

Oracle Identity Manager 11.1.2.3: New Features and Enhancements (Training On Demand)

Code: D95736GC10
URL: [View Online](#)

This Oracle Identity Manager 11.1.2.3: New Features and Enhancements training teaches you about new features associated with Oracle Identity Manager(OIM), one product of the Oracle Identity Governance Suite 11g R2 PS3. Expert Oracle University instructors will teach you about admin roles; examine types of admin roles available in Oracle Identity Manager and see how by managing these roles, you can perform authorization and authentication in Oracle Identity Manager.

Learn To:

- Explore the new identity self-service console user interface.
- Use the system for Cross-domain Identity Management(SCIM) APIs to integrate Oracle Identity Manager with clients through REST and JSON.
- Configure the new approval workflows, associating operations, rules and conditions.
- Manage password policies with custom challenge options, including user defined challenge questions.
- Enable the Identity Audit module, explore role lifecycle management, role history and role analytics.
- Manage Oracle Identity Manager authorization through admin roles and self-service capabilities.
- Promote detective and preventive segregation of duties through identity audit policies, rules and scans.

Benefits to You

By taking this course, you'll develop the knowledge and skills to facilitate CRUD of organizations, users, enterprise roles, administration roles and password policies via the new UI of the Identity Self-Service Console. You'll develop the ability to integrate Oracle Identity Manager with RESTful/JSON clients, such as mobile applications, modern websites and SOA composites.

Dive into Approval Workflows, Lifecycle Management and Role Analytics

Learn about single, bulk and heterogeneous operations, rules and conditions associated with the new approval workflows. Implement conditional password policies per organization, with user defined challenge questions. See how role lifecycle management, role consolidation and role analytics fit seamlessly into role management workflows.

Explore Self-Service Capabilities

You'll also become familiar with self-service capabilities and develop an understanding of the role policies and rules play in restricting a user's self-service capabilities in Oracle Identity Manager. Learn about the new Identity Audit (IDA) module for PS3, including how to use IDA to detect segregation of duties violations in Oracle Identity Manager.

Skills Gained

- Describe the new features in Oracle Identity Manager 11g R2 PS3

- Explore the new user interface
- Explore the SCIM APIs
- Describe the REST architectural style and Java Script Object Notation (JSON)
- Describe the Oracle Identity Manager 11g R2 PS3 workflow policies
- Describe the workflow scenarios supported by Oracle Identity Manager 11g R2 PS3
- Configure password policies in Oracle Identity Manager 11g R2 PS3
- Enable the Identity Auditor module
- Explore role lifecycle management (LCM)
- Configure Oracle Identity Manager 11g R2 PS3 authorization
- Configure Identity Audit (IDA)

Prerequisites

- Experience with previous versions Oracle Identity Manager
- A general comprehension about Oracle WebLogic Server
- A general comprehension about LDAP and SOA
- Familiarity with Linux environment and commands

Course Details

Oracle Identity Manager 11g R2 PS3 New Features

- Overview
- Oracle Identity Manager Navigation
- System for Cross-domain Identity Management(SCIM) APIs
- Workflow Policies
- Password Policies
- Identity Auditor and Role Lifecycle Management (LCM)
- Authorization
- Identity Audit (IDA)

Navigating Oracle Identity Manager

- Starting the Oracle Identity Manager WebLogic Instances
- Launching and Navigating Oracle Identity Manager Administration Consoles
- Exploring the Embedded BI Publisher

Using the System for Cross-domain Identity Management(SCIM) APIs

- Using the Oracle Identity Manager SCIM API

Incorporating Approval Workflows

- Loading Entities into Oracle Identity Manager
- Deploying a custom SOA Composite

- Configuring Workflow Rules and Conditions
- Testing Workflow Rules
- Exploring the SOA Composite in Enterprise Manager

Managing Password Policies

- Exploring the Default Password Policy and Configuration
- Testing Authentication with the Default Policy
- Creating Password Policies
- Associating Password Policies to Organizations
- Testing the New Password Policy Configuration

Performing Role Lifecycle Management (LCM)

- Enabling the Identity Auditor Module
- Performing Role Lifecycle Management (LCM) Tasks
- Exploring Role History
- Exploring Role Analytics

Managing Authorization

- Assigning Admin Roles
- Verifying the Scope of Control
- Understanding Administration Roles
- Creating Administration Roles
- Deleting Nonadministration Roles
- Creating an Alternate Admin Role Administrator
- Restricting Administrator Actions
- Managing Self-Service Capabilities

Understanding Identity Audit (IDA)

- Creating an Identity Audit Rule
- Creating an Identity Audit Policy
- Previewing the Identity Audit Policy
- Creating a Scan Definition
- Reviewing and Managing Policy Violations
- Detecting SoD Policy Violations During a Request
- Exploring Role Consolidation and SoD Violations During Role Management Tasks