

Oracle Identity Manager 11.1.2.3: New Features and Enhancements

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