

Oracle Access Manager: Administration

Volume I • Student Guide

D46987GC10

Edition 1.0

December 2006

D48528

ORACLE®

Author

Shankar Raman

**Technical Contributors
and Reviewers**

Trevor Bowen

Philip Garm

Rohit M Gupta

Robert Lavalie

Yi Lu

Karl Miller

Nagavalli Pataballa

William Prewitt

Sanjay Rallapalli

Editors

Aju Kumar

Richard Wallis

Graphic Designer

Samir Mozumdar

Publishers

Srividya Rameshkumar

Nita Brozowski

Copyright © 2006, Oracle. 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, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Contents

Preface

I 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
- Practices: Overview 1-8

1 Introduction to Oracle Identity and Access Management

- Objectives 1-2
- Enterprise Identity Management 1-3
- What Is Identity Management? 1-4
- Benefits of Identity Management 1-5
- Identity Management: Terminology 1-6
- Identity Management Functionality 1-8
- Overview of Oracle Identity and Access Management Suite 1-9
- Oracle Product Functionality Matrix 1-10
- Directory Services 1-11
- Oracle Internet Directory 1-12
- Oracle Directory Integration Platform 1-13
- Oracle Virtual Directory 1-14
- Identity Administration and Provisioning 1-15
- Oracle Identity Manager 1-16
- Oracle Delegated Administration Services 1-17
- Access Management 1-18
- Oracle Access Manager 1-19
- Oracle Application Server Single Sign-On 1-20
- Oracle Identity Federation 1-21
- Oracle Application Server Infrastructure: Components 1-22
- Summary 1-23

2 Introduction to Oracle Access Manager

- Objectives 2-2

Agenda 2-3
Oracle Access Manager 2-4
Agenda 2-5
Oracle Access Manager Identity System 2-6
Features of the Identity System 2-7
Identity System Applications 2-9
Identity System Applications: Example 2-11
Identity System: Components 2-12
Identity Server 2-13
WebPass 2-14
Identity System Communication Steps 2-15
Communication Between Identity Server and Directory Server 2-16
Communication Between WebPass and Identity Server 2-17
Query Builder 2-18
Agenda 2-19
Oracle Access Manager Access System 2-20
Access System Architecture 2-21
Policy Manager 2-22
Access System Console 2-23
Access Server 2-24
WebGate 2-25
Access System Operation 2-26
Caching 2-27
Auditing the Access System 2-28
Auditing Events 2-29
Agenda 2-30
Authentication Plug-Ins 2-31
Authorization Plug-Ins 2-32
Access Management API 2-33
Identity Event Plug-In API 2-34
IdentityXML 2-35
Presentation Services: Portal Inserts 2-36
PresentationXML 2-37
Summary 2-38
Practice 2 Overview: Exploring and Configuring OracleAS Infrastructure 2-39

3 Installing the Oracle Access Manager Identity System

Objectives 3-2
Oracle Access Manager: Prerequisites 3-3
Preinstallation Tasks with OracleAS Infrastructure on Linux 3-4
Installing the Identity System 3-6

Installing the Identity Server	3-8
Extending the Directory Schema	3-11
Uninstalling the Identity Server	3-12
Installing a WebPass	3-13
Identity System Administrators	3-15
Setting Up the Identity System	3-16
Changing Settings After Installation	3-18
Logging In to the Identity System	3-20
Summary	3-21
Practice 3 Overview: Installing the Identity System	3-22

4 Configuring the Schema Data for the Identity System

Objectives	4-2
Configuring the Identity System	4-3
Identity System Configuration Process: Overview	4-4
Object Classes	4-5
Structural, Auxiliary, and Template Object Classes	4-6
Object Class: Example	4-7
Structural Object Class	4-8
Auxiliary Object Class	4-9
Object Class Types	4-10
Viewing and Modifying Object Classes	4-11
Adding Object Classes to the Identity System	4-12
Selecting the Class Attribute	4-13
Configuring Attributes	4-14
Configuring Attributes: Semantic Type	4-15
Configuring Attributes: Data Type	4-17
Configuring Attributes: Display Type	4-18
Searchable Display Types	4-20
Using Lists to Display	4-21
Using Rules for Display Types	4-22
Object Selector Display Type and Search Filters	4-23
Creating Derived Attributes	4-24
Localizing Attribute Display Names	4-26
Identity System Configuration Process	4-27
Summary	4-28
Practice 4 Overview: Configuring Schema Data for the Identity System	4-29

5 Configuring Tabs, Profile Pages, and Panels

Objectives	5-2
Tabs	5-3

- Configuring Tabs 5-4
- Location Tab 5-5
- Adding a Tab in Organization Manager 5-6
- Configuring Search Attributes on a Tab 5-7
- Adding Auxiliary Classes to a Tab 5-8
- Configuring Group Manager Options 5-9
- Configuring Tab in Group Manager 5-10
- Group Type Panels 5-11
- Profile Page 5-12
- Configuring the Header Panel 5-13
- Configuring the Profile Page 5-14
- Configuring Panels on a Profile Page 5-15
- Summary 5-16
- Practice 5 Overview: Configuring Tabs 5-17

6 Configuring Access Controls in the Identity System

- Objectives 6-2
- Agenda 6-3
- Setting Access Control 6-4
- What Is a Searchbase? 6-5
- Setting a Searchbase 6-6
- Value Substitution in Rules for Searchbase 6-8
- Multiple Searchbases 6-9
- Searchbase Report 6-10
- Agenda 6-11
- Attribute Access 6-12
- Configuring Attribute Access 6-13
- Evaluating Access Control 6-15
- Access Rights Assignment Report 6-16
- Agenda 6-17
- Configuring Reports 6-18
- Viewing Reports 6-20
- Summary 6-21
- Practice 6 Overview: Configuring Access Control for the Identity System 6-22

7 Configuring Workflows

- Objectives 7-2
- What Is a Workflow? 7-3
- Types of Workflows 7-4
- Creating a User Workflow: Example 7-5
- What Is a Subflow? 7-6

Workflow with Subflows	7-7
Creating Workflow Definitions	7-8
Overview of a Workflow Step	7-9
QuickStart Tool	7-11
Creating a Workflow by Using QuickStart	7-12
Creating a Workflow by Using the Workflow Applet	7-13
Using the Workflow Applet: Target Definition	7-14
Variable Targets	7-15
ResourceFilterSearchScope	7-16
Defining Attributes for a Step	7-17
Defining Subsequent Steps	7-18
Creating a Subflow	7-19
Attaching a Subflow to a Workflow	7-20
Defining the Final Step	7-21
Viewing a Summary of the Workflow	7-22
Enabling and Disabling Workflows	7-23
Modifying and Monitoring a Workflow	7-24
Workflow Tickets	7-25
Configuring E-Mail Notification	7-26
Advanced Ticket Routing	7-27
Dynamic Participants	7-28
Specifying Surrogate Participants	7-29
Enabling Surrogate Participants	7-30
Enabling Time-Based Escalation	7-31
Additional Workflow Configurations	7-32
Adding Roles to a Workflow	7-33
Configuring Self-Registration	7-35
Configuring Locations to Show a Map	7-37
Enabling Locations	7-38
Summary	7-39
Practice 7 Overview: Configuring Workflows	7-40
8 Configuring Global Settings for the Identity System	
Objectives	8-2
Password Policies	8-3
Managing Password Policies	8-4
Password Policy for a Domain	8-5
Lost Password Management	8-6
Styles for Identity System Applications	8-8
Configuring Identity Server Settings	8-9
Directory Profiles	8-10

- Configuring WebPass Instances 8-11
- Delegated Identity Administration 8-12
- How to Delegate Administration 8-13
- Delegated Administration Models 8-14
- Extranet-Delegated Administration Model 8-15
- Intranet-Delegated Administration Model 8-16
- ASP-Delegated Administration Model 8-17
- Substitution Rights 8-18
- About Substitution Rights 8-19
- How to Assign and Assume Substitution Rights 8-20
- Summary 8-21
- Practice 8: Overview 8-22

9 Access System Architecture and Installation

- Objectives 9-2
- What Is the Access System? 9-3
- Access System Architecture 9-4
- Access System Applications 9-5
- Access Server 9-6
- Modes of Communication 9-7
- Authentication Steps 9-8
- Steps in Processing User Credentials 9-9
- Authorization Steps 9-11
- Storing User Credentials 9-12
- Auditing for the Access System 9-13
- Auditing Events 9-14
- Web Resource Cache on the WebGate 9-15
- Access Server Caching 9-16
- Authentication Plug-Ins 9-17
- Authorization Plug-Ins 9-18
- Access Server API 9-20
- Access Management API 9-21
- Setting Up the Access System 9-22
- Installing Policy Manager 9-23
- Setting Up the Access System Console 9-25
- Setting Up an Access Server 9-27
- Installing the Access Server 9-28
- Setting Up WebGate or AccessGate 9-30
- Installing WebGate 9-31
- Verifying Installations 9-33

Summary 9-34

Practice 9 Overview: Installing the Access System 9-35

10 Access System Configuration

Objectives 10-2

Access System Administration 10-3

Access System Administrators 10-4

Configuring Master Access Administrators 10-5

Configuring Delegated Access Administrators 10-6

Managing Server Settings 10-7

Configuring the Directory Server 10-8

Access Server Settings 10-9

Auditing: Overview 10-11

Process of Configuring Auditing 10-12

Setting Up the Master Audit Rule 10-13

Enabling Auditing on Access Servers 10-15

Sample Master Audit Rule and Log 10-17

Authentication Scheme 10-18

Creating an Authentication Scheme 10-19

Authentication Plug-Ins 10-21

Configuring Authentication Plug-Ins 10-23

Chained Authentication Schemes 10-24

About Authentication Steps 10-25

Configuring and Managing Steps 10-26

Flows 10-27

Creating Authentication Flow 10-28

Host Identifiers 10-29

Creating a Host Identifier 10-30

Summary 10-31

Practice 10 Overview: Configuring the Access System 10-32

11 Configuring Policy Domains and Policies

Objectives 11-2

Access System: Protecting Resources 11-3

Policy Base, Policy Domain Root, and Policy Domain 11-4

Planning a Policy Domain 11-5

Defining a Policy Domain 11-6

Creating a Policy Domain 11-7

Resource Types 11-8

Creating Resource Types 11-9

URL Prefixes and Patterns 11-10

Planning URL Prefixes	11-11
Adding Resources to a Policy Domain	11-12
Default Rules	11-14
Authentication Schemes	11-15
Default Authentication Rules	11-16
Creating a Default Authentication Rule	11-17
Configuring Authentication Action	11-18
Authorization Schemes, Rules, and Expressions	11-20
Default Audit Rule	11-21
Creating a Default Audit Rule	11-22
Delegating Administration of a Policy Domain	11-23
Policies	11-24
Key URL Patterns	11-25
Creating Policies	11-26
Ordering Policies	11-27
Query Strings	11-28
Summary	11-29
Practice 11 Overview: Configuring Policy Domains	11-30

12 Configuring User Authorization

Objectives	12-2
Authorization Schemes	12-3
Configuring an Authorization Scheme	12-4
Authorization Rules	12-6
Structure of an Authorization Rule	12-7
Creating an Authorization Rule	12-8
Allowing Access	12-9
Specifying the LDAP URL	12-10
Denying Access by Using an Authorization Rule	12-11
Timing Conditions	12-12
Authorization Actions	12-14
Redirection Action	12-15
Returning Cookies or HTTP Header Variables	12-16
Custom Responses and Actions	12-18
Custom Authorization Rules	12-19
Expressions	12-21
Authorization Expressions	12-22
Creating an Authorization Expression	12-24
Authorization Expression Action	12-26
Inconclusive Result	12-27
Duplicate Actions	12-28

- Handling Duplicate Actions 12-29
- Setting Duplicate Handling Behavior 12-30
- Access Tester 12-31
- Access Tester Results 12-32
- Summary 12-33
- Practice 11 Overview: Configuring User Authorization 12-34

13 Managing Access Servers and WebGates

- Objectives 13-2
- Performance and Availability 13-3
- Load Balancing AccessGate Requests 13-4
- Load Balancing: Weighted Round Robin 13-5
- Access Server Failover 13-6
- Configuring Additional Access Servers 13-7
- Creating an Access Server Instance Configuration 13-8
- Modifying Server Settings 13-9
- Removing an Access Server 13-10
- Clustering an Access Server 13-11
- Configuring an Access Server Cluster 13-12
- Adding AccessGates 13-13
- AccessGate Settings 13-14
- Removing AccessGates 13-16
- Directory Server Profiles 13-17
- Configuring a Directory Profile 13-18
- Load Balancing Access Server Requests 13-20
- User Access Configuration 13-21
- Password Cache 13-22
- Summary 13-23

14 Configuring Single Sign-On and Integrating with OracleAS Single Sign-On

- Objectives 14-2
- Single Sign-On: Overview 14-3
- Single Sign-On Cookies 14-4
- Encryption Used for Cookies 14-5
- Generating Shared Secret 14-6
- Single-Domain SSO 14-7
- Configuring SSO for Single Domain 14-8
- Multidomain Single Sign-On 14-10
- Multidomain SSO: Process Flow 14-11
- Configuring the Logout URL 14-12
- OracleAS Single Sign-On: Overview 14-13

Oracle Access Manager: OracleAS Single Sign-On Integration 14-14
Enabling WebGate to Protect OracleAS Single Sign-On Login 14-15
Implementing OracleAS Single Sign-On Authentication Plug-In 14-17
Implementing Global Logout 14-19
Summary 14-20
Practice 14 Overview: Integrating with OracleAS Single Sign-On 14-21

15 Introduction to Oracle Identity Federation

Objectives 15-2
Identity Federation 15-3
Challenges of the Traditional Identity Management Paradigm 15-4
Benefits of Federated Identity Management 15-5
Key Concepts of Federation 15-6
Circle of Trust 15-7
Scenario: Single Sign-On 15-8
Scenario: Federated Partner Site 15-9
Federation Protocols 15-10
Terminology 15-11
Request Response Cycle 15-13
Oracle Identity Federation: Overview 15-14
Oracle Identity Federation: Models 15-15
Oracle Identity Federation Authentication Module 15-16
Deploying Oracle Identity Federation with OracleAS Single Sign-On 15-17
Deploying Oracle Identity Federation with Oracle Access Manager 15-18
Summary 15-19

Appendix A: Practices

Appendix B: Practice Solutions

Appendix C: Description of Workflow Actions

Index