

Oracle Access Manager 11g: Administration

Volume I • Student Guide

D63114GC10

Edition 1.0

December 2010

D71610

ORACLE®

Authors

Vishal Parashar
David Goldsmith

Technical Contributors and Reviewers

Amjad Afanah
Jeremy Banford
Abhijit Bhatode
Rama Bollu
Vikas Pooven Chathoth
Toby Close
Jui Deshpande
Steve Doinidis
Sunil Gupta
Beomsuk Kim
Ashish Kolli
Vadim Lander
Derick Leo
Mayank Maria
Madhu Martin
Vamsi Motukuru
Rey Ong
Vimal Patel
Peter Povinec
Deepak Ramakrishnan
Shankar Raman
Chitra Sabapathy
Narasimhaiah Sreehari
Ramya Subramanya
Ramana Turlapati
Venkat Venkatnarayan
Weifang Xie

Editors

Smita Kommini
Priti Goswami

Graphic Designer

Satish Bettgowda

Publishers

Sujatha Nagendra
Giri Venugopal

Copyright © 2010, Oracle and/or its affiliates. All rights reserved.

Disclaimer

This document contains proprietary information and is protected by copyright and other intellectual property laws. You may copy and print this document solely for your own use in an Oracle training course. The document may not be modified or altered in any way. Except where your use constitutes "fair use" under copyright law, you may not use, share, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, or distribute this document in whole or in part without the express authorization of Oracle.

The information contained in this document is subject to change without notice. If you find any problems in the document, please report them in writing to: Oracle University, 500 Oracle Parkway, Redwood Shores, California 94065 USA. This document is not warranted to be error-free.

Restricted Rights Notice

If this documentation is delivered to the United States Government or anyone using the documentation on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose these training materials are restricted by the terms of the applicable Oracle license agreement and/or the applicable U.S. Government contract.

Trademark Notice

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

Contents

1 Course Overview

- Course Objectives 1-2
- Course Agenda: Day 1 1-4
- Course Agenda: Day 2 1-5
- Course Agenda: Day 3 1-6
- Course Agenda: Day 4 1-7
- Course Agenda: Day 5 1-8
- Practice Environment: Overview 1-9

2 Introduction to Oracle Access Manager

- Objectives 2-2
- Oracle Identity Management: Oracle + Sun Combination 2-3
- Oracle Access Management Suite Plus 2-6
- Salient Features of OAM 2-8
- OAM 11g Architecture 2-10
- Enterprise Deployment Architecture 2-11
- SSO Login Processing with OAM Agents 2-15
- Installation and Configuration 2-18
- Installation and Configuration Configuration Wizard Screenshot: Templates 2-20
- OAM 11g R1 Run-Time Architecture 2-21
- Management Interfaces 2-23
- Backward Compatibility of Agents in a Heterogeneous Environment 2-25
- Coexistence of OAM 10g and 11g Servers 2-26
- Coexistence of OSSO 10g and OAM 11g Servers 2-27
- Session Management 2-28
- Oracle Coherence in Session Management 2-30
- Usability and Life Cycle Management Enhancements 2-32
- Usability and Life Cycle Management Enhancements: Operational Metrics 2-33
- Windows Native Authentication 2-34
- Upgrade for OracleAS Single Sign-On 10.1.4.3.0 2-35
- Rich ADF-Based UI 2-36
- Connection Simulator: Access Tester 11g 2-37
- Access Tester 11g 2-38
- Key Enhancements in OAM 11g 2-39
- Oracle Access Manager 11g Comparison with Oracle Access Manager 10g 2-42

Oracle Access Manager 11g Policy Object Comparison 2-46
Product Component Mapping 2-47
Summary 2-48
Quiz 2-49
Practice 2 Overview: Viewing New Features Viewlet 2-53

3 Installation and Configuration

Objectives 3-2
Road Map 3-3
Domain: Overview 3-4
Domain Diagram 3-6
Domain Restrictions 3-8
Server 3-10
Administration Server 3-11
Managed Server 3-13
Interaction Between the Administration Server and Managed Servers 3-14
What Is a Machine? 3-15
Relationship of Machines to Other Components 3-16
Cluster 3-17
Cluster Guidelines 3-19
WebLogic Scripting Tool (WLST) 3-20
WLST Modes 3-21
WLST Example 3-22
Oracle WebLogic Server ILT Courses 3-23
Road Map 3-24
Oracle Fusion Middleware Home and Oracle WebLogic Server Home 3-25
Oracle Home 3-26
Installing and Configuring Oracle Identity Management: Sequence of Steps 3-27
Wizards: Installation Versus Configuration 3-28
System Requirements for Oracle Identity Management 11g R1(11.1.1.3.0) 3-29
Road Map 3-30
Oracle WebLogic Server 11g R1 PS 2 (10.3.3) Installation 3-31
System Requirements for Oracle WebLogic Server 3-33
GUI Mode Installation 3-35
Choosing or Creating a Home Directory 3-36
Registering for Support 3-37
Choosing an Installation Type and Products 3-38
Choosing the JDK and Product Directory 3-39
Windows-Specific Screens 3-40
Installation and Summary 3-41
QuickStart 3-42

Console and Silent Mode Installations 3-43
Post-Installation: Middleware Home 3-44
Oracle WebLogic Server Directory Structure 3-45
Setting Environment Variables 3-47
Practice 3 Overview: Installing Oracle WebLogic Server 10.3.3 3-48
Road Map 3-49
Installing Oracle Database 3-50
Creating Schemas by Using RCU 3-51
Practice 3 Overview: Running the Repository Creation Utility 3-55
Road Map 3-56
Installing Oracle Identity Management: Welcome and Prerequisite Checks 3-57
Installing Oracle Identity Management: Install Location and Summary 3-58
Installing Oracle Identity Management: Progress Bar and Install Complete 3-59
Practice 3 Overview: Installing Oracle Identity Management 11g 3-61
Road Map 3-62
Configuration Wizard: Creating Domain and Domain Source 3-63
Configuration Wizard: Domain and Administrator Settings 3-65
Configuration Wizard: Server Start Mode, JDK, and Customization Options 3-66
Configuring JDBC Data Source: OAM with Database Policy Store 3-68
Configuration Wizard: Administration and Managed Servers 3-69
Configuration Wizard: Clusters and Machines 3-72
Configuration Wizard: Assigning Servers to Machines
and Target Deployments 3-75
Configuration Wizard: Target Services and RDBMS Security Store 3-77
Configuration Wizard: Configuration Summary and Creating Domain 3-79
Configuring OHS For Oracle WebLogic Server 3-80
Practice 3 Overview: Creating a New Domain and Configuring OAM Server 3-83
Configuration Wizard: Extending Domain and Domain Source 3-84
Output of Configuration Wizard: Directory Structure 3-92
Road Map 3-94
Starting Oracle Access Manager 3-95
Practice 3 Overview: Starting Administration and Managed Server 3-97
Validating a Successful Installation and Configuration 3-98
Oracle WebLogic Server Administration Console 3-99
Oracle WebLogic Server Administration Console: Server Status 3-100
OAM_Server1: Applications Deployed 3-101
AdminServer: Applications Deployed 3-102
Oracle Access Manager Administration Console 3-103
Oracle Enterprise Manager Fusion Middleware Control 3-105
Relationship Between Farm and Domain 3-107

Practice 3 Overview: Sanity Checks and Walkthrough of Management Interfaces 3-108
Road Map 3-109
Uninstalling Oracle WebLogic Server 3-110
Uninstalling Oracle Identity Management Home 3-111
Uninstalling Oracle Common Home and Deleting Domain Home 3-112
Summary 3-113
Quiz 3-114

4 System Configuration: Servers, Data Sources, and Agents

Objectives 4-2
Practice 4 Overview: Installing and Configuring OHS 11g 4-3
Road Map 4-4
Servers 4-5
Creating and Deleting a New Managed Server 4-7
Managing Servers 4-8
Individual Server Properties 4-9
OAM Proxy 4-11
Managing Servers from WLS Admin Console and Command Line 4-12
Road Map 4-13
Agents 4-14
WebGate Provisioning and Installation 4-17
Installing and Configuring WebGate 11g 4-18
Practice 4 Overview: Installing, Creating, and Configuring an OAM 11g WebGate 4-21
Road Map 4-22
Registering Agents 4-23
Creating or Registering OAM Agents by Using OAM Admin Console 4-26
Viewing and Editing OAM Agent Registration by Using OAM Admin Console 4-28
Creating or Registering OSSO Agents by Using OAM Admin Console 4-32
Viewing and Editing OSSO Agent Registration by Using OAM Admin Console 4-33
Configuring OAM 10g WebGate in an Existing OAM 10g Deployment to Use OAM 11g Server 4-35
In-Band Versus Out-of-Band Registration of Agents 4-37
Registration Tool 4-39
Output Files 4-42
Registration Tool 4-43
Request File 4-45
Sample Request File: Short Version 4-47
Key Request Parameters 4-51
Request File: Parameter Guidelines 4-52

In-Band Registration Using `oamreg` Tool 4-54
Out-of-Band Registration Using `oamreg` Tool 4-58
Remote Registration: Common Issues 4-62
10g WebGate Installation: General Comments 4-63
Practice 4 Overview: Registering Agents: OAM Admin
Console, In-Band, Out-Of-Band Modes 4-64
Road Map 4-65
WLS Agent (or OAM Agent) Topology 4-66
General Features of OAM Agent 4-68
WLS Agent Configuration 4-70
Resources Protected via WLS Agent 4-73
Road Map 4-74
Data Sources 4-75
Data Repositories 4-77
User Identity Store: WLS Embedded LDAP Server 4-78
User Identity Store: Managing LDAP Servers 4-80
Testing LDAP Connection 4-84
Practice 4 Overview: WLS Embedded LDAP, OID as LDAP Store, WLS Agent 4-85
Road Map 4-86
Keystore 4-87
Securing Communication Between WebGate and OAM Server 4-88
Generating Private Key, Certificate Request, and Downloading Certificates
from CA 4-90
Configuring OAM Server to Use Certificates 4-91
Configuring WebGate to Use Certificates 4-96
Summary 4-98
Quiz 4-99
Practice 4 Overview: SSL Enabling WebGate and OAM 11g Server 4-104

5 Policy Configuration: Shared Components and Application Domains

Objectives 5-2
Road Map 5-3
Shared Components: Resource Types 5-4
Shared Components: Host Identifier 5-5
Road Map 5-8
Access Control 5-9
Authentication 5-11
Authorization 5-12
Road Map 5-13
Authentication Module 5-14
Authentication Module Features 5-17

Step-Up Authentication Feature 5-19
Shared Components: Authentication Schemes 5-20
Multi-Level Authentication 5-25
Road Map 5-27
Policy Object Comparison: OSSO 10g 5-28
Policy Model: Key Differences Between OAM 11g and OSSO 10g 5-29
Policy Model: Key Differences Between OAM 11g and OAM 10g 5-30
Other Policy Features in OAM 11g 5-32
Road Map 5-33
Application Domain: AuthN Policies 5-34
Application Domain: AuthZ Policies 5-36
Resource 5-38
Key URL Patterns 5-40
Authentication Policies 5-42
Authorization Policies 5-44
What Are Responses? 5-46
Responses 5-47
How Are Responses Used? 5-49
Authentication and Authorization Responses 5-50
Response Expressions 5-51
Response Examples 5-52
Response Flows 5-54
Response Providers 5-56
Supported Variable Names Request information 5-58
Supported Variable Names Session information 5-59
Supported Variable Names User information 5-60
Authorization Constraints 5-61
Road Map 5-63
Application Domain 5-64
Conceptual Relationships for Policy Objects 5-65
Summary 5-67
Quiz 5-68
Practice 5 Overview: Protecting Resources by Using Application Domains 5-72

6 Single Sign-On and Session Management

Road Map 6-2
Objectives 6-3
Road Map 6-4
Oracle Access Manager Single Sign-On 6-5
Oracle Access Manager Single Sign-On Scenario 6-6
Oracle Access Manager Single Logout Scenario 6-7

Road Map 6-8
Session and Cookie Creation in Authentication 6-9
Session and Cookie Usage After Successful Authentication 6-12
The OAM Session and the OAM_ID Cookie 6-14
Agent Cookies 6-15
Single Sign-On Cookie Reference 6-16
Cookie and Communication Security 6-20
Session and Cookies in Single Logout 6-22
Quiz 6-24
Road Map 6-27
Session Life Cycle 6-28
Session Timeouts 6-30
Road Map 6-31
Session Caching and Persistence 6-32
Road Map 6-34
Configuring Single Sign-On: Overview 6-35
Road Map 6-36
Default Login Page 6-37
Options for Displaying the Single Sign-On Login Page by Using
Form-Based Authentication 6-38
Configuring an Authentication Scheme for a Customized Login Page 6-41
Customizing Logout 6-42
Road Map 6-44
Configuring Session Management Options 6-45
Managing Sessions 6-46
Road Map 6-47
Windows Native Authentication 6-48
User Validation Replaces Credential Collection 6-49
Configuring an Oracle Access Manager Deployment for WNA 6-50
Quiz 6-52
Summary 6-53
Practice 6 Overview: Examining Single Sign-On and Managing Sessions 6-54

7 Using Oracle Access Manager With WebLogic Applications

Road Map 7-2
Objectives 7-3
Road Map 7-4
Java EE Authentication and Authorization 7-5
Using OAM for Perimeter Authentication and Authorization With a WebGate 7-6
Using OAM for Perimeter Authentication Without a WebGate 7-8
Road Map 7-9

Identity Assertion Providers 7-10
Oracle Access Manager Identity Assertion Provider 7-11
OAM Identity Assertion Provider Event Sequence 7-12
Road Map 7-14
OAM Authenticator 7-15
Quiz 7-16
Summary 7-17
Practice 7 Overview: Using an Identity Assertion Provider 7-18

8 Auditing and Logging

Road Map 8-2
Objectives 8-3
Road Map 8-4
Auditing and Logging: Overview 8-5
Road Map 8-9
The Fusion Middleware Audit Framework 8-10
Road Map 8-12
Audit Output Options 8-13
Audit Architecture Using a Database as the Audit Store 8-14
Deploying Auditing by Using a Database as the Audit Store 8-15
Road Map 8-17
Audit Settings 8-18
Road Map 8-20
Examples of Audited Events 8-21
Examples of Data Recorded When an Audited Event Occurs 8-22
Quiz 8-23
Road Map 8-25
Oracle Business Intelligence Publisher 8-26
Deploying BI Publisher to Support FMW Audit Framework and Oracle Access
Manager Reports 8-27
Generating Oracle BI Publisher Reports 8-28
Navigating to Common User Activities Reports 8-29
Navigating to Oracle Access Manager Reports 8-30
Oracle BI Publisher Reports for Oracle Access Manager 8-31
Road Map 8-33
Administrator Tasks: Logging 8-34
Logging Configuration Objects 8-35
Log Levels 8-37
Oracle Access Manager Loggers and Log Level Inheritance 8-38
Log Handler Settings 8-39
Logging Configuration Tools 8-41

Viewing the Logging Configuration by Using FMW Control	8-42
Modifying Log Level by Using FMW Control	8-43
Creating or Configuring Log Handlers by Using FMW Control	8-44
Using the WLST Tool to Configure Logging	8-45
Road Map	8-50
Locating Log Files	8-51
Viewing and Downloading Log Files by Using FMW Control	8-52
Road Map	8-53
Log Files from Other Servers in an Oracle Access Manager Deployment	8-54
Quiz	8-55
Summary	8-57
Practice 7 Overview: Auditing and Logging	8-58
9 Upgrading Oracle Single Sign-On 10g to Oracle Access Manager 11g	
Objectives	9-2
Overall Sequence	9-3
Retain Ports Versus Change Ports	9-4
Summary of Upgrade Process	9-5
Upgrade OSSO 10g Associated with Oracle Portal	9-6
Verifying a Successful Upgrade	9-10
Scenarios Not Supported for Upgrade to OAM 11g	9-11
Typical OSSO 10g to OAM 11g Upgrade Topology	9-12
Components Involved in an Upgrade	9-14
Upgrade Flow	9-16
Upgrade Assistant	9-17
Post-Upgrade Validation	9-18
Coexistence of OSSO 10g and OAM 11g	9-20
Key Functionality for Coexistence Model	9-22
Coexistence Scenario I: User Authenticated by OAM 11g	9-23
Coexistence Scenario II: User Authenticated by OSSO 10g	9-25
Typical OSSO Server Production Deployment Topology	9-26
Typical Production Deployment Topology	9-27
Rolling Upgrade: Hybrid Configuration	9-28
Upgrade Process	9-30
Interplay of <code>SSO_ID</code> and <code>OAM_ID</code> cookies	9-31
Summary	9-32
Quiz	9-33
Practice 9 Overview: Performing OSSO 10g to OAM 11g Upgrade	9-36

10 Troubleshooting and Management

- Objectives 10-2
- Road Map 10-4
- Access Tester 10-5
- Use Cases: Access Tester 10-6
- Access Tester Simulating Steps 1, 3, 5, 6 of Agent and OAM Server Interaction 10-8
- Access Tester: Core Functionality 10-9
- Access Tester Architecture 10-10
- Output Files and Security Features 10-12
- Starting Access Tester 10-13
- System Properties 10-15
- Access Tester Console 10-18
- Test Cases and Test Scripts 10-20
- Road Map 10-24
- Using `weblogic.Admin` Utility to Check the State of Servers 10-25
- Examining Admin Server and Managed Server Logs 10-26
- WebLogic Admin Server and Managed Server Thread Dump 10-28
- Agent and Server Monitoring 10-30
- OAM Proxy Errors 10-31
- Configuration Data 10-32
- Road Map 10-33
- Top Problem Areas 10-34
- LDAP Server 10-35
- OAM Runtime Servers 10-36
- Agent Side Issues 10-37
- Run-Time DB Issues 10-38
- Admin Change Propagation and Activation 10-39
- Policy Repository DB Issues 10-40
- Road Map 10-41
- WLST Architecture 10-42
- Offline Mode And Online Mode 10-43
- Executing WLST Commands 10-44
- Example: Create Identity Store Embedding WLST Command in Python Script 10-45
- WLST Commands for OAM 11g 10-46
- Road Map 10-49
- Oracle Enterprise Manager Fusion Middleware Control 10-50
- FMW Control: Performance Overview 10-51
- Topology 10-52
- MBean Browser 10-53
- How to Re-register an Agent from the OAM Admin Console 10-54

Summary 10-55
Quiz 10-57
Practice 10 Overview: Working with Access Tester, WLST, and FMW Control 10-61

11 Horizontal Migration

Objectives 11-2
Use Cases: Horizontal Migration 11-3
Perform Horizontal Migration Using WLS Template Builder 11-4
Performing Horizontal Migration by Using WLS Template Builder 11-5
Source and Target Processing 11-6
Policy Migration 11-7
Partner Migration 11-8
Dependencies 11-9
Horizontal Migration Use Cases 11-10
Summary 11-12
Quiz 11-13
Practice 11 Overview: Performing Horizontal Migration 11-15

12 High Availability

Road Map 12-2
Objectives 12-3
Road Map 12-4
High Availability (HA) Goals 12-5
Road Map 12-7
Potential Points of Failure in an Oracle Access Manager Deployment 12-8
Load Balancing on the Web Tier 12-10
Clustering the Oracle Access Manager Server on the Application Tier 12-12
WebLogic Server Cluster 12-13
Configuring a WebLogic Cluster of Oracle Access Manager Servers on
Multiple Hosts 12-15
Converting a Single OAM Server on a Single Host to a Clustered
Configuration 12-17
Handling Administration Server Failure in a Cluster of Oracle Access Manager
Servers 12-20
Data Tier 12-22
Other Issues to Be Aware of in HA Deployments 12-23
Road Map 12-24
Session Replication and Configuration Change Distribution 12-25
User Session Continuity in a Single Oracle Access Manager Server
Environment 12-28

User Session Continuity in a Clustered Oracle Access Manager Server Environment 12-29
Road Map 12-30
Backing up an Oracle Fusion Middleware Deployment 12-31
Recovering Your Environment 12-33
HA Topology Review 12-35
Summary 12-36
Quiz 12-37
Practice 12 Overview: Configuring Oracle Access Manager for HA 12-38

A Introduction to Oracle Access Manager

Oracle Access Manager 11g Comparison with Oracle Access Manager 10g and OSSO 10g A-2
Credential Collection A-7
Kerberos Operation A-8
Coexistence and Backward Compatibility A-9
Request Flow: Authentication A-11
Request Flow: Authorization A-14

B Installation and Configuration

WebLogic JMX: Overview B-2
Navigating JMX MBeans B-4
Node Manager B-6
Node Manager Architecture B-8

C System Configuration: Servers, Data Sources, and Agents

Coherence Properties C-2
Common Server Properties C-3
Backward Compatibility C-9
WLS Agent Without a WebGate C-11

D Policy Configuration: Shared Components and Application Domains

Custom Resource Types D-2
Custom Authenticator Use Case D-4
Fusion Applications SSO Use Case D-5
Creating Custom Resources D-6
Authentication Parity with OAM 10g D-7
OAM 10g Parity Items Features Not Implemented in 11g R1 D-8
Authentication: Troubleshooting Tips D-9
Success and Failure URL D-10
Returning Session or Cookie or HTTP Header Variable D-11

Validating Authentication and Authorization in an Application Domain	D-13
Authentication Module Features	D-14
Shared Components: Authentication Schemes	D-15
E Monitoring OAM 11g by Using Oracle Grid Control	
Objectives	E-2
Enterprise Manager Architecture	E-3
Oracle Enterprise Manager Grid Control Identity Management Pack	E-5
Oracle Identity Management Pack Key Capabilities: Performance Monitoring and Diagnostics	E-7
Oracle Identity Management Pack Key Capabilities: Service Level Management	E-10
Features in the Upcoming Release of Grid Control Comprehensive Monitoring	E-11
Features in the Upcoming Release of Grid Control Integration with FMW Control and WLS Admin Console	E-13
Features in the Upcoming Release of Grid Control Improved Performance Monitoring and Diagnostics	E-14
Grid Control: Home Page	E-15
Identity and Access Targets	E-16
Identity and Access System	E-18
Generic Service	E-19
Discovering Oracle Access Manager	E-20
Create Identity and Access System	E-21
Create Service	E-22
Create a Service Dashboard Report	E-24
Adding or Removing Targets from the System Topology	E-26
Removing Servers or Components from an Existing Identity Management Topology	E-27
Updating Monitoring Configuration	E-28
Alerts Based on Performance and Usage Metrics	E-29
Metric Baselines	E-31
View All Metrics Collected for Oracle Identity Management Target	E-33
View All Metrics for Oracle Access Manager	E-34
Metric and Policy Settings	E-36
Availability	E-37
Service-Level Rules	E-39
Topology	E-41
Service Performance and System Component Status	E-42
Performance Summary for Oracle Access Manager	E-43
Managing Oracle Access Manager and Running Reports	E-44
Alerts and Alert History	E-45

Blackouts E-47
User-Defined Metrics E-50
Summary E-52

F Introduction to Access SDK

Road Map F-2
Objectives F-3
Road Map F-4
Custom Requirements for Authentication and Authorization Services F-5
Road Map F-7
Access SDK F-8
Road Map F-10
Oracle Access Manager Clients F-11
AccessGate Variations F-12
Road Map F-13
Developing and Deploying AccessGates: Overview F-14
Preparing Systems for AccessGate Development and Deployment F-15
Installing Access SDK F-17
Developing the AccessGate F-19
Example of Access SDK API Usage in an AccessGate F-20
Configuring Oracle Access Manager to Support AccessGates F-22
Road Map F-24
Access SDK Support in Oracle Access Manager 11g F-25
Quiz F-26
Summary F-28

G Single Sign-On and Session Management

Intranet Single Sign-On: End-User Experience G-2
Internet Single Sign-On: End-User Experience G-3
Oracle Fusion Middleware 11g R1 Products for Single Sign-On G-5