim-config.xml file consists of the Scheduler element, whose child elements define the scheduler settings.

After you install Oracle Identity Manager, you can configure the scheduler settings by editing the child elements of the Scheduler element in the oim-config.xml file located in the MDS. To access the oim-config.xml file by using Oracle Enterprise Manager:

1. Log in to Oracle Enterprise Manager.
2. Click **Application Deployments**.
3. Right-click **OIMAppMetadata(11.1.2.0.0)(*oim_server_name*)**, and select **System MBean Browser**.
4. In the System MBean Browser, navigate to **Application Defined MBeans**, **oracle.iam**, **Server: oim server**, **Application: oim**, **XMLConfig**, **Config**, **XMLConfig.SchedulerConfig**, **Scheduler**.

Table 22-1 lists the default elements that you can configure within the Scheduler element in the oim-config.xml file.

> **Note:**
>
> You can add new configurable child elements. For the information about new child elements, refer to the following URL:
>
> http://www.quartz-scheduler.org/

Table 22-1 Child Elements of the Scheduler Element

Element Within Scheduler Element	Description
DSJndiURL	This element is used for configuring transactional data source in the application server, which is used by Quartz to establish the connection. Default value: jdbc/operationsDB
nonTxnDSJndiURL	This element is used for configuring non-transactional data source in the application server, which is used by Quartz to establish the connection. Default value: jdbc/oimJMSStoreDS

Table 22-1 (Cont.) Child Elements of the Scheduler Element

Element Within Scheduler Element	Description
Clustered	Enter `true` if Oracle Identity Manager has been installed in a clustered environment. Otherwise, enter `false`. Default value: `true` **NOTE:** In a clustered environment, the clocks on all nodes of the cluster must be synchronized.
implementationClass	Enter the name of the Java class that implements scheduler. Default value: oracle.iam.scheduler.impl.quartz.QuartzSchedulerImpl
instanceID	Enter a unique string value in this element. This value represents a string that uniquely identifies an Oracle Identity Manager scheduler instance. **NOTE:** In a clustered environment, each node of the cluster must have a unique InstanceId. This can be achieved by entering a value of `AUTO` in the instanceId element.
startOnDeploy	Enter `false` if you do not want scheduler service to start automatically when Oracle Identity Manager is started. Otherwise, enter true. Default value: true
threadPoolSize	Enter an integer value in this element. This value represents the number of threads that must be used for running jobs. Default Value: 10

22.3 Review Dashboard

Use the **Review Dashboard** section to review the history of the Running Jobs, Executed Jobs, and Failed Jobs in the past 24 hours.

To review the jobs details and to check the details of job history in the past 24 hours, perform the following:

1. Log in to Oracle Identity Self Service.
2. Click **Manage** tab.
3. Click **System Configuration** box.
4. Select **Scheduler** from the drop-down.

   The **Manage Scheduler Jobs** page is displayed.
5. In the **Review last 24 hour Activity** dashboard, review the details in **Running Jobs**, **Executed Jobs** and **Failed Jobs** details.

   To check the details of a job history:

   a. Select one or more of the following to review the list of job history details:

      - Name: Enter the name of the job that you want to search.
      - Status: Search the job status that is applicable for the job search. The following are the types of status:

  - Running
  - Success
  - Interrupted
  - Failed
  - All
- Start Time With: Select the following time duration from the drop-down applicable for the search.
  - 1 Hour
  - 1 Day
  - 1 Week
  - 1 Month
  - 3 Months

b. Click **Search** and the **Job Details** page displays the following:

- Job Name
- Start Time
- End Time
- Duration
- Job Status

22.4 Scheduled Tasks

Oracle Identity Manager provides a list of predefined scheduled tasks. In addition, you can create your own custom scheduled tasks based on the requirement.

This section describes the scheduled tasks. This is discussed in the following topics:

- About Scheduled Tasks
- Predefined Scheduled Tasks
- Creating Custom Scheduled Tasks

22.4.1 About Scheduled Tasks

In Oracle Identity Manager, metadata is predefined for the default scheduled tasks. New tasks can be added by the user with new metadata, or the existing tasks can be updated to add or update the parameters or other configuration details.

For example, you can configure a reconciliation run using a scheduled task that checks for new information on target systems periodically and replicates the same in Oracle Identity Manager. Each scheduled task contains the following metadata information:

- Name of the scheduled task
- Name of the Java class that runs the scheduled task
- Description
- Retry

- (Optional) Parameters that the scheduled task accepts. Each parameter contains the following additional information:
  - Name
  - Data Type
  - Required/ Optional
  - Help Text
  - Encryption

22.4.2 Predefined Scheduled Tasks

Oracle Identity Manager provides a set of predefined scheduled tasks that you can use while creating or working with jobs.

Table 22-2 lists the predefined scheduled tasks.

Table 22-2 Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Application Instance Post Delete Processing Job	This scheduled task is used to revoke, delete, or decommision applicaion instances that have been soft-deleted. It can be run in the following modes: • **Revoke:** Deletes the provisioned accounts from the target system after the application instances has been deleted • **Delete:** Hard-deletes the accounts from all provisioning tasks and targets, and subsequently from Oracle Identity Manager • **Decommission:** Changes the account status to Revoke without keeping the accounts in Oracle Identity Manager in provisioned state	None	Yes
Application Bulk Create	This scheduled task is used to seed Application and Instance Application in bulk. There is no default job for this scheduled task however, you can create job using this task.You need to provide directory path of list of Application and Instance Application Template. Template will be processed as per below convention: • All template that does not contain Base Application Name are processed on priority and such templates are eligible for new Application. Such Applications will be created in sequence from job. • All template that contains Base Application Name are eligible for Instance Application. All such template are processed asynchronously.	Template Directory and Archive Directory	Yes

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Application Template Generation Job	This scheduled task is used to generate the template for applications that are created through connector installer or if there is a upgrade. The generated templates are stored in internal database table, which is used to manage the application from Application Tab in Identity Self Service. **Note:** For authoritative applications, create an application instance using API and then use this job to generate the template.	**Application Names:** A list of comma separated application instance names for which templates have to be generated. **Generate in Bulk:** If set to Yes, template is generated for all application instances which are not Deleted. If Generate in Bulk is set to Yes, then **Application Names** should not be set. Default value is No.	Yes
Attestation Grace Period Expiry Checker	This scheduled task delegates the attestation process after the grace period expires.	None	Yes
Automated Retry of Failed Async Task	This scheduled task retries Async Tasks (JMS Messages) that have failed. If the execution of the task succeeds, it is removed from the list of failed tasks. If it fails, the retry count is incremented. The maximum number of times a Failed Task is retried is determined by the 'maxRetries' defined for that task in async-messaging.xml.	None	Yes
Automatically Unlock User	This scheduled task automatically unlocks a user after the specified number of days. This job supports job frequency in days, minutes, and hours. As password policy in supports lockout duration in minutes, It is recommended to keep the frequency of this scheduled job in minutes.	None	Yes

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Bulk Load Archival Job	This scheduled task cleans up the processed entries in the Oracle Identity Manager Database staging tables used during bulk load post processing.	• Archival Date: This attribute specifies the date up to which the records will be purged. It must have a value. The format is **ddMMyyyy** or **MMM dd, yyyy**. • Batch Size: Database records are cleaned up in batches. This attribute specifies the size of the batch and must have a value. The default is 1000.	No
Bulk Load Post Process	This scheduled task starts post processing jobs for the Bulk Load Utility.	• Batch Size for Processing Records: User records are processed in batches. This attribute specifies the size of the batch and must have a value. The default is 500. • Generate Password: This attribute specifies whether a password will be automatically generated when users are created with the Bulk Load Utility. It must have a value of Yes or No; the default is Yes. • Ldap Sync: This attribute specifies whether users created in Oracle Identity Manager using the Bulk Load Utility will also be created in the LDAP repository in an LDAP enabled environment. This attribute must have a value of Yes or No; the default is No. • Notification: This attribute specifies whether users created using the Bulk Load Utility will be notified with an email. It must have a value of Yes or No; the default is Yes. • Process User Ids: This attribute specifies the range of user keys (in the Oracle Identity Manager Database) that need to be processed. The keys are associated with the users created using the Bulk Load Utility. It defines a range from start (From:) to finish (To:).	No

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Catalog Synchronization Job	The scheduled task is used to harvest roles, application instances, and entitlements into the catalog. It is also used to load catalog metadata.	**Mode:** The Catalog Synchronization Job scheduled job can be run in the following modes: • **Incremental:** Updates catalog entries based on the Update Date parameter. Only data changed on or after this date is refreshed in the catalog. • **Full:** Refreshes the entire catalog from the source entities. All the data in the catalog is replaced. • **Metadata:** Updates or adds metadata columns of catalog items based on the supplied CSV file. The CSV file should contain details of the existing catalog items. It should contain Catalog_ID or ENTITY_TYPE, ENTITY_KEY of the existing catalog item. • **Technical Glossary:** Loads data in the catalog that represent hierarchical attributes of entitlements based on external source (XML). • **Recalculate Tags:** Refreshes CATALOG TAGS column using CATALOG.USER_DEFINED_TAGS and other searchable CATALOG attributes. The same values can be used in keyword search.	Yes
Certification Event Trigger Job	This scheduled task is responsible for running event listeners against the set of user modification events that have occurred in the system. All event listeners will be executed by default if none are listed in the Event Listener Name List parameter. See Configuring Event Listeners and Certification Event Trigger Jobs in *Performing Self Service Tasks with Oracle Identity Governance* for more information.	Event Listener Name List: This is a comma-separated list of event listeners to be evaluated. If no value if specified for this attribute, then all event listeners will be evaluated.	No

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Certification Maintenance Job	This job populates the required data for pre-upgrade certifications. If you are using an upgraded deployment of Oracle Identity Manager, then run this job to access certifications from Certification Dashboard UI. See Accessing Pre-Upgrade Certifications in the Dashboard in *Performing Self Service Tasks with Oracle Identity Governance* for information about populating pre-upgrade certifications in the Dashboard by running this scheduled job.	• Batch Size: Number of certifications to process in a thread. • Number of Concurrent Threads: Number of processing threads used by Certification Maintenance Job for parallel processing. This attribute should be updated depending on the OIM host capabilities and performance requirements.	Yes
Certification Comments Mining Job	This schedule job computes and store the latest comments for each entity line item from last completed certification if available or from the request justification.	Mine Comments OOTB Value: No **Note:** To ensure the comments are populated, the value of this attribute must be changed to **Yes**.	No
DataCollection Scheduled Task	This scheduled task is used to populate data from Oracle Identity Manager operational tables to the staging tables in an offline manner. The scheduled task is set to run manually, and is triggered when Oracle Identity Analytics (OIA) invokes the DataCollectionOperationsIntf->startDataCollection API.	None	Yes

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Delayed Delete User	This scheduled task automatically deletes the user whose delete date is before the start of today. The XL.UserDeleteDelayPeriod system property indicates the number of days after which the user is to be deleted. When the administrator deletes a user, the user is marked in the Disabled state, and the user's 'Automatically Delete On' date is set for the future date after the number of days indicated in the XL.UserDeleteDelayPeriod system property. This scheduled task finds all such users for whom the 'Automatically Delete On' date is less than the start of today. All those users are marked as Deleted. For example, Jane Doe is a user with '2014-03-24 01:55:00' as the 'Automatically Delete On' date, and John Doe is a user with '2014-03-25 18:55:00' as the 'Automatically Delete On' date. When the scheduler is run on '2014-03-25', only Jane Doe is deleted. John Doe will be deleted when the scheduler runs on '2014-03-26'. **Note:** See Default System Properties in Oracle Identity Governance for information about the XL.UserDeleteDelayPeriod system property. **Note:** Oracle recommendation is to run this scheduled task once per day.	None	No

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Deleted User Account Clean Up Job	This scheduled task removes sensitive data of deleted users, such as user attributes and account data. **Note:** Transitional data, such as reconciliation events, might have parts of relevant user data, which is taken care of by regular data purge utilities. If archival tables are used, such data persists in archival tables. Running the Deleted User Account Clean Up Job does not clean up certification campaigns for the users under consideration. As base records for users are completely cleaned up meanwhile, a detailed review of such users from certification campaign may not work.	**User Login(s)**: This is a comma-separated list of deleted user login(s). If this list includes any active user, then an error message is displayed. Check the *diag_log* and *diag_log_dtls* tables for details. For diagnostic logging and debugging information during or after the scheduled task execution, see 19c Using PL/SQL Unified Diagnostic Logging and Debugging Framework Framework.	No

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Disable Hierarchical Entitlement Task	This scheduled task cleans up the hierarchy from the TARGET_HIERARCHICAL_DATA table and deletes the assigned indirect entitlements.	• Application Name: Use this field to specify the name of the application. • Nested Object Name: Use this field to identify the name of the nested group object. Example: Use **groups** for AD target. • Number of Threads: Use this attribute to specify the total number of threads.	Yes
Disable/Delete User After End Date	An end date is defined when a user account is created. This scheduled task disables user accounts for which the end date had passed the current date at the time when the task is run. **Note:** Oracle recommendation is to run this scheduled task every 30 minutes or 1 hour.	None	Yes
Enable User After Start Date	A start date is set when a user account is created. This scheduled task enables user accounts for which the start date has passed, and the user status is Disabled Until Start Date. These users are enabled thorough this scheduled task, thereby making the users ACTIVE.	None	Yes
Entitlement Assignments	This scheduled task populates Entitlement Assignment schema from child process form table whose field, Entitlement is marked as true.	RECORDS_TO_PROCESS_IN_BATCH: Number of records to process in a batch.	No
Entitlement List	This scheduled task populates Entitlement schema from the lookup table whose child process form field `Entitlement` is marked as true.	Auto Publish: When the value of this field is true, the entitlement is automatically published to the organization that is already part of the application instance. The default value of this field is true. If the value is false, then the entitlement is not published to the organization that is already part of the application instance.	No

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Entitlement Post Delete Processing Job	This scheduled task is used for post-processing of entitlement soft deletion in the provisioning component. It is used to revoke or delete entitlements that have been soft-deleted. It can be run in the following modes: • **Revoke:** Revokes the entitlement-grant for all the accounts in Oracle Identity Manager, which have that specific entitlement granted. • **Delete:** Hard-deletes the entitlements from the UD_CHILD table. Irrespective of the mode, the entitlement grant entry is removed from the ENT_ASSIGN table.	None	Yes
Evaluate User Policies	This scheduled task evaluates the access policies.	Number of Threads: Use this attribute to specify the total number of threads that will process re-evaluation. The default value is 20. Batch Size: Use this attribute to fetch number of records from the database to be processed in one iteration. The default value is 500. Time Limit in mins: Use this attribute to specify time in minutes, after which the schedule task will stop. By default, this attribute is not specified and disabled. You must enable and configure the time.	Yes
Form Upgrade Job	This scheduled task updates the form version to the latest active version and the form data to the value specified during the field's creation for all accounts. **Note:** If this scheduled task is not run, then the form version and data will be incorrect in the audit snapshot and the reporting tables.	• Application Instance Name: Name of the application instance. The default value is "ALL." • Batch Size: Use this attribute to fetch number of records from the database to be processed in one iteration. The default value is 500.	Yes
Get SOD Check Results Approval	This scheduled task gets back the result of SoD Evaluation from the SoD Server, for example, OAACG, SAP, and GRC for all requests waiting for SoD Check results. It reflects the SoDCheckResult and violation in appropriate dataset attributes. It will pick up all requests that are in 'SoD check result pending' state and mark them as 'SoD check completed'.	None	No

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Get SOD Check Results Provisioning	This scheduled task gets back the result of SoD Evaluation from the SoD Server, for example, OAACG, SAP, and GRC for all pending SoDCheck provisioning tasks. It reflects the SoDCheckResult and violation in appropriate process form attributes.	None	No
Hierarchy Search Recon Task	This scheduled task populates the hierarchy details from the target system to the new OIG database table **TARGET_HIERARCHICAL_DATA**.	• Application Name: Use this field to specify the name of the application. • Object Type: Use this field to identify the type of the object. **Example:** Object Type = Group • Parent Attribute Name: Use this field to specify the name of the parent groups. **Example:** Parent Attribute Name = memberOf for AD target • Attribute Name: Use this field to specify the attribute name. **Example:** Attribute Name = __NAME__ • Form Name: Use this field to specify the name of the form. **Example:** Form Name = groups	Yes

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Hierarchical Entitlement Processing Task	This scheduled task calculates and assigns/ revokes the indirect entitlements between the users for a given application and the nested object name. **Note:** The Hierarchical Entitlement Processing task is performance intensive operation. You must enable the task only if required. To return to the earlier behavior, you must run the Disable Hierarchical Entitlement job.	• Application Name: Use this field to specify the name of the application. • Nested Object Name: Use this field to specify the name of the nested group object name. The value for Nested Object Name is **groups** for AD target. • Number of Threads: Use this field to specify the number of threads to be used while calculating and assigning or revoking the indirect entitlements.	Yes
Identity Audit Scan Cleanup	This scheduled task processes existing detective scan runs and purges old data from the tables used to store history of users and policies connected with the scan runs. Records are purged from the IDA_SCAN_RUN_POLICIES and IDA_SCAN_RUN_USERS tables. To retain the history, enable the job and schedule it to run periodically based on the activity in the system.	Number of Threads: Use this field to specify the number of threads to be used while running a scan cleanup job. Default value is 4. Scan Run Batch Size: Use this field to specify the number of scan run entities per batch for a single processing thread. Default value is 20.	No
Issue Audit Messages Task	This scheduled task fetches audit message details from the aud_jms table and sends a single JMS message for a particular identifier and auditor entry in the aud_jms table. An MDB processes the corresponding audit message.	Max Records: Use this attribute to specify the maximum number of audit messages to be processed for a specified scheduled task run. The default value of this attribute is 400.	Yes

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Job History Archival	This scheduled task is designed to archive/ purge entries for Job History.	Archival Date: Use this attribute to specify date till which the records need to be archived/ purged. Supported archival date format is ddMMyyyy. **Note:** Archival Date parameter is auto incremented by one day on each job execution. So job should be scheduled with daily frequency to work as exp	No

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
		ecte d. Batch Size: Use this attribute to specify the size of a batch in which the records must be processed. Operation Type: Use this attribute to specify the operation type. This attribute can have two possible values, Archive and Purge. The default value is Archive.	
Non Scheduled Batch Recon	This scheduled task tries to process all the events created by non scheduled task based connectors such as PeopleSoft. Such connector created events are in either Event Received State or Data Received State, they only get processed if the batch size specified by the set of events is reached or via this scheduled task. This task executes as per settings to pick up all the unprocessed non scheduled task based events and submits them to the reconciliation engine for processing.	None	No

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
OIM Certification Purge Job	This scheduled task is used to purge data from the certification tables. It provides for some critical parameters to be specified or configured (although default values are available for these), such as retention period, run duration, and purge criteria, for online and continuous purge of data in the background. **Note:** By default, the OIM Certification Purge Job is seeded with default values for input parameters, such as purge interval and purge retention period. You must revisit the input parameters to change their default values as required.	For information about the user-configurable attributes, see Configuring Real-Time Certification Archival and Purge Job.	No
OIM Data Purge Job	This scheduled task is used as a single unified interface for archive/purge of data for the Requests, Reconciliation,Provisioning Tasks, and Orchestration entities. It provides for some critical parameters to be specified/configured (although default values are available for these), such as retention period, run duration, and purge criteria, for online and continuous purge of data in the background. **Note:** By default, the OIM Data Purge Job scheduled job is seeded in the enabled state with a retention period of 90 days. You must revisit the job parameters to disable or to change the purge interval as required.	For information about the user-configurable attributes, see Configuring Real-Time Purge and Archival.	Yes

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
OIM Entitlement Assignment History Purge Job	The scheduled task is used for archive/ purge of data for the Entitlement Assignment History table.	For information about using Entitlement Assignment History Purge, see Using the Real-Time Entitlement Assignment History Purge in Oracle Identity Governance.	No
Password Expiration Task	This scheduled task sends e-mail to users whose password expiration date had passed at the time when the task was run and then updates the USR_PWD_EXPIRED flag on the user profile.	Email Definition Name: Name of the email definition created in the Design Console for sending password expired notification to the user. The default value is "Password Expired".	Yes
Password Warning Task	This scheduled task sends e-mail to users whose password warning date had passed at the time when the task was run and then updates the USR_PWD_WARNED flag on the user profile.	Email Definition Name: Name of the email definition created in the Design Console for sending password expiration warning notification to the user. The default value is "Password Expiration Warning".	No
Process Pending Role Grants	This scheduled task is responsible for processing of future role grants. It grants the role for which start date has reached and revokes the role if role grant end date has reached. This task is scheduled to run daily.	None	Yes
Reconciliation Retry Scheduled Task	This scheduled task processes the failed reconciliation event for the users whose status is set as Failed.	None	Yes
Refresh Materialized View	The materialized view is used to generate reports related to reconciliation. This view needs to be updated periodically (at a specified interval, for instance, once a day).	None	No
Refresh Organization Memberships	This evaluates the organization memberships and assigns users to organizations based on rules. This job evaluates all the organizations whose membership rules have changed since the last job run and their immediate evaluation have not been opted by the administrator.	None	Yes
Refresh Role Memberships	This evaluates the role memberships and assigns users to roles based on rules. This job evaluates all the roles whose membership rules have changed since the last job run and their immediate evaluation have not been opted by the administrator.	None	Yes

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Remove Audit Log Entries	This scheduled task is used to permanently remove audit log events which are older than a specified number of days. On job completion, the scheduled task will add a single audit log event in AUDIT_EVENT table recording the number of records removed from the database, the job return code, and an error message if the job fails. For more information on how to control audit data growth in Lightweight audit framework, see About Audit Data Growth Control Measures in Lightweight Audit Framework.	• Batch Size: The number of records to be removed as a batch. Default value is 500. • Maximum Job Duration (in Mins): Default value is 30 minutes. • Remove Audit Log Events older Than (in days): Audit events whose date is older than this value will be permanently deleted from the audit event table. Default value is 180 days.	Yes
Remove Open Tasks	This scheduled task removes information about open tasks from the table that serves as the source for the list displayed in Oracle Identity System Administration.	Day Limit Number of days for which information about an open task should be retained in the table before the information is deleted By default, this attribute is not specified and disabled. You must enable and configure the time.	No
Request Execution Scheduled Task	This is a periodic scheduled task searches for requests with status "Request Awaiting Completion" and moves requests forward to the next stage "Operation Initiated" if the effective date set during the request submission is prior or equal to the current date.	Job Periodic Settings: Use this attribute to specify the time interval for the scheduled task to be run. The default value is 6 hours.	Yes
Resubmit Uninitiated Approval SODChecks	This scheduled task tries to initiate SoD Check for pending requests, which have SoDCheckStatus as "SoD check not initiated" or "SoD check completed with error". The pending requests are the ones for which SoD initiation failed in first try and are pending for some level of approval.	None	No
Resubmit Uninitiated Provisioning SODChecks	This scheduled task tries to initiate SoD Check by submitting a JMS message for all pending SoDCheck provisioning tasks. The SoD Check initiation may have failed because of SoD server being down at the time of entitlement add/update via direct provisioning.	None	No

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Retry Failed Orchestrations	This scheduled task retries all failed orchestrations based on the attribute values provided. If there is no parameter value defined, no orchestration will be retried.	• Orchestration ID: This attribute takes a comma separated list of Orchestration Ids to be retried. • Entity Type: Orchestrations submitted for the given Entity will be retried. • Operation: Orchestrations submitted for given Operation will be retried. • Stage: Orchestrations on the given stage will be retried. • From Date: Orchestrations submitted after the given date will be retried. The format is **ddMMyyyy** or **MMM dd, yyyy**. • To Date: Orchestrations submitted before given date will be retried. The format is **ddMMyyyy** or **MMM dd, yyyy**.	No
Retry Reconciliation Batch Job	This scheduled task is used to re-process batches with the 'Ready for Processing' status.	Batch ID: This is the comma-separated ID of the batches to be retried.	No
Risk Aggregation Job	This scheduled task is used for calculating the risk summary value for users, roles, and accounts based on their item-risk and risk-factor levels as defined in the system **Note:** See About Risk Aggregation and Risk Summaries in the *Performing Self Service Tasks with Oracle Identity Governance* for more information.	• Number of Concurrent Threads: Use this attribute to specify the number of threads that process risk aggregation. • User Batch Size: Use this attribute to specify the number of users that must be processed in each thread.	No
Run Future Dated Reconciliation Events	This scheduled task processes the current dated reconciliation event for the users whose status is set as Deferred.	None	No
Set User Deprovisioned Date	A deprovisioning date is defined when a user account is created. For users whose deprovisioning date had passed at the time when this scheduled task was run, the task sets the deprovisioned date as the current date.	None	Yes

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Set User Provisioned Date	This scheduled task sets the provisioned date to the current date for users for whom all of the following conditions are true: • The provisioning date is in the past. • The deprovisioned date has not been set. • The deprovisioning date has not been reached or is NULL.	None	Yes
Seed Home Organization	This scheduled task evaluates and updates organization data for existing users based on configured Home Organization Policy. For more information, see Managing the Home Organization Policy. Ensure that Home Organization Policy rule for organization evaluation is configured correctly, and the organization should already exist in Oracle Identity Manager. This job can be run for environments that are based on LDAP synchronization. For information about LDAP synchronization, see Enabling LDAP Synchronization in Oracle Identity Manager in *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*. Example scenario for LDAP synchronization: During first time identity data sync from the directory server to Oracle Identity Manager, you want to sync organizations based on a rule, which is based on, say department number. To do so: 1. Run the User Create/Update Full Reconciliation scheduled job. This creates users with default organizations provided within the job parameter. 2. Create a home organization rule, and run the Seed Home Organization scheduled job with `Reset Home Organization` option as **Yes**. This overwrites organizations based on the configured rule. **Note:** Run the Seed Home Organization scheduled job with `Reset Home Organization` option as **Yes** with caution because organizations will be overwritten.	Batch Size: Use this attribute to fetch number of entries from the persistent store in each query. Reset Home Organization: Use this attribute to determine if the organization value of default users will be re-evaluated and overwritten. Select one of the following options: • **No:** If the requirement is to set the organization value for users that do not have any value. • **Yes:** If the requirement is to reset the organization value for all users. This re-evaluates and overrides the organization value for all nondefault users. This option re-evaluates the rule for all existing user data and resets the organization value. If you run the scheduled job with this option selected, then data will be overwritten. The **No** option is the default for this scheduled job.	No

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Sunrise of Accounts and entitlements	This scheduled task sets the status of an account to ENABLE when the start date of the account is reached. In the case of entitlements, this scheduled task grants an entitlement to an account when the start date of the entitlement is reached. **Note:** This task impacts only the accounts and entitlements provisioned directly or through a request.	• Application Instance Name: Name of the application instance. The default value is "ALL." • Max Execution Time: Use this attribute to specify time in minutes, after which the schedule task will stop. The default value is empty. • Process Entity Types: Use this attribute to specify whether the task should process accounts or entitlements. The default value is "ALL."	Yes
Sunset of Accounts and entitlements	This scheduled task sets the status of an account to REVOKE or DISABLE when the end date of the account is reached. In the case of entitlements, this scheduled task revokes an entitlement from an account when the end date of the entitlement is reached. **Note:** This task impacts only the accounts and entitlements provisioned directly or through a request.	• Account Sunset Action: Use this attribute to specify whether the status of the accounts should be set to REVOKE or DISABLE. The default value is REVOKE. • Application Instance Name: Name of the application instance. The default value is "ALL." • Max Execution Time: Use this attribute to specify time in minutes, after which the schedule task will stop. The default value is empty. • Process Entity Types: Use this attribute to specify whether the task should process accounts or entitlements. The default value is "ALL."	Yes
Task Escalation	This scheduled task escalates pending tasks whose escalation time had elapsed at the time when the scheduled task was run.	None	Yes
Task Timed Retry	This scheduled task creates a retry task for rejected tasks whose retry time has elapsed and whose retry count was greater than zero.	None	Yes

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
Update Accounts with App Instance Job	This scheduled task is used to ensure that application instance keys are populated for all entries in the OIU table. In some instances, the application instance might not be available when the account is provisioned. This is possible when: • Oracle Identity Manager is upgraded, when app_instance_key is to be populated for all the existing entries in the OIU table. • Accounts are brought in via reconciliation, but the application instances are not available when the accounts are reconciled. The application instances are created after the reconciliation. • Accounts are provisioned via access policies, but the application instances are not available when the accounts are provisioned. The application instances are created after the provisioning. The Update Accounts with App Instance Job scheduled task checks all the entries in the OIU table corresponding to the resource objects that have a null app_instance_key. It attempts to determine the application instance key based on the obj_key and the IT Resource instance value in the process form. If the scheduled task finds an application instance corresponding to the obj_key and IT resource instance value, then it updates the app_instance_key in the OIU table.	None	Yes
User Operations	This scheduled task performs the operation specified by the UserOperation attribute on the user account specified by the UserLogin attribute.	• UserLogin: User ID of the user account. • UserOperation: Operation that you want to perform on the user account. The value of this attribute can be ENABLE, DISABLE, or DELETE.	No

Table 22-2 (Cont.) Predefined Scheduled Tasks

Job Name	Description	User-Configurable Attributes	Enabled By Default
User Password Upgrade Task	This scheduled task is used to enable the No Password Propagation Support feature in OIG by setting the value of the *No Password Propagation Support* system property to True.	• Batch Size for Processing Records: User records are processed in batches. This attribute specifies the size of the batch and must have a value. The default is 500. • Status for initiating the task: This task is executed if the value of the status is INITIATE. After the job is run successfully, this is changed to STOPPED. It is recommended not to change this status or run this job again. This job changes the login behavior of OIG, hence it should be executed with prior consultation.	No
User Profile Audit Compression	This job compresses the uncompressed user profile audit data and reduces the size of UPA table.	• **Number of Threads:** The number of threads to be executed during the job run. This is a required parameter and the default value is 2. • **Batch Size:** The size of the batch for the job run. This is a required parameter and the default value 1000. • **Time Limit in mins:** Time for which you want to run the job. This is an optional parameter and the default value is 90. See Legacy Audit Data Compression for information about user profile audit data compression.	No

22.4.3 Creating Custom Scheduled Tasks

You can create your own scheduled task metadata, develop the scheduled task class, package it in a JAR file, and upload the JAR file to MDS.

> **See Also:**
>
> Developing Scheduled Tasks in *Developing and Customizing Applications for Oracle Identity Governance* for detailed information about creating a scheduled task.

To create a custom scheduled task:

1. Create the scheduled task XML file and seed it in MetaData Store (MDS).
2. Develop the schedule task class and package it in a Jar.
3. Upload the Jar by:

   Using Plug-ins:

   You can upload the jar using the Plug-in Framework provided by Oracle Identity Manager.

   To upload the jar using plug-ins:

   a. Create the plugin.xml file.
   b. Create the directory structure (plugin.zip) for the scheduled task.
   c. Place the ZIP file in the file store (the *OIM_HOME*/plugins/ directory) or database store.

   Using DB:

   You can upload the jar in the database (DB) of Oracle Identity Manager.

   To upload the jar using DB:

   Upload the jar in DB using UploadJar utility. You can run this utility from the following location:

   ```
   $OIM_HOME/bin/
   ```

> **See Also:**
>
> Upload Jar Utility in *Developing and Customizing Applications for Oracle Identity Governance* for information about running the Upload Jar utility

22.5 Managing Jobs

A job is a task that can be scheduled to run at the specified interval. A job run is a specific execution of a job. Each job run includes information such as the start time, stop time, job status, exceptions and status of the execution.

This section contains the following topics:

- Searching for Jobs
- Creating Jobs
- Editing and Viewing Jobs
- Modifying Jobs
- Disabling and Enabling Jobs
- Running the Jobs
- Deleting Jobs

22.5.1 Searching for Jobs

Use the **Manage Scheduler Jobs** page to perform search for jobs.

To search for the jobs, perform the following steps:

1. Login to Oracle Identity Self Service.
2. Click **Manage** tab and select **System Configuration** box.
3. Select **Scheduler** from the drop-down.
4. Select one or more of the following search conditions to list the history of the job details:
   - Name: Enter the name of the job that you want to search.
   - Status: Search the job status that is applicable for the job search.The following are the types of status:
     - Running
     - Success
     - Interrupted
     - Failed
     - All
   - Start Time With: Select the time duration from the drop-down applicable for the search.
5. Click **Search**.
   The list of jobs that match your search criteria are displayed in a tabular format.

22.5.2 Creating Jobs

Use the **Create Job** page in the **Manage Scheduler** section of Identity System Administration to create a new job.

> **Note:**
>
> The procedure described in this section assumes that the XML file for the scheduled task, which contains the job description is available in the *OIM_HOME*/metadata/file directory.

To create a job:

1. Login to Oracle Identity Self Service.
2. Select **Manage**, under **System Configuration**, click **Scheduler**.

   The **Manage Scheduler Jobs** section is displayed.
3. Select **Create Job**.
4. On the **Create Job page**, enter values in the following fields under the Job Information section:
   - **Name:** Enter a name for the job.

- **Template:** Specify the template of the scheduled task that runs the job.
- **Start Date:** Specify the date and time on which you want the job to run. To do this, select the date and time along with timezone from the date editor and click **Ok**. By default, the timezone is "(UTC-08:00) US Pacific Time".
- **Retries:** Retry count is used to manage the job in case of failure. A job cannot execute more than its retry count if it fails consecutively. The job is disabled if it fails consecutively till its retry count is exhausted. The job must be enabled from the UI for further execution.
- **Schedule Type:** Depending on the frequency at which you want the job to run, select one of the following schedule types:
  - **Periodic:** Select this option if you want the job to be run at a time that you specify, on a repeating basis. If you select this option, then you must enter an integer value in the Run every field under the Job Periodic Settings section and select one of the following values:
    - Minutes
    - Hours
    - Days
    - Weeks
    - Months
    - Yearly
  - **Single:** Select this option if the job is to be run only once at the specified start date and time.
  - **None:** This option specifies that no schedule is attached to the job you are creating, and therefore, it is not triggered automatically. As a result, the only option to trigger the job is by clicking **Create and Run Now**.
- **Sub Types**: Select the sub category type for the job.

5. Enter the following values in the **Parameters** section:

> **Note:**
>
> The following values are dynamic and change depending on the job template that you select.

- **Flat File Path**: Enter the path of CSV file for seeding metadata or directory path containing XML for seeding technical glossary.
- **Batch Size**: Enter the size of the batch.
- **Thread Size**: Enter the Thread size.
- **Mode**: Enter the mode.

6. Enter values in the following fields under the **Scheduling Failed Notification** section:
   - **Beneficiary**: Select the Beneficiary type to whom the scheduled job failure notification email is sent.
     - User Login

  - Role Name
  - Specified Address
- **Send To**: Enter the User Login, Role name or specific email id to which scheduled job failure notification email is sent.

7. Click **Next**.
8. Select one of the following schedule types in **Schedule** section:

> **Note:**
>
> This is a mandatory field.

   - Periodic: Select this option if you want the job to be run at a time that you specify, on a repeating basis. If you select this option, then you must enter an integer value in the Run every field under the Job Periodic Settings section and select one of the following values:
     - Minutes
     - Hours
     - Days
     - Weeks
     - Months
     - Yearly
   - Single: Select this option if the job is to be run only once at the specified start date and time.
   - None: This option specifies that no schedule is attached to the job you are creating, and therefore, it is not triggered automatically. As a result, the only option to trigger the job is by clicking **Create and Run Now**.
9. In the **Summary** section, verify if the details are correct.
10. Select one of the following options:
    - **Create and Run Now**: Select to save and create and run the job immediately.
    - **Create**: Select to create the job.
    - **Back**: Select to go to the previous screen.
    - **Cancel**: Select to cancel the operation/.

22.5.3 Editing and Viewing Jobs

Use the **Edit Job** action item in **Manage Scheduler** page to view and edit job-related information, such as job status, scheduled job failed notifications, job history information, along with a display of errors and milestones during the job search operation.

To edit or view the details of a job:

1. Login to Oracle Identity Self Service.
2. Click **Manage** tab and select **System Configuration** box.

3. Select **Scheduler** from the drop-down.
   The **Manage Scheduler Jobs** page is displayed.
4. Click **Edit** in the **Jobs** tab for the job you want to edit or view in the **Job Search results** table.
   The **Job Details** page is divided into the following sections:
   - **Template**: Enter the template name to modify the details of the job name.
   - **Retries**: Enter the retry count for the job.
   - **Schedule Type**: Select one of the following schedule types:
     - Periodic: Select this option if you want the job to be run at a time that you specify, on a repeating basis.
     - Single: Select this option if the job is to be run only once at the specified start date and time.
     - None: This option specifies that no schedule is attached to the job you are creating, and therefore, it is not triggered automatically.
   - **Start Time**: Select the start date and time on which you want the job to run.
   - **Interval Type**: Select the interval frequency from the following drop-down options:
     - Minutes
     - Hours
     - Days
     - Weeks
     - Months
     - Yearly
   - **Minutes Between Runs**: Enter the interval type for the scheduled job that needs to be run.
   - **Beneficiary**: Select the type of beneficiary from the list:
     - User Login
     - Role Name
     - Specified Address
   - **Send To**: Enter the User Login, Role name or specific email id to which scheduled job failure notification email is sent.

   After viewing the details of the job, you can either modify, run, or stop the job. In addition, you can also enable or disable the job. Job Detail screen can be refreshed.

   After you view the details of the job on the Job Details page, you can perform one of the following:
   - If you want to modify the details of the job, then make the relevant change and click **Execute** to run the job.
   - You can enable or disable by selecting either **Enable** or **Disable**.
   - You can reset the values by selecting **Reset**.
   - If the Disable button is enable, then it means that the job is currently enabled and you can disable the job by clicking **Disable.**

- If the Enable button is enable, then it means that the job is currently disabled and you and enable the job by clicking **Enable.**

22.5.4 Modifying Jobs

Use the **Job Details** page to modify the attributes of a scheduled job.

To modify a job:

1. Login to Oracle Identity Self Service.
2. Click **Manage** tab and select **System Configuration** box.
3. Select **Scheduler** from the drop-down.
4. On the **Job Details** page, you can modify all the details of the job, except for the Job Name and Task fields under the Job information section and the fields under the Job Status section. See Step 4 of Creating Jobs for details about the fields that you want to modify.
5. Click **Apply** to commit the changes made on the Job Details page to the database.

   A message confirming that the job has been successfully modified is displayed.

22.5.5 Disabling and Enabling Jobs

Use the Job Details page to enable or disable a scheduled job.

To enable or disable a job:

1. Login to Oracle Identity Self Service.
2. Click **Manage** tab and select **System Configuration** box.
3. Select **Scheduler** from the drop-down.

   The **Manage Scheduler Jobs** page is displayed.
4. In the **Job Results** table, select the job name you want to enable or disable.
5. Select **Enable** or **Disable**.
6. Click **Yes** to confirm.

   A confirmation box confirming the success is displayed.

22.5.6 Running the Jobs

In addition to scheduling jobs to run automatically at the specified time, you can run the jobs.

For example, you create and schedule a job that runs every Friday. However, if you want to run the job on any day other than Friday, then you must run the job manually.

To run a job, perform the following steps:

1. Login to Oracle Identity Self Service.
2. Select **Manage** tab.
3. Click **System Configuration** box, and select **Scheduler**.

   The **Manage Scheduler Jobs** section is displayed.
4. In the **Job Search** results table, click **Run Job**.

5. Click **Yes** to confirm, or click **No**.

   A confirmation box confirming the success is displayed.

   OR

6. Select the job and click **Edit** to run the job.
7. In the **Edit or View Job** section, Click **Action** and select **Execute**.

   A dialog box prompting you to confirm if you want to run the job is displayed.

22.5.7 Deleting Jobs

Use the Manage Scheduler section under the Manage tab to delete scheduled jobs that are not required or are not in use.

To delete a job:

1. Login to Oracle Identity Self Service.
2. Click **Manage** tab and select **System Configuration** box.
3. Select **Scheduler** from the drop-down.

   The Manage Scheduler Jobs page is displayed.
4. Navigate to the **Jobs** tab, in the search option, search for the job you want to delete by entering the name of the job.
5. Click **Delete** button.
6. Click **Yes.**

   A message indicating that the job has been deleted successfully is displayed.

22.6 Diagnosing Scheduled Jobs

Diagnose issues related to scheduled job run when the scheduled job is not running according to the scheduled time.

This section describes how to diagnose issues related to scheduled job run.

- Schedule Job Errors
- Resolving the Schedule Job Errors
- Configuring a Custom Property to Avoid Delay in Scheduled Job Run

22.6.1 Schedule Job Errors

Typical scheduled job errors include no job run at the specified time, no entry in the JOB_HISTORY table for the run, and no exceptions recorded in the server logs.

Scheduled job is not running according to the scheduled time, and the following is observed:

- Scheduled job is not run on the scheduled time.
- No exceptions are recorded in the server logs.

22.6.2 Resolving the Schedule Job Errors

Diagnosing scheduled job errors include activities such as, enabling scheduler logging, and verifying that scheduler is running, the job is enabled, and clocks are in sync on all nodes.

To diagnose this issue:

1. Verify whether scheduler service is running or not. Scheduler service is deployed on each node of the cluster until this service is not explicitly disabled. This can be disabled by setting the `scheduler.disabled` server level property to `false` for that node. The following URL can be used to verify the status of the scheduler service:

   http://*OIM_HOST*:*OIM_PORT*/SchedulerService-web/status

   In this URL, *OIM_HOST* is the name of the computer hosting the Oracle Identity Manager server and *OIM_PORT* is the port on which Oracle Identity Manager server is listening.
2. Verify whether the specific job is enabled or not. This can be verified from the Scheduler section of Identity System Administration. The job must be enabled to run per the schedule.
3. Verify whether clocks are in sync for all nodes. Clocks must be within a second of each other
4. Delete the existing trigger from Scheduler UI, and schedule a new trigger from the UI. Verify whether the issue persists or not.
5. Enable scheduler logs by changing log level to `DEBUG`. This can be done by changing log level for the `oracle.iam.scheduler.impl` package from Oracle Enterprise Manager. Verify whether the following messages are traced in logs or not:

   ```
   Job Listener, Job was executed '$JOB_NAME'
   Job Listener, Job to be executed '$JOB_NAME'
   ```

   Here, $*JOB_NAME* is the name of the job that is supposed to be executed at that time.

   If the messages are not logged, then contact Oracle Support.
6. In Oracle Enterprise Manager, check the `threadPoolSize` parameter for the `schedulerConfig` segment in the `oim-config.xml` file. This is the number of threads that are available for concurrent execution of jobs. Therefore, the number of jobs that can be executed on a particular time cannot be more than the configured `threadPoolSize` count. Running of such jobs is skipped and executed as per the next scheduled time, which gives an impression that the job is not executed per the scheduled time. The default value of this parameter is `10`, but is can be tuned as required.
7. Restart the server and verify whether the job has been run or not.
8. Verify whether the following exception is logged:

   ```
   Caused By: java.lang.NullPointerException at
   org.quartz.SimpleTrigger.computeNumTimesFiredBetween(SimpleTrigger.java:800)
   ```

   Run following query to fix this issue:

   ```
   UPDATE QRTZ92_TRIGGERS SET NEXT_FIRE_TIME=1 WHERE  NEXT_FIRE_TIME<1;
   ```
9. Sometimes the trigger status is not updated in the `QRTZ92_TRIGGER` table from `BLOCKED` to `PAUSED` state. This situation happens if the environment is not tuned properly, and database connections from the pool are exhausted by other parallel operations running on the server. As a result, QUARTZ framework is not able to get connection from the pool

to update the running job. This situation can be identified if exceptions related to database connection pool is observed in the server logs. Usually, such triggers get fixed after server restart, but if trigger status still remains the same, then running the following query can help:

```
UPDATE QRTZ92_TRIGGERS SET TRIGGER_STATUS='WAITING' WHERE JOB_NAME
='$JOB_NAME'
```

Replace $*JOB_NAME* with the job name.

10. Sometimes manual trigger for a job is not updated in the `QRTZ92_TRIGGER` table. Manual trigger is created in the system when you execute the job by clicking **Run Now** from the Scheduler UI or use the Scheduler `runNow()` API. Such trigger is supposed to be deleted after the job is executed successfully. To fix this issue:
    a. Shutdown the server.
    b. Run the following queries on Oracle Identity Manager database:

```
DELETE FROM QRTZ92_FIRED_TRIGGERS where TRIGGER_NAME like ('MT_%');
DELETE FROM QRTZ92_SIMPLE_TRIGGERS where TRIGGER_NAME like ('MT_%');
DELETE FROM QRTZ92_TRIGGERS where TRIGGER_NAME like ('MT_%');
```

Automatic deletion of such manual triggers is maintained by the Quartz framework.

22.6.3 Configuring a Custom Property to Avoid Delay in Scheduled Job Run

In the Scheduler section of the Identity System Administration, when you click the **Run Now** button, the scheduled job run does not start immediately. It starts running after a delay of a few minutes.

To workaround this issue:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control 12c.
2. Navigate to the System MBean Browser.
3. Under Application Defined Mbeans, expand **Oracle.iam**, **Server: *OIM_SERVER***, **Application: oim**, **XMLConfig**, **XMLConfig.SchedulerConfig**.
4. Click the **Scheduler** mbean, and then click the **Operations** tab.
5. Click **createCustomProperty**.
6. In the Operation: createCustomProperty page, under Parameters, enter the following parameter values:
    - **propName:** `org.quartz.jobStore.misfireThreshold`
    - **propValue:** `10000`
7. Click **Invoke**. After the operation is successful, click **Return**.
8. In the Operations tab, verfiy the property by clicking **fetchCustomProperties**.
9. Click **Invoke**. The property you set in step 6 is displayed under Return Value.
10. Restart the Oracle Identity Governance server.

23
Managing System Properties

You can control the behavior of various Oracle Identity Governance components by using System Properties. Managing system properties involve understanding the predefined and configurable system properties, searching and modifying the system properties, and configuring various components and the identity provider by using the Manage System Properties.

This content applies only to OIG Bundle Patch 12.2.1.4.221004 and later releases.

This chapter describes how to manage system properties, predefined and configurable system properties. It contains the following sections:

- About System Properties
- Types of System Properties
- Managing System Properties

23.1 About System Properties

System Properties are entities that lets you control the configuration of Oracle Identity Manager.

System properties define the characteristics that control the behavior of Oracle Identity Manager. You can define the functionality of user interfaces, such as the Oracle Identity Manager Self Service and Oracle Identity Administration, by using system properties. For example, you can define the number of consecutive attempts the user can make to login to Oracle Identity Manager unsuccessfully before Oracle Identity Manager locks the user account. In other words, a system property is an entity by which you can control the configuration of Oracle Identity Manager.

23.2 Types of System Properties

Various system properties are predefined in the PTY table of the database. In addition, you can add some system properties to the PTY table.

This section describes the different types of system properties in the following topics:

- Default System Properties in Oracle Identity Governance
- Non-Default System Properties in Oracle Identity Governance

23.2.1 Default System Properties in Oracle Identity Governance

Default system properties are predefined in the PTY table. Each system property has a keyword and default value.

Table 23-1 describes default system properties in Oracle Identity Governance.

Table 23-1 Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Access Policy Revoke If No Longer Applies Enhancement	XL.AccessPolicyRevokeIfNoLongerAppliesEnhancement	FALSE	Determines if the Revoke if no longer applies flag in access policy is applicable. If the value is true, then this flag is applicable to child table data (entitlements) along with parent data. The user can determine if child data must be removed or retained when access policy no longer applies to user based on this flag. If the value if false, then child table data (entitlements) are always removed after access policy is no longer applied. **Note**: This property is not used in Oracle Identity Manager Release 2 (11.1.2) or later.
Administrator capability to manage proxies	ADMIN_CAPABILITY_TO_MANAGE_PROXIES	True	This property is used to control the administrator capabilities for proxy users. If the property is set to FALSE, the Proxy User tab will not be visible on the User Details screen. **Note:** • If you change the value of this property to False, then it is important to log in again to ensure there are no errors. • The system administrator role has the capabilities, however now a delegated system administrator can manage the proxy users for any user.
Allows access policy based provisioning of multiple instances of a resource	XL.AllowAPBasedMultipleAccountProvisioning	FALSE	Determines if multiple instances of a resource can be provisioned to multiple target resources. When the value is false, provisioning multiple instances of resource object via access policy is not allowed. When the value is true, provisioning multiple instances of resource object via access policy is allowed.
Allows control over role hierarchical access policy evaluation	XL.AllowRoleHierarchicalPolicyEval	FALSE	This property is used to control allowing role hierarchical access policy evaluation. When this system property is set to TRUE, access from inherited access policies is given to the user. If set to FALSE, access from access policies attached to inherited roles is not given to the user.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Allows linking of access policies to reconciled and bulk loaded accounts	XL.AllowAPHarvesting	FALSE	Determines if access policy engine can link access policies to reconciled accounts and to accounts created by the Bulk Load Utility. This property is used in the context of evaluating access policies for reconciled accounts and to accounts created by the Bulk Load Utility. **Note:** This property is used in Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0) or later.
Allows linking of access policies to Direct Provisioned accounts	XL.APHarvestDirectProvisionAccount	FALSE	This property is used to link access policies to accounts that are provisioned through Direct Provisioning. When this system property is set to True, the account which is provisioned through Direct Provisioning is linked to the Access Policy based provisioned account. If set to FALSE, then the account which is provisioned through Direct Provisioning is not linked to the Access Policy based provisioned account.
Allows linking of access policies to request based accounts	XL.APHarvestRequestAccount	FALSE	This property is used to link access policies to accounts that are provisioned through Request Provisioning. When this system property is set to True, the account which is provisioned through Request Provisioning is linked to the Access Policy based provisioned account. If set to FALSE, then the account which is provisioned through Request Provisioning is not linked to the Access Policy based provisioned account.
XL.APHarvesting.AllowAccountDataUpdate	XL.APHarvesting.AllowAccountDataUpdate	FALSE	This property is used to update the account data with the policy defaults for the accounts linked to the access policies. When this system property is set to True, the account data is updated with the policy defaults for the accounts linked to access policy. If set to False or if the system property does not exist, the account data is not updated. **Note:** This system property is available only after you apply Oracle Identity Governance Bundle Patch 12.2.1.4.201011.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Do not evaluate Access policy for disabled user	XL.DoNotEvaluateAPForDisableUsers	FALSE	If the value is set to TRUE, then disabled users are not evaluated for **Evaluate User Policies** by Access Policy. If the value is set to FALSE, then disabled users are evaluated by **Evaluate User Policies** Scheduler Job. **Note:** This system property is available only after you apply Oracle Identity Governance Bundle Patch 12.2.1.4.211010.
Are challenge questions disabled in OIM	OIM.DisableChallengeQuestions	FALSE	Determines if challenge questions are enabled or disabled when a user logs in to Oracle Identity Manager for the first time. When value is False, challenge questions are enabled. When value is True, challenge questions are disabled. This property is primarily used in the context of Oracle Adaptive Access Manager (OAAM) configuration. When the value is TRUE, the challenge questions are handled by OAAM. When the value is FALSE, then PWR.PWR_CHA_POLICY_ENABLED is honored to determine if challenge policy is enabled or not.
Catalog Additional Application Details Task Flow	CatalogAdditionalApplicationDetailsTaskFlow	/WEB-INF/oracle/iam/ui/common/tfs/empty-tf.xml#empty-tf	A custom task flow is to be displayed when an application is selected from the catalog checkout page. The task flow page will display as a tab in the cart details section.
Catalog Additional Entitlement Details Task Flow	CatalogAdditionalEntitlementDetailsTaskFlow	/WEB-INF/oracle/iam/ui/common/tfs/empty-tf.xml#empty-tf	A custom task flow is to be displayed when an entitlement is selected from the catalog checkout page. The task flow page will display as a tab in the cart details section.
Catalog Additional Role Details Task Flow	CatalogAdditionalRoleDetailsTaskFlow	/WEB-INF/oracle/iam/ui/common/tfs/empty-tf.xml#empty-tfs	A custom task flow is to be displayed when a role item is selected from the catalog checkout page. The task flow page will display as a tab in the cart details section.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Catalog Advanced Search Maximum Applications	CatalogAdvancedSearchMaxApps	15	In the default form for catalog advanced search, you can search for entitlements by specifying the list of applications to search from. This system property controls the maximum number of applications that can be selected for entitlement search.
Catalog Advanced Search Taskflow	CatalogAdvancedSearchTaskflow	/WEB-INF/oracle/iam/ui/catalog/tfs/catalog-advanced-search-tf.xml#catalog-advanced-search-tf	Determines the taskflow used for catalog search. If you create custom taskflow for catalog search, then change the value of this property to the complete path of the custom taskflow.
Catalog Attributes for Sorting Search Results	CatalogSortAttributes	ENTITY_DISPLAY_NAME; ENTITY_TYPE	This property determines the attributes that will be displayed in the Sort By drop down in the catalog results tab.
Catalog Audit Data Collection	XL.CatalogAuditDataCollection	none	Determines if catalog auditing is enabled or disabled. The default value is `none`, which specifies that catalog auditing in disabled. To enable catalog auditing, set the value of this property to `catalog`.
Category count option can be 0, 1 or 2	CATALOG.CATEGORY_COUNT_OPTION	2	Determines what is displayed in the Category count block. If the value is 0, then Category Count block is deactivated. If the value is 1, then distinct categories across the system are displayed without respective category count. If the value is 2, then Categories with count are displayed. **Note**: It is recommended that the values be modified in cases they are observing poor Catalog Search performance.
Catalog Regex for special characters	Catalog.SpecialCharacterRegex	[^\w]	Enables text parsing and escaping of special characters when performing a catalog search by using some special characters. If you do not want any text parsing and escaping of special characters, then change the value of this property to `[^\w^\W]`.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Catalog search MAX result size. Default value is -1 which means return all	XL.CatalogSearchResultCap	-1	When the data is huge in the request catalog and you encounter any issue with the performance of the catalog, you can change the value of this system property and provide some reasonable values, such as 500. As a result, catalog search will not return more than the specified value. If the value is -1, then no result size limit is applied on the catalog search result.
Catalog Searchable UDF In Tags	CATALOG.SearchableUdfInTags	FALSE	If want to use searchable UDF in TAGS, then you can set the value of this property to TRUE. Then, you can run the scheduled task in recalculate tags mode and searchable UDF values will be part of the TAGS column. The same value can be used in keyword search.
Catalog Table Rows To Display Size	CatalogTableRowsToDisplaySize	10	This property is used to control the number of rows displayed in all tables found in all catalog-related pages. **Note:** The value of this system property must be less than or equal to 50.
CommonName generation plugin	XL.DefaultCommonNamePolicyImpl	oracle.iam.ldapsync.impl.plugins.FirstNameLastNamePolicy	Determines the common name generation plugin to generate common name.
Compiler Path for Connectors	XL.CompilerPath	*JAVA_HOME*	Specifies the Java home depending on the application server. **Note:** If the path of the JDK directory is not included in the System Path variable, then you must set the path of the JDK directory in the XL.CompilerPath system property. If this is not done, then an error is encountered during the adapter compilation stage of the process performed when you import an XML file by using the Deployment Manager.
Compute and Persist Min Age On Password Change	ComputePersistMinAgeOnPasswordChange	proactive	Password minimum age calculation has two modes, proactive and reactive mode. In proactive, where minimum age date is calculated at password change time, any subsequent change to the user's applicable password policy's minimum age property will not be honored until the next password change, where as with the reactive approach, policy changes will be applied immediately. To enable proactive or reactive approach, system property Compute Persist Min Age On Password Change is introduced.
Control allowing Request Data to Prepopulate Adapters	XL.AllowRequestDataToPrepopAdapter	FALSE	This property is used to control the order of preference for populating the process form data during provisioning. If this property is set to TRUE, pre-populate adapters data will take precedence over access policy or request data. That is access policy or request data will be overridden with pre-populate adapters data. If the property is set to FALSE, access policy or request data will have precedence over pre-populate adapters data.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Copy manager of user also for create user email notification	XL.NotifyUserCreateToOther	TRUE	Copies the user's manager in the email notification that is sent when a user is created.
Data Collection Session ID	XL.DataCollectionSessionID	dummy	Specifies the session ID of the current Oracle Identity Analytics (OIA) Data collection session.
Data Collection Status	XL.DataCollectionStatus	FINALIZED	Specifies the status of the current OIA data collection session.
DB Diagnostic Level for Data Truncate	OIM.DBDiagnosticLevelDataTrunc	NONE	This property controls the amount of diagnostic logging for Complete Nuke Cleanup operation. The values can be: • **NONE:** No information is collected to debug the complete nuke cleanup operation. This is the default value. • **FINEST:** Fine-grained information is collected to debug the complete nuke cleanup operation.
DB Diagnostic Level for Offline Data Purges	OIM.DBDiagnosticLevelOffPurge	NONE	This property controls the amount of diagnostic logging for Offline Data Purge operation. The values can be: • **NONE:** No information is collected to debug the offline data purge operation. This is the default value. • **FINEST:** Fine-grained information is collected to debug the offline data purge operation.
DB Diagnostic Level for OIM GDPR support	OIM.DBDiagnosticLevelGdprSupp	NONE	This property is used to enable or disable detailed logging in database. The values can be: • **NONE:** Logging is disabled. This is the default value. • **FINEST:** Logging is enabled.
DB Diagnostic Level for OIM Mview Legacy Data Migration	OIM.DBDiagnosticLevelMviewMig	NONE	This property defines the DB diagnostic level for OIG materialized view legacy data migration. The values can be: • **NONE:** Logging is disabled. This is the default value. • **FINEST:** Logging is enabled.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
DB Diagnostic Level for MView creation for BIP report	OIM.DBDiagnosticLevelMviewBIP	NONE	This property defines the DB diagnostic level for Mview creation for BIP reports. The values can be: • **NONE:** Logging is disabled. This is the default value. • **FINEST:** Logging is enabled.
DB Diagnostic Level for Online Data Purge	OIM.DBDiagnosticLevelDataPurge	NONE	This property controls the amount of diagnostic logging and debugging required in PL/SQL layer during OIM Data Purge scheduled task operation. The values can be: • **NONE:** No information is collected to debug the online data purge operation in PL/SQL layer. This is the default value. • **FINEST:** Fine-grained information is collected to debug the online data purge operation in PL/SQL layer.
DB Diagnostic Level for Recon	OIM.DBDiagnosticLevelRecon	INFO	This property controls the amount of diagnostic logging and debugging required in PL/SQL layer during reconciliation operations. The values can be: • **INFO:** Coarse-grained level information is collected to debug the reconciliation operation in PL/SQL layer. This is the default value. • **FINE:** Fine-grained information is collected to debug the reconciliation operation in PL/SQL layer. • **FINEST:** Fine-grained information along with data for collection variables used as input to Stored Program Units is collected to debug the reconciliation operation in PL/SQL layer. • **NONE:** No information is collected to debug the reconciliation operation in PL/SQL layer.
DB Diagnostic Level for Online Recon Exceptions Purge	OIM.DBDiagnosticLevelRecx	NONE	This property controls the amount of diagnostic logging and debugging required in PL/SQL layer during Recon Exceptions Purge operation. The values can be: • **INFO**: Coarse-grained level information is collected to debug the Recon Exceptions Purge operation in PL/SQL layer. • **FINE**: Fine-grained information is collected to debug the Recon Exceptions Purge operation in PL/SQL layer. • **FINEST**: Fine-grained information along with data for collection variables used as input to Stored Program Units is collected to debug the Recon Exceptions Purge operation in PL/SQL layer. • **NONE**: No information is collected to debug the Recon Exceptions Purge operation in PL/SQL layer. This is the default value.
Default Date Format	XL.DefaultDateFormat	yyyy/mm/dd hh:mm:ssz	When creating reconciliation events by calling the APIs and date format is not passed as one of the arguments to the API, Oracle Identity Manager assumes that all the date field values are specified in Default Date Format.
Default policy for username generation	XL.DefaultUserNamePolicyImpl	oracle.iam.identity.usermgmt.impl.plugins.DefaultComboPolicy	Determines the username policy to use when generating a username.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Default user name domain	XL.UserNameDomain	oracle.com	This property is used by the DefaultComboPolicy to generate a user name in e-mail format.
Disable Catalog Blank Search	CATALOG.DISABLE_BLANK_SEARCH	True	This property is used to enable or disable blank text search in Catalog. If the value is True, then blank text search is disabled. If the value is False, then blank text search is enabled. **Note**: Catalog search functionality can run slow depending upon the volume of data in the system. It is recommended to disable blank search functionality to improve search performance.
Disabling Default Search of UI pages	OIG.DisableDefaultTableSearches	FALSE	This property is used to enable or disable blank text search in the Users, Roles, Organizations, and Administration Roles page. If the value is TRUE, then blank text search is enabled. If the value is FALSE, then blank text search is disabled.
Display Certification or Attestation	OIM.ShowCertificationOrAttestation	attestation	This property has been superseded by the `Identity Auditor Features Enabled` system property, and attestation is no longer supported. **Note:** In this release, this property is not used as Attestation is not supported. This property is superceded by the `Identity Auditor Features Enabled` system property.
DM Global Search Result Size	DMGlobalSearchResultSize	100	This system property controls the number of records displayed for deployment manager global search result. If incorrect or non-numeric value is set, then default value is considered. **Note:** It is recommended that the value of this system property is less than 1000.
Does user have to provide challenge information during registration	PCQ.PROVIDE_DURING_SELFREG	TRUE	If the value is TRUE, then users will have to provide challenge information during registration.
Email Server	XL.MailServer	Email Server	Name of the e-mail server. **Note:** After modifying the Email Server system property value, you must restart the server for the change to take effect.
Email URL token expiration time (in days)	OIM_EMAIL_URL_EXPIRE_TIME	1	This system property determines the time until when the forgot password Email link is valid.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Email Validation Pattern	XL.EmailValidationPattern	[A-Za-z0-9\._\#\!\$\&\'*\/\=\?\^\`\{\}\~|\%\+\-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}	This property contains the regular expression used to validate the email ID of a user.
Enable disabled resource instances when a user is enabled	XL.EnableDisabledResources	TRUE	If the value is TRUE, then the disabled resource instances are enabled when a user is enabled.
Enable email notification based password reset	OIM_ENABLE_EMAIL_SEC_FEAT	True	This property is used to enable Email notification for forgot password. If this property is set to False, then the feature is disabled.
Enable Exception Reports	XL.EnableExceptionReports	TRUE	This property is used to enable the exception reporting feature. Exception reporting is enabled only if the value is set to TRUE.
Enable User Login Validation	XL.ValidateWhiteSpace	FALSE	This property enforces the validation of the user login for special characters.
Enable SQL Query Based Role Membership	RoleUserMembershipRuleSQLSupported	FALSE	If the property value is TRUE, an admin can define SQL query as the user membership rule for Roles.
Evaluate All Role for SQL Membership Rule in Refresh Role Membership Job	RefreshRoleMembershipJob.EvaluateAllRolesForSQLMembershipRule	FALSE	If the property is set to TRUE, then the **Refresh Role Membership Job** job evaluates all the SQL based membership rules.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Evaluate LDAP Container Rules for Entity Modification	LDAPEvaluateContainerRulesForModify	FALSE	If the property value is TRUE, then the LDAP container rules defined in LDAPContainerRules.xml are evaluated for entity modification. However, if none of the rules match, then the default container is not returned. The original parent container of the entity is returned, which means that there is no change in the entity DN. If the property value is FALSE, then the LDAP container rules defined in LDAPContainerRules.xml are not evaluated. The entity DN does not change. **Note:** This property only applies to a modification scenario and not to the entity creation scenario.
Execute Dymanic RoleMembershipOrchUsingAsync	XL.ExecuteDymanicRoleMembershipOrchUsingAsync	false	If the value of this property is set to true, then the role grant/revoke takes place asynchronously.
Force to set questions at startup	PCQ.FORCE_SET_QUES	False	When the user logs into the Oracle Identity Self Service or Oracle Identity System Administration for the first time, the user must set the default questions for resetting the password. **Note:** After modifying the value of this property, you must restart Oracle Identity Manager server for the changes to take effect.
GTC Auto Import	XL.GTCAutoImport	true	Based on the value of this property, the DM xml that is generated while Generic Technology Connector (GTC) creation can be saved to a directory. The default value of this property is true. When the value of this property is set to "False", then while creating GTC, the DM xml (the xml that GTC creates and imports using Deployment Manager internally while GTC creation) created by the GTC framework is stored in the following directory: *OIM_HOME*/GTC/XMLOutput The naming convention followed for the DM xml is: *GTCNAME_CURRENTDATE_ TIMESTAMP* created using date format "yyyy-MM-dd-HH-mm-ss".xml For example: TRUSTEDCSV_2009-02-05-22-41-11.xml
IDMDF: Attachment FilePath	IDM.Diagnostics.IDMDFClient.Notifier.Attachment.File	/scratch/IDMDFAttachment	This property determines the path to store the attachment files.
IDMDF: Buffer size to hold context sensitive logs	IDM.Diagnostics.EventProcessing.ContextSensitiveLogsBufferSize	10000	This property determines the size of the buffer that holds detailed logs of the product.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
IDMDF: Buffer size to hold failed records	IDM.Diagnostics.EventProcessing.FailedRecordBufferSize	1000	This property determines the size of the buffer that holds failed (functional/SLA) events.
IDMDF: Debug mode (true/ false)	IDM.Diagnostics.Debug	False	This property determines if logs of IDMDF framework in a log file is saved. When set to TRUE, debug mode is enabled. When set to False, debug mode is disabled.
IDMDF: Default SLA	IDM.Diagnostics.DefaultSLA	300000	This property determines the size of the default SLA for events.
IDMDF: E-mail notification to	IDM.Diagnostics.Notification.Email.To	dummy.dummy@dummy.com	This property determines the email address to which notification is sent.
IDMDF: E-mail notification from	IDM.Diagnostics.Notification.Email.From	dummy.dummy@dummy.com	This property determines the email address from which notification is sent.
IDMDF: Email Message Template Path	IDM.Diagnostics.IDMDFClient.Notifier.Email.MessageTemplatePath		This property determines the path of the email message template.
IDMDF: Enabled/ Disabled By Sysadmin	IDM.Diagnostics.Enabled	false	This property is used by the system administrator to enable or disable IDMDF.
IDMDF: Flood Control Duration(In Days)	IDM.Diagnostics.EmailFloodControl.DurationInDays	1	This property indicates the retention period in days for Flood Control Max email. After the defined number of days, the Flood Control Max email counter is reset.
IDMDF: Flood Control Max Email	IDM.Diagnostics.EmailFloodControl.MaxEmail	2	This property determines the maximum number of notifications allowed per use case.
IDMDF: In-Memory Logging	IDM.Diagnostics.IDMDFClient.InMemoryLogging	false	This property determines if logs are stored in the memory.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
IDMDF: Max failed event to execute concurrently	IDM.Diagnostics.EventProcessing.MaxConcurrent.FailedEvent	2	This property determines the number of threads to execute events concurrently and put it in the database.
IDMDF: Notification provider	IDM.Diagnostics.NotificationProvider	oracle.idm.diagnostics.notification.service.impl.IdmdfNotifier	This property determines the service used for sending notifications.
IDMDF : Notification template file name	IDM.Diagnostics.IDMDFClient.Notifier.Email.MessageTemplateName		This property determines the notification template file name.
IDMDF: IDMDF Rest service end-point	IDM.Diagnostics.IDMDFServiceEndPoint	http://localhost:14000/idmeventrecording	This property determines the URL where IDMDF services are deployed. **Note:** If the REST service is not working as expected, then check and if required update the local host name and port number configured in `IDMDF: IDMDF Rest service` end point. On a clustered environment, the `IDMDF: IDMDF Rest service` end point should be updated with host name and port number where OHS is running. In a single node configuration, this end point should be updated with host name and port number where OIG is running.
IDMDF: SMTP Server Name	IDM.Diagnostics.Email.Server.Host	localhost	This property represents the server responsible for sending email notification.
IDMDF: SLA template file	IDM.Diagnostics.IDMDFClient.Notifier.Sla.File	None	This property determines the file that contains the list of SLAs for defined use cases.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Identity Auditor Feature Set Availability	OIG.IsIdentityAuditorEnabled	FALSE	When the value of this property is TRUE, role lifecycle management, Segregation of Duties (SoD), and identity certification are enabled. **Note:** After modifying the value of this system property, you must restart Oracle Identity Governance server for the changes to take effect.
Inbox Task Tabs (none/all)	UI.INBOX.VIEW.TaskTabs	none	This property determines whether or not to show additional links, such as Initiated tasks, Reportees and Administrative tasks, in the Inbox. When set to all, the following links are displaied in the Inbox: My tasks,Initiated tasks, Reportees, Administrative tasks. When set to none, only the My tasks link is displayed in the Inbox.
Indicates if referential integrity is enabled in target LDAP directory	XL.IsReferentialIntegrityEnabledInLDAP	FALSE	The value of this property is TRUE if referential integrity in target LDAP directory is turned on. The value of this property is FALSE if referential integrity in target LDAP directory is turned off. To be able to modify an entity stored in LDAP, this prop must be set to TRUE.
Is DataProvider LDAP/DB	OIM.DataProvider	DB	Specifies the data provider, which is Oracle Identity Manager database. The default value is DB, which indicates that the database is the data provider.
Is disabled manager allowed	AllowDisabledManagers	FALSE	Specifies whether a user in the disabled state can be set as a manager for another user.
Is OIM Notifications disabled (true/false)	XL.DisableAllNotifications	false	This property is used to enable or disable all notifications in Oracle Identity Manager. When the value of this property is set to false, notifications are enabled. When the value of this property is true, notifications are disabled.
Is Self-Registration Allowed	XL.SelfRegistrationAllowed	TRUE	If the value is TRUE, then the users are allowed to self-register.
LDAP Reservation Plugin	XL.LDAPReservationPluginImpl	oracle.iam.identity.usermgmt.impl.plugins.reservation.ReservationInOID	This property determines the LDAP reservation plugin implementation to be picked up for reservation of user attributes.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Level of Role Auditing	XL.RoleAuditLevel	None	This property controls the amount of audit data collected when an operation is performed on a role, such as creation or modification. The supported levels are: • **None:** No audit data is collected. • **Role:** Creation, modification, and deletion of role is audited. • **Role Hierarchy:** Changes made to the role inheritance is audited.
Login Validation Pattern	XL.LoginPattern	(^[A-z0-9@._-]{2,256}$)	This property contains the regular expression used to validate the login of a user when XL.ValidateWhiteSpace is set to true. If XL.LoginPattern is empty, then user login is validated against the default pattern. **Note:** It is recommended that the regular expression is developed and tested fully for specific validation requirements before using this system property.
Locale for dependent request justification created by server of a bulk request.	OIM.RequestJustificationLocale	en_US	The value of the property is a locale, the same locale will be used to translate request justification text for bulk requests. The format of locale is languageCode_CountryCode such as en_US, fr_FR. For details, refer Preparing to Install and Configure PRODUCT.
Notify other recipients with the password reset email if email of user is null	XL.NotifyPasswordGenerationToOther	TRUE	When the value of this property is TRUE, the email notification for reset password is sent to other recipients if the email ID of the user is not specified.
Number of records to be executed in a batch during Catalog Enrichment	XL.CatalogEnrichmentBatchSize	500	This property determines how many records must be processed in a batch by the catalog job during catalog enrichment.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Maximum number of records to be fetched from Catalog	Catalog.SearchResultCap	-1	This property determines how many records must be fetched from catalog when a search is performed. If the value is -1, then all records are fetched from catalog table. If the value is 10000, then only 10000 records are fetched from catalog. **Note**: It is recommended that you set the value to 10000 only if poor catalog search performance is experienced.
Max Result size for lookups	LOOKUP_MAX_RESULTSIZE	1000	This property determines how many records must be fetched from the lookup table when a search is performed. For example, if the value is set to 500, then only 500 records are fetched from the lookup table. If the value is set to 0, then there is no restriction on the number of records fetched from the lookup table.
Midtier compression for Audit(UPA) data	OIM.AuditCompression	0	This property is used to configure user profile audit data compression. It can have the following values: • **0**: This is the default value. It determines that none of the columns in the UPA table are compressed. • **1**: This value determines that the SNAPSHOT column in the UPA table is compressed. • **3**: This value determines that the SNAPSHOT and DELTAS columns in the UPA table are compressed.
Midtier compression for Audit(UPA) data algo	OIM.AuditCompressionAlgo	GZIP	This property determines that GZIP is used as the compression algorithm. Only GZIP is supported in this release.
OIA integration status	OIM.IsOIAIntegrationEnabled	FALSE	Specifies whether OIA is integrated with Oracle Identity Manager. Set the value of this property to `TRUE` before you add role memberships in Oracle Identity Manager. If you set the value of this property to `FALSE`, incremental role memberships into OIA will not work. **Note:** You must do a full import of role memberships at least once after this property is enabled.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
OIM Complex Password Policy compatible with Active Directory	OIM.ADPasswordPolicyCompatibilityEnabled	FALSE	On setting the value of this property to TRUE, the last rule (inclusion of user ID, first name, or last name in password) of the OIG complex password policy is replaced with the Active Directory (AD) password policy (inclusion of Display Name and User Login in password). This property is applicable to all complex password policies. **Note:** This system property is available only after you apply Oracle Identity Governance Bundle Patch 12.2.1.4.200624.
OIM No Password Propagation Support	NO_PASSWORD_PROPAGATION_SUPPORT	FALSE	This property determines if the No Password Propagation Support is enabled in Oracle Identity Governance. If this property is set to true, then the access policy based password provisioning is disabled. It is recommended not to change this property value directly as it changes the Oracle Identity Governance login behavior.
Old Password Validator	OIM.OldPasswordValidator	oracle.iam.identity.usermgmt.impl.ContainerLoginPasswordVerifier	The property specifies the name of the plugin class to be used for verifying old passwords.
OMSS Enabled	OMSS Enabled	false	When the value of this property is true, OMSS integration is enabled, and the OMSS links and tabs are displayed in Oracle Identity Self Service. **Note:** After modifying the value of this system property, you must restart Oracle Identity Manager server for the changes to take effect.
Period to Delay User Delete	XL.UserDeleteDelayPeriod	0	This property is used to specify the time period before deleting a user. When this property is set and a user is deleted, the user's state is changed to disabled and "automatically delete on date" is set to current date plus the delay period. If this property is not set, then the user is automatically deleted at the expiration of the end date by the Disable/Delete User After End Date scheduled job.
Proxy User Email Notification	XL.ProxyNotificationTemplate	Notify Proxy User	The corresponding PTY_VALUE is the e-mail definition name that is sent when a proxy user is created. User gets a notification e-mail when the user is made the proxy for some other user.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
ProxyDelegateEnabled	ProxyDelegateEnabled	FALSE	This property allows to manage proxy assignment type. When you set the value of this property to TRUE and the user is assigned with proxy, then the request is assigned to both the user and proxy. When you set the value of this property to FALSE and the user is assigned with proxy, then the request is assigned to only proxy and not to user.
Recon Batch Size	OIM.ReconBatchSize	500	This property is used to specify the batch size for reconciliation. You can specify 0 as the value for this to indicate that the reconciliation will not be performed in batches. **Note:** You must restart Oracle Identity Manager server after setting this property.
Request Notification Level	RequestNotificationLevel	0	This property indicates whether or not notification is sent to the requester and beneficiary when a request is created or the request status is changed. This property can have the following values: • **0:** The notification feature is disabled. • **1:** Notifications are sent for every change in request status. • **2:** Notifications are sent for request creation and change of status to any of the Request End statuses. Request End statuses include Request Failed and other failure related statuses, Request Completed, Request Withdrawn, and Request Closed. • **3:** Email notifications are sent only on request completion. For request notification level 2, notifications are sent for request creation and change of status to any of the Request End statuses. Request End statuses include Request Failed and other failure related statuses, Request Completed, Request Withdrawn, and Request Closed.
Retry Count for recon event	Recon.RetryCount	5	This property determines the reconciliation retry count. The retry count value is picked up from the value of this property. If you specify a value that is greater than 0, then auto retry is configured. If you specify 0 as the value of this property, then auto retry is not configured.
Reset Password	SSO.RESETPASSWORDONTARGETBYPASSINGCONNECTOR	False	Set this value to true and import the Active Directory (AD) certificate into Oracle Identity Governance (OIG) to improve the performance of Reset Password in AD integration. This system property is available only after you apply Oracle Identity Governance Bundle Patch 12.2.1.4.210708. **Note:** For details, see Improving Reset Password Performance on AD Integration in *Integration Guide for Oracle Identity Management Suite*.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Search Stop Count	XL.IDADMIN_STOP_COUNT	300	This property determines the maximum number of records that are displayed in the advanced search result. If the search criteria specified returns more number of records than that value of this property, then the number of records displayed is limited to this value. In addition, a warning is displayed stating that the results exceed maximum counts and you must refine your search with additional attributes.
Segregation of Duties (SOD) Check Required	XL.SoDCheckRequired	FALSE	This property indicates whether or not Segregation of Duties (SoD) check is required.
Send email notification based on user locale	XL.SendEmailNotificationBasedOnUserLocale	false	This property determines whether an email notification is sent based on the receiver's (user/manager/assignee/requestor) locale when the value is set to true. If the value is set to false, then notification is sent in the server locale. **Note:** This system property has been deprecated in this release of Oracle Identity Manager.
Should send notifications in recon or not	Recon.SEND_NOTIFICATION	true	Determines if notification is sent to the user when the user login and password are generated in postprocess event handler for user creation via trusted source reconciliation. If the value is set to true, then notification is sent when user login and password are generated in postprocess event handler for user creation via trusted source reconciliation. If the value is set to false, then notification is not sent when user login and password are generated in postprocess event handler for user creation via trusted source reconciliation.
Shows Revoked Accounts In the Accounts Tab	ShowRevokedAccountsInAccountsTab	TRUE	By default, the revoked accounts always appear in the Accounts tab. To hide the revoked accounts, this feature should be updated to "FALSE".
Shows tasks assigned to group users with highest priority or least load only	XL.ShowTaskAssignedToGroupUserOnly	FALSE	If the value is TRUE, then the tasks are assigned to group users with highest priority or least load only when the assignment type is Group User With Least Load.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Specifies the LDAP container mapper plug-in to be used	LDAPContainerMapperPlugin	oracle.iam.ldapsync.impl.DefaultLDAPContainerMapper	When Oracle Identity Manager is installed with LDAP synchronization enabled, this plug-in determines in which container users and roles are to be created. Value of this system property indicates the default Oracle Identity Manager plug-in name used for computing the container values. If the default plug-in does not meet the requirement, then you can define your own plug-in to determine the container and specify the name of the plug-in in this system property.
URL for challenge questions modification	OIM.ChallengeQuestionsModificationURL	NONE	When a user is locked, an automatic unlock occurs after a prescribed time period. This property defines that time period in seconds. Therefore, for example, if a user account is locked and the value of this property is 86400 seconds (one day), then the account is automatically unlocked after one day. The value of this property is the URL within OAAM that handles the challenge questions. For example: http://*OAAM_HOST*:*OAAM_PORT*/*OAAM_SERVER*/userPreferences.do?showView=registerQuestions
URL for change password	OIM.ChangePasswordURL	NONE	This property is used in combination with the property OIM.DisableChallengeQuestions. The value of this property is the URL within OAAM that handles the change password functionality. For example: http://*OAAM_HOST*:*OAAM_PORT*/*OAAM_SERVER*/userPreferences.do?showView=changePassword
User Attribute Reservation Enabled	XL.IsUsrAttribReservEnabled	TRUE	This property is used to enable user attribute reservation.
User Id reuse property. Requires dropping the index present on USR_LOGIN column	XL.UserIDReuse	FALSE	Determines whether a deleted user account can be reused. To reuse a deleted user account, assign this property a value of TRUE and drop the unique index for the USR_LOGIN column in the USR table and create a nonunique index. To prevent a user account from being reused, assign this property a value of FALSE. **Note:** It is imperative to de-provision all accounts associated with a deleted user, because if you create a new user with the same user name as that of the deleted user by setting the `XL.UserIDReuse` property to `true`, then the new user might get access to offline accounts of the deleted user that was not deleted as part of the de-provisioning process.
User Language	user.language	en	The user.language value is configured during installation for Locale handling at server side.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
User profile audit data collection level	XL.UserProfileAuditDataCollection	Resource Form	This property controls the user profile data that is collected for audit purpose when an operation is performed on the user, such as creation, modification, or deletion of a user, role grants or revokes, and resource provisioning or deprovisioning. Depending upon the property value, such as Resource Form or None, the data is populated in the UPA table. The audit levels are specified as values of this property. The supported levels are: • **Process Task:** Audits the entire user profile snapshot together with the resource lifecycle process. • **Resource Form:** Audits user record, role membership, resource provisioned, and any form data associated to the resource. • **Resource:** Audits the user record, role membership, and resource provisioning. • **Membership:** Only audits the user record and role membership. • **Core:** Only audits the user record. • **None:** No audit is stored.
User Region	user.region	US	The user.region value is configured during installation for Locale handling at server side.
Whether or not email should be validated for uniqueness	OIM.EmailUniqueCheck	TRUE	This property is available in a deployment that has been upgraded from an earlier release of Oracle Identity Manager. If the value of this property is FALSE, then Email Uniqueness check is not performed by Oracle Identity Manager. If the value if TRUE, then Email Uniqueness check is performed by Oracle Identity Manager. **Note:** If this property is not present, then Email Uniqueness check is performed by Oracle Identity Manager.
Width of JGRAPH CELL	XL.GTCNexawebUIColumnWidth	155	This property controls the field length of GTC mapping attributes. Default value is 155, Maximum value is upto 255.
Workflows Enabled	Workflows Enabled	TRUE	This property determines whether SOA server is turned on or turned off. If the value of this property is TRUE, then SOA sever is turned on. If the value of this property is FALSE, then SOA server is turned off. **Note:** After setting the value of this system property, you must restart Oracle Identity Manager. **Note:** Toggling between enabling and disabling workflows is not supported.

Table 23-1 (Cont.) Default System Properties in Oracle Identity Governance

Property Name	Keyword	Default Value	Description
Workflow Policies Enabled	Workflow Policies Enabled	TRUE	This property determines whether approval workflows is enabled or disabled in Oracle Identity Manager. Approval workflows is used to determine if operation requires approval or not, and if approval is required, then which workflow is to be invoked. If the value of this property is TRUE, then approval workflow is enabled. If the value of this property is FALSE, then approval workflow is disabled. For detailed information about approval workflow, see Managing Workflows.
XL.AlternativeReviewerIDForManager	XL.AlternativeReviewerIDForManager	xelsysadm	This property provides an alternative certification reviewer for users who do not have a manager or whose manager is disabled. If this property is set to NULL, or if the specified alternative reviewer is disabled or does not exist, then a warning message is logged and these users are omitted from user certifications-by-manager.
OIG.DefaultTaskReassignee	OIG.DefaultTaskReassignee	SYSTEM ADMINISTRATORS	This property defines the default task reassignee to reassign tasks to other assignees when the current assignee is disabled or deleted. By default, the value of the OIG.DefaultTaskReassignee system property is the SYSTEM ADMINISTRATORS role so that pending tasks can be reassigned to the SYSTEM ADMINISTRATORS role when a user is disabled or deleted. When the value of the OIG.DefaultTaskReassignee system property is a manager, Oracle Identity Governance finds the closest active manager from the hierarchy if the current target assignee is disabled. When the value of the OIG.DefaultTaskReassignee system property is a user, Oracle Identity Governance reassigns the task to the user. When the value of the OIG.DefaultTaskReassignee system property is a role, Oracle Identity Governance reassigns the task to the role. Here, the role name as the value of the OIG.DefaultTaskReassignee system property is case-sensitive. If Oracle Identity Governance cannot find any valid assignee, then the tasks are reassigned to the System Administrator. It is important to set the value of this property with an active user or role. For example: OIG.DefaultTaskReassignee=Manager OIG.DefaultTaskReassignee=User:user1 OIG.DefaultTaskReassignee=Role:role1
OIG.BeneficiaryManagerApprovalWorkflows	OIG.BeneficiaryManagerApprovalWorkflows	default/BeneficiaryManagerApproval!4.0	When the initial target assignee is disabled, Oracle Identity Governance looks for the closest manager of the beneficiary of the request with the approval workflow specified in this system property. You can specify multiple composites with the comma separator.
OIG.RequesterManagerApprovalWorkflows	OIG.RequesterManagerApprovalWorkflows	default/RequesterManagerApproval!4.0	When the initial target assignee is disabled, Oracle Identity Governance looks for the closest manager of the requester of the request with the approval workflow specified in this system property. You can specify multiple composites with the comma separator.

23.2.2 Non-Default System Properties in Oracle Identity Governance

Oracle Identity Manager provides a set of system properties that are not present in the PTY table by default.

You can add these non-default system properties to the PTY table by using the Identity System Administration, and then use the properties to change some of the default settings in Oracle Identity Manager. For example, if you want to configure the number of times Oracle Identity Manager retries to get a connection when the JDBC connection fails, then you can configure the JDBC Connection Retry Attempts system property.

> **See Also:**
>
> Overview of Generic Technology Connectors in *Developing and Customizing Applications for Oracle Identity Governance* for more information about GTC

Non-Default System Properties in Oracle Identity Governance lists and describes Non-Default system properties which you can add to the PTY table

Table 23-2 Non-Default System Properties

Property Name	Description	Keyword	Sample Value
OIM Database Query Retry Attempts	Number of times SQL queries to be retried for handling Oracle RAC failures. In the absence of this property in the PTY table, SQL queries for handling Oracle RAC failures are retried three times by default.	OIM.DBQueryRetryAttempts	5
OIM Database Query Retry Interval	Time in seconds after which each SQL retry takes place for Oracle RAC failures. In the absence of the property in the PTY table, SQL query occurs after every 7 seconds by default.	OIM.DBQueryRetryInterval	10 seconds
OIM Paging Limit	Default paging limit for search operations on user entity.	OIM.PagingLimit	300
JDBC Connection Retry Attempts	Number of times Oracle Identity Manager retries to get a connection when the JDBC connection fails. In the absence of this property in the PTY table, the JDBC connection is retried three times by default.	OIM.JDBCConnectionRetryAttempts	5 When the value is 0, it means no retry.

Table 23-2 (Cont.) Non-Default System Properties

Property Name	Description	Keyword	Sample Value
JDBC Connection Retry Interval	Time in seconds between each JDBC connection retry. In the absence of this property in the PTY table, each JDBC connection retry occurs at an interval of 7 seconds.	OIM.JDBCConnectionRetryInterval	10 seconds
Allowed Back URLs	This property is required if you want to setup any non-OIM/OAM URLs to be a valid backURL on the Track Self Registration Request page. Oracle Identity Manager validates the back URLs and redirect URLs against a list of URLs provided by this system property. The value of this property is a comma-separated list of URLs that Oracle Identity Manager allows for redirection.	XL.AllowedBackURLs	http://*OIM_HOST*:*OIM_PORT*/
Allowed Back URLs Mode	This system property determines the mode in which the XL.AllowedBackURLs system property works. It has the following possible values: • **Enforce:** Ensure that the current URL is present in the white list specified as the value of XL.AllowedBackURLs. If not present, then change the back URL to the default URL, which is the sign-in page. • **Disable:** Log all the white list validations. The default value is `Enforce`.	XL.AllowedBackURLsMode	Enforce

Table 23-2 (Cont.) Non-Default System Properties

Property Name	Description	Keyword	Sample Value
XL.AllowedOrigins	Allows users to set the whitelist for the CORS filter.	XL.AllowedOrigins	Apply the following guidelines for specifying the value: • The URLs can be comma separated, for example http://www.example.com:14001 and https://www.test.com:14003. • The URL can contain simple wildcard matching (for example http://*.example.com:14000, http://*.com:14001) with only a single '*' character. '*.example.*.com' will not work correctly. • The pattern matching is very simple and only pertains to the domain part of the URL. No matching on scheme or port is supported (*://example.com:14001 or http://example.com:*). • Only http and https schemes are supported. • The matching goes from right to left. • The '*' will only match the text of domain after the period and before the next period. Patterns such as '*ampl.com' and '*.*partial*.c*' are not supported. • A single '*' will match anything and should be used for test/development only.

23.3 Managing System Properties

Managing system properties involve modifying system properties by using Identity System Administration, and purging the cache.

This section contains the following topics:

- Searching for System Properties
- Adding System Properties
- Editing System Properties
- Deleting System Properties
- Purging Cache

23.3.1 Searching for System Properties

Use **Configuration Properties** section in the **Manage** tab to search the system properties.

To search for a system property, perform the following steps:

1. Login to Oracle Identity Self Service.
2. Select **Manage** tab.
3. In the **System Configuration** box, click **Configuration Properties**.
   The **Manage Configuration Properties** page is displayed.
4. In the **Manage Configuration Properties** page, enter the name of the property you want to search in the **Name** option.
5. Click **Search**.
   The search results displays the details of the System Properties.

23.3.2 Adding System Properties

To add a system property, perform the following steps:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab.
3. Navigate to **System Configuration** box, click **Configuration Properties**.

   The **Manage Configuration Properties** section is displayed.
4. In the **Manage Configuration Properties** section, select **Add Property**.

   The **Add a new Configuration Property** page appears.
5. Provide values for the following fields:
   - Name
   - Keyword
   - Value
6. Click **Save**.

23.3.3 Editing System Properties

The Edit option allows you to modify an existing system property by using the System Property Details page. If any system property is tagged with a set of allowed values, then you must specify a value from that set only.

You cannot modify the Property Name and Keyword fields of a system property created in a non-English locale. As a workaround, delete the existing system property and create a new one with the desired values.

In an English locale, non-ASCII characters are allowed in a system property name. When you modify the name of a system property to include non-ASCII characters, you must ensure the following if you want the changes to be translated into other languages:

To edit a System Property:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab.
3. Navigate to **System Configuration** box, click **Configuration Properties**.

   The **Manage Configuration Properties** section is displayed.

4. In the **Manage System Properties** section, search for the system property that you want to modify.
5. In the search results table, click **Edit** button for the system property that you want to modify.

   The **Edit Configuration Property** page is displayed.
6. Modify the values in the fields. Generally, you need to modify the Value field to change the functionality that the system property provides.
7. Click **Save** to save the changes made.

   A message confirming that the system property has been modified is displayed.

23.3.4 Deleting System Properties

The Delete option allows you to delete an existing system property by using the **System Property Details** page.

To delete a System Property, perform the following:

> **Note:**
>
> The delete option is not available for default system out-of-box properties.

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab.
3. Navigate to **System Configuration** box, click **Configuration Properties**.

   The **Manage Configuration Properties** section is displayed.
4. In the **Manage System Properties** section, search for the system property that you want to delete.
5. In the search results table, click **Delete** button for the system property that you want to delete.

   A message confirming that the system property has been deleted is displayed.

23.3.5 Purging Cache

Whenever you make any change to a system property by using any method other than from the Identity System Administration, you must run purge cache utility to fetch the changes that are reflected in Oracle Identity Manager.

To clear the server cache:

1. Depending on the operating system being used, navigate to the following directory:
   - For Microsoft Windows:

     OIM_HOME\server\bin\
   - For UNIX:

     OIM_HOME/server/bin/
2. Run one of the following commands:

- For Microsoft Windows:

  ```
  PurgeCache.bat CATEGORY_NAME
  ```

- For UNIX:

  ```
  sh PurgeCache.sh CATEGORY_NAME
  ```

The *CATEGORY_NAME* name argument represents the Oracle Identity Manager category name that is to be purged, for example, FormDefinition.

To purge all the categories, pass a value of "All" to the PurgeCache utility. It is recommended to clear all the categories.

```
sh PurgeCache.sh All
```

Note:

- If Oracle Identity Governance is installed on IPv6 Linux host computer, then pass `ipv6` as the last input argument to the PurgeCache.sh script, as shown:

  ```
  sh PurgeCache.sh All ipv6
  ```

  On Windows environment, do not pass any parameter for IPv6 while running PurgeCache.bat.

- When you run the PurgeCache.sh utility in an IPv6 enabled setup, the following error is encountered:

  ```
  Exception in thread "main"
  javax.security.auth.login.LoginException:
  java.net.UnknownHostException: exampledomain.com: Name or
  service not known
  ```

  To workaround this issue:

  a. Open the PurgeCache.sh script in a text editor.

  b. Modify the following line:

     ```
     bash oimClientWrapper.sh $CLIENT_CLASS $1
     ```

     To:

     ```
     bash oimClientWrapper.sh $CLIENT_CLASS $*
     ```

  c. Save the file.

24

Managing Notifications Template Services

Managing notification involves understanding the notification service, managing notification providers and notification templates, disabling notification, and troubleshooting notification issues.

This content applies only to OIG Bundle Patch 12.2.1.4.230408 Bundle Patch and later releases.

Topics:

- About Notification Providers
- Default Notification Template
- Managing Notification Templates

24.1 About Notification Providers

Information about events occurring in Oracle Identity Manager is required to be sent to various users, such as requesters, beneficiaries, or administrators. This information about events is sent by using the notification service in the form of notification e-mail messages. The notification service allows you to perform all notification-related operations.

An event is an operation that occurs in Oracle Identity Manager, such as user creation, request initiation, or any custom event created by the user. The events are generated as part of business operations or via generation of errors. Event definition is the metadata that describes the event. To define metadata for events, it is important to identify all event types supported by a functional component. For example, as a part of the scheduler component, metadata can be defined for scheduled job execution failed and shutting down of the scheduler. Every time a job fails or the scheduler is shut down, the events are raised and notifications associated with that event are sent.

The data available in the event is used to create the content of the notification. The different parameters defined for an event help the system to select the appropriate notification template. The different parameters that are defined for an event help the system decide which event variables can be made available at template design time.

A notification template is used to send notifications. These templates contain variables that refer to available data to provide more context to the notifications. The channel through which a notification is sent is known as the notification provider. Examples of such channels are e-mail, Instant Messaging (IM), Short Message Service (SMS), and voice. To use these notification providers, Oracle Identity Manager uses Oracle User Messaging Service (UMS).

At the backend, the notification engine is responsible for generating the notification, and utilizing the notification provider to send the notification.

24.2 Default Notification Template

Default notification templates are available for various notification scenarios, such as for bulk requests, proxies, password generation, warning, expiry, and reset, and request creation and status change.

Oracle Identity Manager provides a set of default notification templates, as shown in Table 24-1.

Table 24-1 Default Notification Templates

Notification Template	Description
Add Proxy Notification	Template to send notification after a proxy has been added for a user.
Bulk Request Creation	Template to send notification during a bulk request creation.
Create User Self Service Notification	Template to send notification after a new user is created.
End Date	Template to send notification to the manager when end date of the reportee expires.
Forgotten Username Notification	Template to send notification after user submits the Forgotten Username form.
Generated Password Notification	Template to send notification after a password is generated by Oracle Identity Manager.
Password Expired Notification	Template to send notification after password has expired.
Password Warning Notification	Template to send notification before password expires.
Request Creation	Template to send notification during a request creation.
Request Identity Creation	Template to send notification during a Create User request.
Request Status Change	Template to send notification during a request status change.
Reset Password	Template to send notification after password has been reset.
User Deleted	Template to send notification to the manager when the user account of the reportee is deleted as a result of expired end date.

24.3 Managing Notification Templates

A notification template, which contains variables that refer to available data to provide more contexts to the notifications, is used to send notifications. Managing notification templates include searching, creating, modifying, enabling and disabling, and deleting notification templates, adding and removing locales to and from notification templates, and configuring notification for a proxy.

This section describes about notification templates in the following topics:

- Searching for a Notification Template
- Adding a Template
- Modifying a Notification Template

- Enabling or Disabling a Notification Template
- Deleting Notification Templates

24.3.1 Searching for a Notification Template

You can perform a notification template search specific for a event name or search based on the locale specific template.

This section contains the following topics:

- Performing Template Name Search for a Notification
- Performing Locale Specific Notification Template Search

24.3.1.1 Performing Template Name Search for a Notification

To perform a template name search for a notification template, follow the below provided steps:

1. Login to Identity Self Service.
2. Click the **Manage** tab, and then click **System Configuration**.
3. Select **Notification** from the drop-down.

   The **Manage Notification Templates** page is displayed.
4. In the **Templates** tab, enter either one of the following details:

   > **Note:**
   >
   > If multiple criteria is selected, then the search results are based on the OR condition.

   - Template: Enter the name of the template name to perform search.
   - Event: Select the event name from the default template drop-down list.
5. Click **Search**.

   The search results are displayed in a tabular format.

24.3.1.2 Performing Locale Specific Notification Template Search

You can perform search locale specific template attributes using the **Locale Specific Templates** tab.

To perform a locale specific search for a notification template:

1. Log in to Identity Self Service.
2. Click the **Manage** tab, and then click **System Configuration**.
3. Select **Notification** from the drop-down.
   The **Manage Notification Templates** page is displayed.
4. In the **Locale Specific Templates** tab, enter either one of the following details:

> **Note:**
>
> If multiple criteria is selected, then the search results are based on the OR condition.

- Template: Enter the name of the template.
- Event: Select one of the available events from the drop-down list.
- Subject: Enter the subject for the locale.
- Locale: Select the type of locale from the drop-down list for the search.

5. Click **Search**.
   The search details are displayed in a tabular format.

24.3.2 Adding a Template

Use the **Manage Notification Templates** page to add a new notification template by specifying various attributes, such as template name and description, event details, and locale information.

To create a notification template:

> **Note:**
>
> Corresponding to each event that happens, you have to configure an XML file. The XML file defines the behavior of each event. You must first configure the XML for an event. After this is done, you can create a notification template for that event. For information about creating the event XML file, see Defining Event Metadata for Oracle Identity Governance.

1. Log in to Identity Self Service.
2. Click the **Manage** tab, and then click **System Configuration**.
3. Select **Notification** from the drop-down.
4. Click **Add Template**.
5. Enter values for the following fields:
   - Name: Enter the template name.
   - Description: Enter a brief description of the template.
   - Event: Select the type of event for the template from the available drop-down list.

   Under the **Locale Information** section, enter values in the following fields:
   - Locale: Chose the locale from the list.
   - Encoding: To specify a form of encoding.

> **Note:**
>
> The encoding values displayed varies depending on the type of locale you have selected.

- Message Subject: Enter a subject for the notification.
- Type: Select the data type in which you want to send the message. You can choose between HTML and Text/Plain.
- Short Message: Enter a short version of the message.
- Long Message: Enter a detailed version of the message.

6. Click **Save**.

   A message is displayed confirming the creation of the notification template.

24.3.3 Modifying a Notification Template

To modify the attributes of a notification template, perform the following:

1. Log in to Oracle Identity Self Service.
2. Click **Manage** tab and select **System Configuration** box.
3. Select **Notification** from the drop-down.
4. Search for the notification template that you want to modify.

   The following types of search is available:

   - Search by the template name.
   - Search by the locale specific template.
5. Select **Edit** icon in the Action column for the locale that you want to modify.
6. Modify the values that you want to and click **Save.**
7. A message is displayed confirming the modification of the notification template.

24.3.4 Enabling or Disabling a Notification Template

Use the **Notification** option in the Self Service section, to enable or disable a notification template.

You can enable or disable a notification template in the following ways:

1. Log in to Oracle Identity Self Service.
2. Click **Manage** tab and select **System Configuration** box.
3. Select **Notification** from the drop-down.
4. Search for the notification template that you want to enable or disable.

   The search results are displayed in a tabular format.
5. Select the template that you want to enable or disable.
6. Click **Enable** or **Disable** in the **Action** column.

   A message is displayed prompting you to confirm the enable or disable operation.

7. Click **Yes**.

   A message is displayed confirming the enable or disable operation.

Alternatively, you can enable or disable a notification template by following:

1. Log in to Oracle Identity Self Service.
2. Click **Manage** tab and select **System Configuration**.
3. Select **Notification** from the drop-down.
4. Search for the notification template that you want to disable.
5. From the search results, select the notification template.
6. From the **Action** drop-down option in the top right corner, click **Enable** or **Disable**. A message is displayed confirming the enable or disable operation.

24.3.5 Deleting Notification Templates

The Delete option in the **Manage Notification Templates** section allows you to delete notification template and to delete only the locales that are specific to the notification template.

The following topic are described in this section:

- Deleting a Notification Template
- Deleting a Locale Specific Notification Template

24.3.5.1 Deleting a Notification Template

The **Templates** tab allows you to delete one or more notification templates.

> **Note:**
>
> You cannot delete out-of-the-box templates that are pre-configured.

To delete a notification template, perform the following:

1. Login to Oracle Identity Self Service.
2. Click **Manage** tab and select **System Configuration** box.
3. Select **Notification** from the drop-down.
4. Select **Templates** tab.
5. Search for the specific template to be deleted.
6. Select the template that you want to delete, click **Delete** in the **Action** column.

   A message is displayed prompting you to confirm the delete operation.
7. Click **Yes**.

   A message is displayed confirming the delete operation.

24.3.5.2 Deleting a Locale Specific Notification Template

The **Locale Specific Templates** tab allows you to delete a template specific to a locale.

> **Note:**
>
> You cannot delete the last remaining locale of a template.

To delete a locale specific notification template, perform the following:

1. Login to Oracle Identity Self Service.
2. Click **Manage** tab and select **System Configuration** box.
3. Select **Notification** from the drop-down.
4. Select **Locale Specific Templates** tab.
5. Click **Delete** in the Action column to delete the locale of a specific template.

   Alternatively, to delete the locale for one specific template:

   - Click the **Edit** button for the locale template, and click **Delete** in the Action column.

   A message is displayed prompting you to confirm the delete operation.
6. Click **Yes**.

   A message is displayed confirming the delete operation.

Part V
Reporting

Running reports include running identity audit policy violation reports and other reports.

This part describes how to run Oracle Identity Manager Reports.

It contains the following chapter:

- Running Reports

25
Running Reports

You can use the reporting feature of Oracle Identity Manager to create various types of reports in multiple formats.
For detailed information about Oracle Identity Manager Reports, see Using Reporting Features in *Administering Oracle Identity Governance*.

This chapter describes how to run reports in Oracle Identity Manager. It contains the following sections:

- Running Oracle Identity Governance Reports
- Running Policy Violation Reports

25.1 Running Oracle Identity Governance Reports

You can run Oracle Identity Governance reports by specifying input parameters for the report in Oracle BI Publisher.

To run a report:

1. Login to BI Publisher by using your Oracle Identity Governance system administrator credentials by navigating to the following URL:

   http://*HOST_NAME*:*PORT*/xmlpserver

   The default port for BI Publisher server is 9704.
2. Expand **Shared Folders**.
3. Expand **Oracle Identity Manager Reports** to display the reports classified according to their functional areas.
4. To view a report:
   a. In the left menu, select the report functional area, for example, Access Policy Reports.
   b. On the right side page, under the desired report, for example Access Policy Details, click **Open**.

   The Report Input Parameters page is displayed. This page displays the input parameters that must be provided to run a report. The report input parameters act as a filter criterion.

   In some cases, at least one or more parameter fields are required fields. Some reports do not require any input parameter. If this is not the case, then you must populate at least one of the fields to run a report.

> **Note:**
>
> If you leave the input parameter field blank, and then click **Apply**, then all the information associated with the report is displayed.

5. Enter the information required to identify what information the report contains.
6. Click **Apply** to run the report.

   The report is displayed.

25.2 Running Policy Violation Reports

Generating identity audit reports involves specifying the report type, report category, and report format.

For information about running identity audit policy violation reports, see Generating Identity Audit Policy Violation Reports.

Part VI
Appendix

Supplementary information for self service users includes personalization features of the Oracle Identity Self Service and list of functional capabilities of the Admin role and self capabilities.

Part VI contains the following chapters:

- Personalizing Self Service
- Functional Capabilities
- Sample Application Template XML

A
Personalizing Self Service

This chapter describes the personalization features of the Oracle Identity Self Service. It contains the following sections:

- Performing Search in Self Service
- Adding and Removing Attributes in Advanced Search Criteria
- Personalizing the Search Result
- Using Saved Search
- Sorting Data in Search Results
- Using Query By Example

> **Note:**
>
> Personalization of the Self Service is allowed for all users, and is applicable on a per user basis. In other words, the personalization that is saved for a user, is not applicable when another user logs in to Identity Self Service.

A.1 Performing Search in Self Service

Identity Self Service allows you to search for records in various pages, such as the Users page or the Roles page. There are two options available, Basic Search and Advanced Search.

To perform search, navigate to a page in Self Service with search option, such as the Users page or the Roles page. For example, following two searches can be performed in the Roles page:

- Performing Basic Search in Self Service
- Performing Advanced Search in Self Service

A.1.1 Performing Basic Search in Self Service

To open the Roles page and perform search, do the following:

1. In Identity Self Service, click the **Manage** tab, click **Roles**. The Roles Search page is displayed.
2. From the **Search** list, select an attribute based on which you want to search the role. The attributes in the drop-down are:
   - Display Name
   - Name

- Role Category
- Role Namespace

3. In the Search box, enter a value for the selected attribute, and click the Search icon. The search result is displayed.

   If you do not specify any value, all the default roles are listed. The asterisk (*) character is used as a wildcard character.

A.1.2 Performing Advanced Search in Self Service

To perform advanced search:

1. In Identity Self Service, click the **Manage** tab, click **Roles**. The Roles Search page is displayed.
2. Click **Advance** link. Advance Roles search page is displayed.
3. Select any one of the **Match** options:
   - **All:** On selecting this option, the search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.
   - **Any:** On selecting this option, the search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.
4. In the searchable user attribute fields, such as Display Name, specify a value. You can include wildcard characters (*) in the attribute value.

   For some attributes, select the attribute value from the lookup. For example, to search all roles in the Default role category, select Default in the Role Category field.
5. For each attribute value that you specify, select a search operator from the list. The following search operators are available:
   - Starts with
   - Ends with
   - Equals
   - Does not equal
   - Contains
   - Does not contain

   The search operator can be combined with wildcard characters to specify a search condition. The asterisk (*) character is used as a wildcard character. For example, you can specify the value of the Display Name attribute to be Jo* as the search criteria, and select Equals as the search operator. The roles with Display Name that begins with Jo are displayed.
6. To add a searchable role attribute to the Search Roles page, click **Add Fields**, and select the attribute from the list of attributes.

   For example, if you want to search all roles in a role namespace, then you can add the Role Namespace attribute as a searchable field and specify a search condition.

> **Note:**
>
> You can configure the attributes that are searchable. The attributes available for search must be a subset of the attributes defined for the role entity that are marked with the Searchable = Yes property.

7. Optionally click **Reset** to reset the values that you specified as search conditions. Typically, you perform this step to remove the specified search conditions and specify a new search condition.
8. Click **Search**. The search results is displayed in a tabular format, as shown in Figure:
9. If you want to hide columns in the search results table, then perform the following steps:
   a. Click **View** on the toolbar, select **Columns**, **Manage Columns**. The Manage Columns dialog box is displayed.
   b. From the **Visible Columns** list, select the columns that you want to hide.
   c. You can view the details of the role click the left arrow icon to add the columns in the **Hidden Columns** list.
   d. Click **OK**. The selected columns are not displayed in the search results. A status message displays along the bottom of the search table to identify how many columns are currently hidden. Figure shows that two columns are hidden.

A.2 Adding and Removing Attributes in Advanced Search Criteria

Default attributes are available in the advance search pages based on which you can perform the search. In addition to the default search attributes, you can add search attributes based on which you can perform the search.

Identity Self Service allows you to perform advanced search for records in various pages, such as the Users page or the Roles page. To add attributes to advanced search criteria:

1. Navigate to a page in Identity Self Service with advanced search option, such as the Users page or the Roles page. Click **Advance**.
2. Click **Add Fields**. The list of attributes that you can add to the search criteria is displayed.
3. Select an attribute from the list, for example, Role Description. The selected attribute is added to the Search section.

Note that a cross icon is displayed with the attribute that you added in the Search section. To remove the attribute from the search criteria, click the cross icon.

A.3 Personalizing the Search Result

You can personalize the search result to display or hide search attributes that are displayed as columns in the search results table. You can also change the order in which the columns are displayed in the search results table.

To personalize the search result:

1. To show or hide columns in the search results table:

a. On the toolbar of the search results page, click **View**, and then select **Columns**. A list of column names for the search results table are displayed. The column names that are already displayed in the search results table have a check mark.

b. Select or deselect column names to show or hide respectively in the search results table.

   Alternatively, select **Manage Columns** to display the Manage Columns dialog box. In this dialog box, you can move the column names in the **Hidden Columns** and **Visible Columns** lists to show or hide the columns respectively. When finished, click **OK**.

2. To change the order or the columns in the search results table:

   a. On the toolbar of the search results page, click **View**, and then select **Reorder Columns**. The Reorder Columns dialog box is displayed.

      Alternatively, click **View** and select the columns. Then, select **Manage Columns** to display the Manage Columns dialog box.

   b. In the **Visible Columns** list, move the column names up or down by using the arrow keys to the right of the list. The columns will be displayed in the order that you specify here.

   c. Click **OK**.

3. To detach the search result table from the page, from the **View** menu, select **Detach.** Alternatively, click **Detach** on the toolbar.

   To close the detached search result, click the cross icon at the top right corner or click **Detach** on the toolbar.

4. To browse through the search result pages, use the navigation panel at the bottom of the search result table.

   To jump to a particular page, enter the page number in the **Page** box and press enter. Alternatively you can use the navigational arrows to move to the First page, Previous page, or Next page.

A.4 Using Saved Search

Instead of specifying the search criteria every time you search for similar records, you can save a search and use the saved search to search for the records.

To search for entities, such as users or roles, you specify a search criteria. The search criteria includes search attributes that you have added and other search conditions. This section contains the following topics:

- Creating a Saved Search
- Personalizing Saved Search
- Deleting a Saved Search
- Using Saved Search to Perform a Search Operation

A.4.1 Creating a Saved Search

To save a search:

1. Perform a search by specifying search criteria.

2. Click **Save**. The Create Saved Search dialog box is displayed.
3. In the Name field, enter a name for the search.
4. Select one or more of the following options:
   - **Set as Default:** Selecting this option sets the saved search as the default search for the page whenever the search page is opened.
   - **Run Automatically:** Selecting this option runs the saved search when you open the page.
5. Click **OK.** The search is saved with the name you specified.

   The saved search name is displayed in the Saved Search list on the top right of the Search section. You can select the saved search to perform the search.

A.4.2 Personalizing Saved Search

To personalize saved search:

1. From the Save Search list, select **Personalize**. The Personalize Saved Searches dialog box is displayed.
2. From the Personalize Saved Searches list, select the saved search that you want to personalize.
3. In the Name field, edit the name of the saved search.
4. Select any one or more of the following options:
   - **Set as Default:** Selecting this option sets the saved search as the default search for the page whenever the search page is opened.
   - **Run Automatically:** Selecting this option runs the saved search when you open the page.
   - **Show in Search List:** Selecting this option displays the saved search in the Saved Search list.
5. Click **Apply**, and then click **OK**.

> **Note:**
>
> The default saved searches are view-only and cannot be used for personalization (modification or deletion).

A.4.3 Deleting a Saved Search

To delete a saved search:

1. From the Save Search list, select **Personalize**. The Personalize Saved Searches dialog box is displayed.
2. From the Personalize Saved Searches list, select the saved search that you want to delete.
3. Click **Delete**. A warning message is displayed.
4. Click **Yes** to confirm deletion.

5. Click **OK** to close the Personalize Saved Searches dialog box.

A.4.4 Using Saved Search to Perform a Search Operation

If you select the **Set as Default** option when creating the saved search, then the saved search is displayed in the Saved Search list when you open the page. To search for records by using the default saved search, click **Search**.

If you select the **Run Automatically** option when creating the saved search, then the search operation based on the saved search is performed automatically when you open the page.

If you have not selected the **Set as Default** and **Run Automatically** options, then to perform the search by using the saved search, select the saved search from the Saved Search list.

A.5 Sorting Data in Search Results

You can sort the data in the search results table in ascending or descending order.

When you place the mouse pointer on the column names in the search results table, up and down arrow keys are displayed. Clicking the up arrow key sorts the data in ascending order, and clicking he down arrow key sorts the data in descending order.

The sort is restored as a preference in the Self Service. As a result, when you logout, and login again and perform a search, sorted data is displayed in the search result. The sort preference works only for the logged in user. For other users, the search results table is displayed with default settings.

A.6 Using Query By Example

By using the Query By Example feature, you can refine the search results by providing additional filters. Oracle Identity Manager allows you to turn this feature on and off based on your requirement.

In many Self Service pages, data is displayed in a tabular format. Users can have hundreds of roles and resources, and thousands of entitlements provisioned to them. When you are looking at a large number of records, you need to scroll through multiple pages of results to find specific role, resources, and entitlements. When looking for a few records in a list of large number of records, you can use Query By Example to refine the search. To do so:

1. In the search results table, click **View** on the toolbar, and then select **Query By Example**. Text fields are displayed on top of each column of the search results table.
2. Enter a value in a text field for a column. For example, to refine the search for all users with Disabled status, enter Disabled on the text field above the Status column.

   Instead of entering the complete value, you can enter a few letters that match the values you are searching, such as `Di`. Users with Disabled status are displayed. If you enter D as the value, then all users with Disabled or Deleted are displayed (because both the Disabled and Deleted status begin with the letter "D").
3. Press **Enter**. All records that match the Query By Example value are displayed.

4. To disable Query By Example, click **View**, and then select **Query By Example.**

   Alternatively, click **Query By Example** on the search result toolbar.

B
Functional Capabilities

The authorization model provides flexibility to create a new Admin role and select the capabilities for these Admin roles. This is possible with the use of Admin role capabilities and self capabilities.
This appendix provides the list of Admin Role capabilities and the list of Self capabilities.

- List of Authorization Functional Capabilities
- List of Self Capabilities

B.1 List of Authorization Functional Capabilities

The Authorization Functional Capabilities list provides the different admin role capabilities that a new admin role can be assigned with.

This section provides the list of admin role capabilities in Table B-1.

Table B-1 Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
Admin Role	AdminRole - Create	Allows a User to create an Admin Role	Create Admin Role View or Search Admin Roles Assign Capabilities Assign Admin Role Members Set Organization Scope of Control Publish Admin Role to Organization
Admin Role	AdminRole - Modify	Allows a User to modify an Admin Role	Modify Admin Role Attributes View or Search Admin Roles Assign Capabilities Assign or Unassign Admin Role Members Set Organization Scope of Control Publish Admin Role to Organization
Admin Role	AdminRole - Delete	Allows a User to delete an Admin Role	Delete Admin Role View or Search Admin Roles

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
Admin Role	AdminRole - View/ Search	Allows a User to view and search for Admin Roles	View or Search Admin Roles View Capabilities View Admin Role Members View Organization Scope of Control View Organizations Published To
Role	Role - Create	Allows a User to create a Role	Create Role Assign Role Hierarchy Assign Access Policy Assign Role Members Publish Role to Organization
Role	Role - Modify	Allows a User to modify a Role	Modify Role Attributes Assign or Unassign Role Hierarchy Assign or Unassign Access Policy Assign or Unassign Role Members Publish Role to Organization
Role	Role - Delete	Allows a User to delete a Role	Delete Role View or Search Role
Role	Role - View / Search	Allows a User to view and search for Roles	View or Search Role View Role Hierarchy View Role Members View Role Access Policy View Organizations Published To
User	User - Create	Allows a User to create another User	Create User View or Search User
User	User - Modify	Allows a User to modify another User	Modify User Attributes View or Search User Request, Remove, or Modify Roles View Direct Reports View AdminRoles
User	User - Delete	Allows a User to delete another User	Delete User View or Search User
User	User - Enable	Allows a User to enable another User	Enable User View or Search User
User	User - Disable	Allows a User to disable another User	Disable User View or Search User

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
User	User - Lock	Allows a User to lock an Oracle Identity Manager Account	Lock User View or Search User
User	User - Unlock	Allows a User to unlock an Oracle Identity Manager Account	Unlock User View or Search User
User	User - Change Password	Allows a User to change another User's password	Change User Password View or Search User
User	User - View/Search	Allows a User to search for and view Users and their details	View or Search User View Roles View Direct Reports View Admin Roles
User	User - View Requests	Allows a User to search for requests	View User Requests View or Search Users
Relationships	Provision Accounts	Allows a User to provision Accounts, including start and end dates, on another User	Request Account View or Search User View or Search Accounts Modify Accounts
Relationships	Deprovision Accounts	Allows a User to deprovision Accounts on another User, including setting end dates	Remove Account View or Search User View or Search Accounts Modify Accounts
Relationships	Modify Provisioned Accounts	Allows a User to modify another User's provisioned Account, including start and end dates	Modify Accounts View or Search User View or Search Accounts
Relationships	Enable Provisioned Accounts	Allows a User to enable Account of another User	Enable Account View or Search User View or Search Accounts
Relationships	Disable Provisioned Accounts	Allows a User to disable Account of another User	Disable Account View or Search User View or Search Accounts
Relationships	Change Provisioned Account Password	Allows a User to change Account password for another User	Change Account Password View or Search User View or Search Accounts
Relationships	View Provisioned Accounts	Allows a User to see another User's provisioned Accounts	View or Search User View or Search Accounts

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
Relationships	Grant Account Entitlements	Allows a User to grant Entitlements, including start and end dates, for another User	Request Entitlement View or Search User View or Search Account View or Search Account Entitlement Modify Entitlement
Relationships	Modify Account Entitlements	Allows a User to modify Account Entitlements for another User	Modify Entitlement View or Search User View or Search Account View or Search Account Entitlement
Relationships	Revoke Account Entitlements	Allows a User to revoke Account Entitlements for another User, including setting end dates	Remove Entitlement View or Search User View or Search Account View or Search Account Entitlement Modify Entitlement
Relationships	View Account Entitlements	Allows a User to see another User's Entitlements	View or Search Account Entitlement View or Search User View or Search Account Entitlement
Password Policy	Password Policy - Create	Allows a User to create a Password Policy	Create Password Policy View or Search Password Policy
Password Policy	Password Policy - Modify	Allows a User to modify a Password Policy	Modify Password Policy View or Search Password Policy
Password Policy	Password Policy - Delete	Allows a User to delete a Password Policy	Delete Password Policy View or Search Password Policy
Password Policy	Password Policy - View/ Search	Allows a User to view and search for Password Policies	View or Search Password Policy

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
Proxy User	ProxyUser - View	Allows a User to view proxy for another User.	

Note:

While creating a custom admin role to manage eth

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
			e p r o x i e s , a p a r t f r o m t h e **P r o x y U s e r - V i e w** , **P r o x y U s e r - A d d** , **P r o x**

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
			yUser-Modify, ProxyUser-Delete capabilities, you need to add

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
		the **User-View/Search** capability to the admin role. This will le	

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
			nsureth eadmi nuser canvi ewand sear chfo rthe user stos eeta sp

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
		r o x y .	
Proxy User	ProxyUser - Add	Allows a User to add proxy for another User.	
Proxy User	ProxyUser - Modify	Allows a User to modify proxy for another User.	
Proxy User	ProxyUser - Delete	Allows a User to delete proxy for another User.	
Organization	Organization - Create	Allows a User to create an Organization	Create Organization View or Search Organization View or Search User View or Search Password Policy Create Sub-Organization
Organization	Organization - Modify	Allows a User to modify an Organization	Modify Organization Attributes View or Search Organization Disable Organization View Organization Members Set User Membership Rule View Available Roles View Available Accounts View Available Entitlements Provision Accounts Assign or Unassign AdminRoles
Organization	Organization - Delete	Allows a User to delete an Organization	Delete Organization View or Search Organization
Organization	Organization - View / Search	Allows a User to view and search for Organizations	View or Search Organization View Child Organizations View Members View Available Roles View Admin Roles View Provisioned Accounts
Organization	Organization - View Organization Members	Allows a User to see the members of an Organization	View Organization Members View or Search Organizations
Organization	Organization - View Organization Published Entitlements	Allows a User to see the Entitlements published to an Organization	View Available Entitlements View or Search Organizations

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
Organization	Organization - View Organization Published Application Instances	Allows a User to see the applications published to an Organization	View Available Accounts View or Search Organizations

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
Identity Audit Policy	Identity Audit Policy - Create	Allows a User to create an Identity Audit Policy	Create Identity Audit Policy View or Search Identity Audit Policy Assign or Unassign Identity Audit Rule Create Identity Audit Scan Run View Identity Audit Configuration

Note:

Entity types IdentityAuditScanRunandIdent

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
			ityAuditPolicyViolationCausesareNotSupportedinthisrel

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
		e a s e .	
Identity Audit Policy	Identity Audit Policy - Modify	Allows a User to modify an Identity Audit Policy	Modify Identity Audit Policy View or Search Identity Audit Policy Assign or Unassign Identity Audit Rule Create Identity Audit Scan Run View Identity Audit Configuration
Identity Audit Policy	Identity Audit Policy - Delete	Allows a User to delete an Identity Audit Policy	Delete Identity Audit Policy View or Search Identity Audit Policy
Identity Audit Policy	Identity Audit Policy - Enable	Allows a User to enable an Identity Audit Policy	Enable Identity Audit Policy View or Search Identity Audit Policy
Identity Audit Policy	Identity Audit Policy - Disable	Allows a User to disable an Identity Audit Policy	Disable Identity Audit Policy View or Search Identity Audit Policy
Identity Audit Policy	Identity Audit Policy - Assign Rule	Allows a User to assign Identity Audit Rules to an Identity Audit Policy	Assign Identity Audit Rule View or Search Identity Audit Policy
Identity Audit Policy	Identity Audit Policy - Unassign Rule	Allows a User to unassign Identity Audit Rules from an Identity Audit Policy	Unassign Identity Audit Rule View or Search Identity Audit Policy
Identity Audit Policy	Identity Audit Policy - View / Search	Allows a User to view an Identity Audit Policy	View or Search Identity Audit Policy View Identity Audit Rule
Identity Audit Rule	Identity Audit Rule - Create	Allows a User to create an Identity Audit Rule	Create Identity Audit Rule View or Search Identity Audit Rule
Identity Audit Rule	Identity Audit Rule - Modify	Allows a User to modify an Identity Audit Rule	Modify Identity Audit Rule View or Search Identity Audit Rule
Identity Audit Rule	Identity Audit Rule - Delete	Allows a User to delete an Identity Audit Rule	Delete Identity Audit Rule View or Search Identity Audit Rule

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
Identity Audit Rule	Identity Audit Rule - Enable	Allows a User to enable an Identity Audit Rule	Enable Identity Audit Rule View or Search Identity Audit Rule
Identity Audit Rule	Identity Audit Rule - Disable	Allows a User to disable an Identity Audit Rule	Disable Identity Audit Rule View or Search Identity Audit Rule
Identity Audit Policy	Identity Audit Rule - View/Search	Allows a User to view an Identity Audit Rule	View or Search Identity Audit Rule
Identity Audit Configuration	Identity Audit Configuration - Modify	Allows a User to modify the Identity Audit Configuration	Modify Identity Audit Configuration View Identity Audit Configuration
Identity Audit Configuration	Identity Audit Configuration - View	Allows a User to view the Identity Audit Configuration	View Identity Audit Configuration
Identity Audit Scan Definition	Identity Audit Scan Definition - Create	Allows a User to create an Identity Audit Scan definition	Create Identity Audit Scan Definition View or Search Identity Audit Scan Definition Create Identity Audit Scan Run
Identity Audit Configuration	Identity Audit Scan Definition - Modify	Allows a User to modify an Identity Audit Scan definition	Modify Identity Audit Scan Definition View or Search Identity Audit Scan Definition Create Identity Audit Scan Run
Identity Audit Configuration	Identity Audit Scan Definition - Delete	Allows a User to delete an Identity Audit Scan definition	Delete Identity Audit Scan Definition View or Search Identity Audit Scan Definition

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
Identity Audit Configuration	Identity Audit Scan Definition - View	Allows a User to view and search for Identity Audit Scan Definitions	View or Search Identity Audit Scan Definition View User View Role View Application Instance View Entitlement View Organization View Requests View User Roles View User Accounts View User Entitlements View Identity Audit Policy View Identity Audit Configuration View Identity Audit Scan Run Search Catalog Item View Identity Audit Policy Violation
Identity Audit Policy Violation	Identity Audit Policy Violation - Force Close	Allows a User to force close an Identity Audit Policy Violation	Force Identity Audit Policy Violation Close View or Search Identity Audit Policy Violation
Identity Audit Policy Violation	Identity Audit Policy Violation - Assign	Allows a User to assign or reassign an Identity Audit Policy Violation	Assign Identity Audit Policy Violation View or Search Identity Audit Policy Violation
Identity Audit Policy Violation	Identity Audit Policy Violation - Complete	Allows a User to complete an Identity Audit Policy Violation	Complete Identity Audit Policy Violation View or Search Identity Audit Policy Violation Accept Identity Audit Policy Violation Cause Risk Request Identity Audit Policy Violation Cause Remediation Mark Identity Audit Policy Violation Cause as Fixed
Identity Audit Policy Violation	Identity Audit Policy Violation - View	Allows a User to view an Identity Audit Policy Violation	View or Search Identity Audit Policy Violation View or Search Identity Audit Policy Violation Cause
Certification	Certification - Modify	Allows a User to modify a Certification	Modify Certification View Certification
Certification	Certification - View	Allows a User to view a Certification	View Certification

Table B-1 (Cont.) Authorization Functional Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
Certification	Certification - Modify Configuration	Allows a User to modify the Certification Configuration	Modify Certification Configuration
Certification	Certification - View Configuration	Allows a User to view the Certification Configuration	View Certification Configuration
Access Policy	Access Policy - Create	Allows a User to create Access Policies	Create Access Policy View or Search Access Policy
Access Policy	Access Policy - Delete	Allows a User to delete Access Policies	Delete Access Policy View or Search Access Policy
Access Policy	Access Policy - Modify	Allows a User to modify Access Policies	Edit Access Policy View or Search Access Policy
Access Policy	Access Policy - View/ Search	Allows a User to view and search for Access Policies	View or Search Access Policy

B.2 List of Self Capabilities

This appendix provides the list of Admin Role capabilities in Table B-1 and the list of Self capabilities in Table B-2.

Table B-2 Self Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
Self Service	Self Service - Modify Profile	Allows a User to modify their own user profile	Modify Self View or Search Self
Self Service	Self Service - Modify Proxy	Allows a User to add, modify, delete or view their own proxies	Modify Self Proxy View or Search Self Add Self Proxy Delete Self Proxy View Self Proxy
Self Service	Self Service - Request Role Memberships	Allows a User to request Roles published to their home organization	Request Self Role Modify Self Role View Self Roles
Self Service	Self Service - Modify Roles Memberships	Allows a User to modify Roles assigned to them	Modify Self Role View Self Roles
Self Service	Self Service - Revoke Role Memberships	Allows a User to delete Roles assigned to them	Remove Self Role Modify Self Role View Self Roles
Self Service	Self Service - Request Accounts	Allows a User to request Accounts published to their home organization, including start and end dates	Request Self Account Modify Self Accounts View Self Accounts

Table B-2 (Cont.) Self Capabilities

Functional Type	Functional Capability	Description	Implied Capabilities
Self Service	Self Service - Modify Accounts	Allows a User to modify Accounts assigned to them	Modify Self Accounts View Self Accounts
Self Service	Self Service - Change Account Password	Allows a User to change password on Accounts assigned to them	Change Self Account Password View Self Accounts
Self Service	Self Service - Revoke Accounts	Allows a User to delete Accounts assigned to them now or on a specified end date	Remove Account Modify Self Account View Self Accounts
Self Service	Self Service - Request Entitlements	Allows a User to request Entitlements published to their home organization, including start and end dates	Request Self Entitlement Modify Self Entitlement View Self Entitlements
Self Service	Self Service - Modify Entitlements	Allows a User to modify Entitlements assigned to them	Modify Self Entitlement View Self Entitlements
Self Service	Self Service - Revoke Entitlements	Allows a User to delete Entitlements assigned to them now or at a specified end date	Remove Self Entitlement Modify Self Entitlement View Self Entitlements

C

Sample Application Template XML

A sample application template.xml file is shown below:

```
<application>
<applicationName>Generic UNIX Target</applicationName>
<applicationDisplayName>Generic UNIX Target</applicationDisplayName>
<description>Generic UNIX Target</description>
<connectorDisplayName>Generic UNIX Connector</connectorDisplayName>
<connectorVersion>11.1.1.8.0</connectorVersion>
<disconnected>false</disconnected>
<basicConfigurations>
   <basicConfig name="host" value="" helpText="Enter the UNIX host."
dataType="String" required="true" displayName="Host"/>
   <basicConfig name="loginUser" value="" helpText="User name with which to
login to the target. Eg. root." dataType="String" required="true"
displayName="Login User"/>
   <basicConfig name="loginUserpassword" value="" helpText="Password for the
Login User." dataType="GuardedString" required="true" encrypted="true"
displayName="Login User Password"/>
   <basicConfig name="loginShellPrompt" value="[#$]" helpText="The shell
prompt which is displayed when you login to the target. Eg. $ or #."
dataType="String" required="false" displayName="L    ogin Shell Prompt"/>
   <basicConfig name="port" value="22" helpText="Port on which to connect.
Eg. 22 for SSH, 23 for Telnet." dataType="int" required="false"
displayName="Port"/>
   <basicConfig name="Connector Server Name" value="" helpText="Name of the
connector server." required="false" displayName="Connector Server Name"/>
   <basicConfig name="connectionType" value="SSH" helpText="The connection
type to use. SSH, TELNET or SSHPUBKEY (for key based authentication)."
dataType="String" required="false" displayNam    e="Connection Type"/>
   <basicConfig name="connectorPrompt" value="#@#" helpText="The prompt
which should be used by the connector for its operations. This expression
should not be contained in user logins, users     attribute values like
GECOS etc. Default is #@#." dataType="String" required="false"
displayName="Connector Prompt"/>
   <basicConfig name="passphrase" value="" helpText="The passphrase for the
private key." dataType="GuardedString" required="false" encrypted="true"
displayName="Passphrase"/>
   <basicConfig name="propertyFileName" value="" helpText="The relative path
of the Script.properties file specific to the UNIX flavor. The connector
uses this to decide which script to use f    or what operation. Eg. scripts/
linux/nonsudo/ScriptProperties.properties. If this is left blank, the
connector would try to determine the value for this field."
dataType="String" required    ="false" displayName="Property File Name"/>
   <basicConfig name="rbacAuthorization" value="false" helpText="If RBAC
authorization is used for Solaris, it should be true, otherwise false."
dataType="boolean" required="false" displayNam     e="RBAC Authorization"/>
   <basicConfig name="rbacRoleName" value="" helpText="Role name in RBAC."
```

```
dataType="String" required="false" displayName="RBAC Role Name"/>
   <basicConfig name="rbacRolePassword" value="" helpText="RBAC Role
Password" dataType="GuardedString" required="false" encrypted="true"
displayName="RBAC Role Password"/>
   <basicConfig name="sudoAuthorization" value="false" helpText="If
the user required sudo authorization or not. false for root user, true
otherwise." dataType="boolean" required="false" disp    layName="Sudo
Authorization"/>
</basicConfigurations>
<advanceConfigurations>
   <advanceConfig name="Connector Name"
value="org.identityconnectors.genericunix.GenericUnixConnector"
required="false" displayName="Connector Name"/>
   <advanceConfig name="defaultConnectorShell" value="sh"
helpText="Default Connector Shell" dataType="String" required="false"
displayName="Default Connector Shell"/>
   <advanceConfig name="Bundle Name"
value="org.identityconnectors.genericunix" required="false"
displayName="Bundle Name"/>
   <advanceConfig name="Bundle Version" value="1.0.1" required="false"
displayName="Bundle Version"/>
   <advanceConfig name="targetDateFormat" value="MM/dd/yy"
helpText="The date format expected by the target when specifying the
Expire Date attribute." dataType="String" required="false" disp
layName="Target Date Format"/>
   <advanceConfig name="whitelistRegex" value="[A-Za-z0-9_//]*"
helpText="The list of acceptable characters in field values. This
property is a regex. Note: it does not apply to the GECOS (co
mments field). Default is [A-Za-z0-9_//]*." dataType="String"
required="false" displayName="Whitelist Regex"/>
   <advanceConfig name="sudoPasswdExpectExpression" value="password:"
helpText="The password prompt displayed when running a command in sudo
mode. Default value is password." dataType="String    "
required="false" displayName="Sudo Passwd Expect Expression"/>
   <advanceConfig name="rbacRoleExpectExpressions" value="password:,
[$#]" helpText="The password expression displayed when switching to
the RBAC role and the expected shell prompt separated b    y comma.
Eg. password,#." dataType="String" required="false" displayName="RBAC
Role Expect Expressions"/>
   <advanceConfig name="commandTimeout" value="10000000" helpText="The
command timeout value in milliseconds." dataType="int"
required="false" displayName="Command Timeout"/>
   <advanceConfig name="configPropertiesOnScripts"
value="moveHomeDirContents,shadow,defaultHomeBaseDir,defaultPriGroup,de
faultShell,nisPwdDir,nisBuildDirectory,removeHomeDirContents,forceDel
  eteUserHome,syncToken,mirrorFilesLocation,connectorPrompt"
helpText="The properties whose value if provided, would be available
in the scripts." dataType="String" required="false" display
Name="Config Properties On Scripts"/>
   <advanceConfig name="mirrorFilesLocation" value="/etc/
connector_mirror_files" helpText="The directory where the connector
can create copies of the /etc/passwd and shadow files. Default
is     /etc/connector_mirror_files." dataType="String"
required="false" displayName="Mirror Files Location"/>
   <advanceConfig name="passwordExpectExpressions" value="new[\s]
```

```
(unix[\s])?password:,new[\s](unix[\s])?password([\s]again)?:" helpText="The
expressions displayed on the target when setting t     he users password.
Eg. If the expressions displayed on running the passwd command are: Enter
password: and Re-enter password:, then the value for this field can be enter
password,re-ente     r password. Note: a regex can be provided here and the
two expressions should be comma separated." dataType="String"
required="false" displayName=" Password Expect Expressions"/>
   <advanceConfig name="supportedLanguage" value="Bourne" helpText="The
supported language for ScriptOnResource opertation. Default is Bourne."
dataType="String" required="false" displayName=     "Supported Language"/>
   <advanceConfig name="telnetAuthenticationPrompts"
value="login: ,Password:" helpText="The authentication prompts displayed
when doing telnet login. The prompts for user name and password s    hould
be provided as comma separated values. Eg. login,password."
dataType="String" required="false" displayName="Telnet Authentication
Prompts"/>
   <advanceConfig name="moveHomeDirContents" value="true"
helpText="Specifies whether the old home directory contents should be moved
to the new directory location when changing the Home Dire    ctory. Possible
values are true or false. Default is true." dataType="String"
required="false" displayName="Move Home Dir Contents"/>
   <advanceConfig name="privateKey[LOADFROMURL]" value="" required="false"
displayName="Private Key"/>
 </advanceConfigurations>
 <objectClass name="User">
   <provisioningConfig>
     <accountName>User Login</accountName>
     <validationScript>
     </validationScript>
     <transformationScript
            def getBeneficiaryAttrFromContext(attrName) {
                        if (context.beneficiary != null) {
                               return
context.beneficiary.getAttribute(attrName);
                            }
                return null;
                }

                def getBeneficiaryPwdFromContext() {
                    return context.beneficiaryPassword;
                }

                if (binding.variables != null) {
                    if (binding.variables.containsKey("context")) {
                        if (context.operationType != null) {

if(context.operationType.equalsIgnoreCase("create")){
                                if (context.provisionMechanism != null) {

if(context.provisionMechanism.equalsIgnoreCase("POLICY")) {
                                        User_Login =
getBeneficiaryAttrFromContext("User Login");
                                        Password =
getBeneficiaryPwdFromContext();
                                    } else if
```

```
(context.provisionMechanism.equalsIgnoreCase("REQUEST") ||
context.provisionMechanism.equalsIgnoreCase("ADMIN")) {
                                        if (User_Login == null ||
User_Login == "") {
                                            User_Login =
getBeneficiaryAttrFromContext("User Login");
                                        }

                                        if (Password == null ||
Password == "") {
                                            Password =
getBeneficiaryPwdFromContext();
                                        }
                                    }
                                }
                            }
                        }
                    }

         </transformationScript>
         <capabilities>
         <capability actionName="disable" enabled="true"/>
         <capability actionName="delete" enabled="true">
              <actionScripts>
                   <actionScript language="Shell" triggerTime="Before"
target="Connector"/>
                   <actionScript language="Shell" triggerTime="After"
target="Connector"/>
              </actionScripts>
         </capability>
         <capability actionName="enable" enabled="true"/>
         <capability actionName="create" enabled="true">
               <actionScripts>
                   <actionScript language="Shell" triggerTime="Before"
target="Connector"/>
                   <actionScript language="Shell" triggerTime="After"
target="Connector"/>
               </actionScripts>
          </capability>
          <capability actionName="update" enabled="true">
             <actionScripts>

                 <actionScript language="Shell" triggerTime="Before"
target="Connector"/>
                 <actionScript language="Shell" triggerTime="After"
target="Connector"/>
              </actionScripts>
           </capability>
       </capabilities>
    </provisioningConfig>
    <reconConfig>
    <reconJobDetails>
      <jobDetail mode="Entitlement" jobName="UNIX User Primary Group
Lookup Reconciliation">
```

```
          <parametersList>
              <parameter dataType="String" helpText="Application Name"
value="" name="Application Name" />
              <parameter dataType="String" helpText="Code Key Attribute"
value="__NAME__" name="Code Key Attribute" />
              <parameter dataType="String" helpText="Decode Attribute"
value="__NAME__" name="Decode Attribute" />
              <parameter dataType="String" helpText="Lookup Name"
value="Lookup.UNIX.PrimaryGroup" name="Lookup Name" />
              <parameter dataType="String" helpText="Object Type"
value="Group" name="Object Type" />
          </parametersList>
       </jobDetail>
       <jobDetail mode="Entitlement" jobName="UNIX User Shell Lookup
Reconciliation">
           <parametersList>
               <parameter dataType="String" helpText="Application Name"
value="" name="Application Name" />
               <parameter dataType="String" helpText="Code Key Attribute"
value="__NAME__" name="Code Key Attribute" />
               <parameter dataType="String" helpText="Decode Attribute"
value="__NAME__" name="Decode Attribute" />
               <parameter dataType="String" helpText="Lookup Name"
value="Lookup.UNIX.UserShell" name="Lookup Name" />
               <parameter dataType="String" helpText="Object Type"
value="__SHELLS__" name="Object Type" />
           </parametersList>
        </jobDetail>
        <jobDetail mode="Full" jobName="UNIX Target Resource Full User
Reconciliation">
        <parametersList>
                <parameter dataType="String" helpText="Application Name"
value="" name="Application Name" />
                <parameter dataType="String" helpText="Batch Size" value="0"
name="Batch Size" />
                <parameter dataType="String" helpText="Batch start index"
value="0" name="Batch start index" />
                <parameter dataType="String" helpText="Filter" value=""
name="Filter" />
                <parameter dataType="String" helpText="No. of Batches"
value="0" name="No. of Batches" />
                <parameter dataType="String" helpText="Object Type"
value="User" name="Object Type" />
         </parametersList>
         </jobDetail>
         <jobDetail mode="Incremental" jobName="UNIX Target Incremental
Resource User Reconciliation">
         <parametersList>
                <parameter dataType="String" helpText="Application Name"
value="" name="Application Name" />
                <parameter dataType="String" helpText="Batch Size" value="0"
name="Batch Size" />
                <parameter dataType="String" helpText="Batch start index"
value="0" name="Batch start index" />
                <parameter dataType="String" helpText="No. of Batches"
```

```
value="0" name="No. of Batches" />
                <parameter dataType="String" helpText="Object Type"
value="User" name="Object Type" />
                <parameter dataType="String" helpText="Scheduled Task
Name" value="UNIX Target Incremental Resource User Reconciliation"
name="Scheduled Task Name" />
                <parameter dataType="String" helpText="Sync Token"
value="" name="Sync Token" />
          </parametersList>
          </jobDetail>
       </reconJobDetails>
             <identityCorrelationRule ruleOperator="AND">
                   <ruleElement targetAttribute="__NAME__"
userAttribute="User Login" elementOperator="Equals"
transformName="NONE"/>
             </identityCorrelationRule>
             <situationResponses>
                <situationResponse situation="No Matches Found"
response="None"/>
                 <situationResponse situation="One Entity Match Found"
response="Establish Link"/>
                 <situationResponse situation="One Process Match
Found" response="Establish Link"/>
             </situationResponses>
       </reconConfig>
       <form name="UNIX">
          <schemaAttributes>
             <schemaAttribute name="__NAME__" dataType="String"
displayName="User Login" length="32" keyField="true" required="true"
fieldType="TextField" reconcileable="true"
provisionable=                  "true"/>
             <schemaAttribute name="__PASSWORD__" dataType="String"
displayName="Password" length="32" fieldType="PasswordField"
provisionable="true" encrypted="true"/>
             <schemaAttribute name="COMMENTS##COMMENTS##"
dataType="String" displayName="GECOS" length="250"
fieldType="TextField" reconcileable="true" provisionable="true"/>
             <schemaAttribute name="CREATE_HOME_DIR"
dataType="String" displayName="Create home directory" length="10"
fieldType="ComboBox" reconcileable="true" provisionable="true"
listOfVa                  lues="Lookup.UNIX.YesNo.Options"/>
             <schemaAttribute name="HOME_DIR" dataType="String"
displayName="Home Directory" length="250" fieldType="TextField"
reconcileable="true" provisionable="true"/>
             <schemaAttribute name="EXP_DATE##DATE##" dataType="Date"
displayName="Expire Date" length="0" fieldType="DateFieldDlg"
reconcileable="true" provisionable="true"
advanceFlags="DA                TE"/>
             <schemaAttribute name="INACTIVE" dataType="Int"
displayName="Inactive Days" length="10" fieldType="TextField"
reconcileable="true" provisionable="true"/>
             <schemaAttribute name="PGROUP" dataType="String"
displayName="Primary Group" length="50" fieldType="LookupField"
reconcileable="true" provisionable="true"
advanceFlags="LOOKUP"
```

```
listOfValues="Lookup.UNIX.PrimaryGroup"/>
              <schemaAttribute name="USID" dataType="Int" displayName="UID"
length="10" fieldType="TextField" reconcileable="true" provisionable="true"/>
              <schemaAttribute name="USER_SHELL" dataType="String"
displayName="User Shell" length="250" fieldType="LookupField"
reconcileable="true" provisionable="true"
advanceFlags="LOOKUP                " listOfValues="Lookup.UNIX.UserShell"/>
              <schemaAttribute name="SKEL_DIR" dataType="String"
displayName="Skeleton Directory" length="250" fieldType="TextField"
provisionable="true"/>
              <schemaAttribute name="__UID__" dataType="String"
displayName="ReturnValue" length="100" fieldType="TextField"
reconcileable="true" provisionable="true"/>
              <schemaAttribute name="__ENABLE__" dataType="String"
displayName="Status" length="0" fieldType="TextField" reconcileable="true"/>
          </schemaAttributes>
          <form name="Secondary Groups">
               <schemaAttributes>
                   <schemaAttribute name="SECONDARYGROUP" dataType="String"
displayName="Secondary Group" length="50" keyField="true"
fieldType="LookupField" entitlement="true"
reconcileable=                    "true" provisionable="true"
advanceFlags="LOOKUP" listOfValues="Lookup.UNIX.PrimaryGroup"/>
               </schemaAttributes>
          </form>
        </form>
      </objectClass>
     <catalogAttributes>
     </catalogAttributes>>
     <organizations>
         <organization name="Top" heirarchy="true" type="System"/>
     </organizations>
     <status>ACTIVEstatus>ACTIVE>
 </application>
```