

Oracle® Fusion Middleware

Integration Guide for Oracle Identity Management Suite

11g Release 2 (11.1.2.3.0)

E55996-06

September 2016

Describes how to integrate Oracle Identity Management components.

Copyright © 2012, 2016, Oracle and/or its affiliates. All rights reserved.

Primary Author: Debapriya Datta

Contributors: John Boyer, Damien Carru, Andre Correa, Sidhartha Das, Fabienne Dorson, Yagnesh Gajjar, Daniel Gralewski, Stephen Grenholm, Manish Gulati, Lancer Guo, Tiexin Guo, Lakshmi Hariharan, Achyut Jagtap, Dan Joyce, Rakesh K, Kevin Kessler, Rajesh Kishore, Simon Kissane, Peter LaQuerrie, Wei Jie Lee, Eric Locatelli, Harsh Maheshwari, Tim Melander, Rajesh Pakkath, Nitin Patel, Paulo Pereira, Mehul Poladia, Sanjay Rallapalli, Deepak Ramakrishnan, Loganathan Ramasamy, Rima Rana, Ajit Raskar, Pardha Reddy, Sanjay Sadarangani, Abhimanyu Seth, Kuldeep Shah, Pulkit Sharma, Daniel Shih, Semyon Shulman, Bhupinder Singh, Uppili Srinivasan, Dawn Tyler, Yogaraja Thyagarajan, Rohit Tiwari, Ken Vincent, Ning Wang, Norman Wang, Mark Wilcox, Michele Williams, Haisheng Yu, Amy Yue

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 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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	xix
Audience	xix
Documentation Accessibility	xix
Related Documents	xix
Conventions	xix
What's New	xxi
Updates in October 2016 Documentation Refresh for 11g Release 2 (11.1.2.3.0)	xxi
Updates in July 2016 Documentation Refresh for 11g Release 2 (11.1.2.3.0)	xxi
Updates in January 2016 Documentation Refresh for 11g Release 2 (11.1.2.3.0).....	xxi
Updates in September 2015 Documentation Refresh for 11g Release 2 (11.1.2.3.0).....	xxi
Updates in June 2015 Documentation Refresh for 11g Release 2 (11.1.2.3.0).....	xxi
Updates and New Features for 11g Release 3 (11.1.2.3.0).....	xxii
Updates in February 2014 Documentation Refresh for 11g Release 2 (11.1.2.2.0)	xxii
Updates and New Features for 11g Release 2 (11.1.2.2.0)	xxii
Updates in September 2013 Documentation Refresh for 11g Release 2 (11.1.2.1.0).....	xxii
Updates in July 2013 Documentation Refresh for 11g Release 2 (11.1.2.1.0)	xxiii
Updates in May 2013 Documentation Refresh for 11g Release 2 (11.1.2.1.0)	xxiii
New and Changed Features for 11g Release 2 (11.1.2.1.0)	xxiii
Updates in November 2012 Documentation Refresh for 11g Release 2 (11.1.2).....	xxiii
Updates in August 2012 Documentation Refresh for 11g Release 2 (11.1.2)	xxiii
New and Changed Features for 11g Release 2 (11.1.2)	xxiv
Other Significant Changes in this Document for 11g Release 2 (11.1.2).....	xxiv

Part I IdM Integration Topology

1 Introduction

1.1 Prerequisites to Integration	1-1
1.1.1 Understanding the Installation Roadmap.....	1-1
1.1.2 Understanding Deployment Topologies.....	1-2
1.1.3 About LDAP Synchronization in Oracle Identity Manager	1-2
1.1.3.1 The Identity Store	1-2
1.1.3.2 Integration Between LDAP Identity Store and Oracle Identity Manager.....	1-2
1.1.3.2.1 Configuring the Integration with LDAP.....	1-3
1.1.3.2.2 Provisioning Data From Oracle Identity Manager to LDAP Identity Store .	1-4

1.1.3.2.3	Managing Users.....	1-5
1.1.3.2.4	Managing Roles	1-5
1.1.3.2.5	Reconciliation From LDAP Identity Store to Oracle Identity Manager	1-5
1.1.3.2.6	Consolidated LDAP Sync Full Reconciliation.....	1-6
1.1.4	About Using Oracle Virtual Directory with Access Manager.....	1-9
1.1.5	Common Environment Variables.....	1-9
1.2	Integration Topologies	1-9
1.2.1	Basic Integration Topology	1-9
1.2.1.1	The Three Tier Architecture.....	1-11
1.2.1.2	Understanding the Web Tier	1-11
1.2.1.3	Understanding the Application Tier.....	1-11
1.2.1.4	Understanding the Data Tier	1-12
1.2.2	The Enterprise Integration Topology.....	1-12
1.2.3	Using Multiple Directories for an Identity Store.....	1-12
1.2.4	Integration Terminology.....	1-13
1.3	About Oracle Identity Management Components.....	1-14
1.3.1	Oracle Unified Directory	1-15
1.3.2	Oracle Internet Directory.....	1-15
1.3.3	Oracle Virtual Directory	1-15
1.3.4	Oracle Access Management Access Manager.....	1-15
1.3.4.1	A Note About IDMDomain Agents and Webgates.....	1-16
1.3.5	Oracle Identity Manager.....	1-16
1.3.6	Oracle Adaptive Access Manager	1-16
1.3.7	Oracle Mobile Security Suite	1-17
1.3.8	Oracle Access Management Identity Federation	1-17
1.4	IdM Integration Quick Links.....	1-17
1.5	Common Integration Scenarios	1-18
1.5.1	Resource Protection and Credential Collection Scenarios (OAAM Advanced Integration Using TAP) 1-18	
1.5.1.1	Case 1: The User is Authenticated by Access Manager with Oracle Adaptive Access Manager Performing Step Up Authentication 1-19	
1.5.1.2	Case 2: User is Not Authenticated by Access Manager	1-20
1.5.1.3	Case 3: User is Authenticated by Access Manager and Oracle Adaptive Access Manager Does Not Perform Step Up Authentication 1-21	
1.5.2	Resource Protection and Credential Collection Scenario (OAAM Basic Integration).....	1-21
1.5.3	Password Management Scenarios.....	1-22
1.5.3.1	Access Manager Integrated with Oracle Identity Manager	1-22
1.5.3.2	Self-Registration.....	1-23
1.5.3.3	Password Change	1-24
1.5.3.4	Forgot Password	1-25
1.5.3.5	Account Lock and Unlock	1-27
1.5.3.6	Challenge Setup	1-28
1.5.3.7	Challenge Reset.....	1-29
1.5.4	Manage Mobile Security Accounts and Applications Using Identity Self-Service	1-30
1.6	System Requirements and Certification	1-30
1.7	Using My Oracle Support for Additional Troubleshooting Information.....	1-31

Part II Core Integrations

2 Integrating Access Manager and Oracle Identity Manager

2.1	About Oracle Identity Manager and Access Manager Integration.....	2-1
2.1.1	Integrating Oracle Identity Manager with Access Manager	2-2
2.1.2	Access Manager and Oracle Identity Manager Single-Node Integration Topology .	2-2
2.1.3	Access Manager and Oracle Identity Manager Integration Roadmap	2-2
2.1.4	Access Manager and Oracle Identity Manager Integration Prerequisites.....	2-3
2.2	Configuring LDAP Synchronization.....	2-5
2.3	Configuring the Identity Store	2-5
2.3.1	Extending Directory Schema for Access Manager	2-6
2.3.2	Creating Users and Groups for Access Manager	2-9
2.3.3	Creating Users and Groups for Oracle Identity Manager	2-14
2.3.4	Creating Users and Groups for Oracle WebLogic Server.....	2-17
2.3.5	Creating Readonly user, ReadWrite user and Superuser for Oracle Fusion Applications 2-19	
2.4	Configuring Access Manager for Oracle Identity Manager Integration.....	2-23
2.5	Integrating Access Manager with Oracle Identity Manager	2-27
2.6	Configuring Oracle HTTP Server to Front-End Resources on Oracle Identity Manager.....	2-33
2.7	Deleting the IAMSuiteAgent Security Provider from WebLogic	2-35
2.8	Validating the Integration.....	2-36
2.8.1	Validate Oracle Identity Manager SSOConfig.....	2-36
2.8.2	Validate Security Provider Configuration	2-36
2.8.3	Validate Oracle Identity Manager Domain Credential Store.....	2-37
2.8.4	Validate Event Handlers for SSO	2-38
2.8.5	Validate SSO Logout Configuration	2-38
2.9	Functionally Testing the Access Manager and Oracle Identity Manager Integration...	2-39
2.10	Troubleshooting Common Problems.....	2-40
2.10.1	Single Sign-On Issues	2-40
2.10.1.1	Checking HTTP Headers.....	2-41
2.10.1.2	User is Redirected to Wrong Login Page	2-41
2.10.1.3	Login Fails	2-41
2.10.1.4	Oracle Access Management Console Login Page Does Not Display.....	2-42
2.10.1.5	Authenticated User is Redirected to Oracle Identity Manager Login Page.....	2-42
2.10.1.6	User is Redirected to Oracle Identity Manager Login Page.....	2-43
2.10.1.7	New User is Not Redirected to Change Password	2-45
2.10.1.8	User is Redirected in a Loop	2-45
2.10.2	Auto-Login Issues.....	2-46
2.10.2.1	TAP Protocol Issues.....	2-46
2.10.2.1.1	404 Not Found Error	2-46
2.10.2.1.2	System Error.....	2-47
2.10.2.2	Oracle Access Protocol (OAP) Issues.....	2-48
2.10.3	Session Termination Issues	2-50
2.10.4	Account Self-Locking Issues	2-51
2.10.5	Miscellaneous Issues	2-53
2.10.5.1	Client Based Login to Oracle Identity Manager Fails	2-53

2.10.5.2	Logout Throws 404 Error	2-54
2.10.5.3	Old Password Still Works After a Password Reset	2-54
2.10.5.4	ConfigOIM Failed While Seeding Oracle Identity Manager Policies into Access Manager	2-54

3 Integrating Access Manager, OAAM, and OIM

3.1	About Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager Integration	3-1
3.1.1	Deployment Options for Strong Authentication.....	3-2
3.1.2	Deployment Options for Password Management	3-3
3.2	Definitions, Acronyms, and Abbreviations	3-4
3.3	Integration Roadmap.....	3-11
3.4	Integration Prerequisites.....	3-11
3.5	Integrating Access Manager and Oracle Identity Manager	3-14
3.6	Enabling LDAP Synchronization for Oracle Identity Manager	3-14
3.7	Integrating Access Manager and Oracle Adaptive Access Manager	3-14
3.8	Integrating Oracle Identity Manager and Oracle Adaptive Access Manager.....	3-16
3.8.1	Setting Oracle Identity Manager Properties for Oracle Adaptive Access Manager	3-16
3.8.2	Updating OAAM Properties to Enable Integration Between Oracle Identity Manager and OAAM	3-17
3.8.3	Configuring Oracle Identity Manager Credentials in the Credential Store Framework	3-20
3.8.4	Configuring Cross Domain Trust Between Oracle Identity Manager and Oracle Adaptive Access Manager	3-21
3.9	Performing Additional Configuration Depending on Deployment	3-22
3.9.1	Adding the -Djava.security.auth.login.config JAVA System Property if Using JDK 7	3-22
3.9.2	Changing the Authentication Scheme to TAPScheme for Upgrade of Oracle Identity Manager	3-22
3.9.3	Changing the Authentication Scheme to TAPScheme After Moving from a Test to a Production Environment	3-23
3.10	Troubleshooting Common Problems.....	3-24
3.10.1	User Encounters a Non-Working URL.....	3-24
3.10.2	User is Redirected in a Loop After User Enters Wrong Password.....	3-24
3.10.3	User is Redirected to an Oracle Identity Manager Page	3-25
3.10.4	Successful Authentication Creates Two User Sessions	3-25
3.10.5	OAAM Test Login URL Fails After Access Manager and OAAM Integration	3-25
3.10.6	Initialization Error Occurs When the User Resets the User Password	3-25

4 Configuring SSL for Integrated IdM Components

4.1	About SSL for Integrated IdM	4-1
4.1.1	Assumptions about Integrated IdM Environment	4-1
4.1.2	Roadmap for End-to-End IdM SSL	4-2
4.2	Configuring SSL on Servers in the OAM Domain	4-2
4.3	Configuring SSL for Oracle Identity Manager.....	4-3
4.3.1	Generating Keys.....	4-4
4.3.2	Signing the Certificates	4-5
4.3.3	Exporting the Certificate.....	4-5

4.3.4	Importing the Certificate	4-5
4.3.5	Enabling SSL for Oracle Identity Manager and SOA Servers	4-6
4.3.5.1	Enabling SSL for Oracle Identity Manager	4-6
4.3.5.2	Changing Front End URLs using MBeans.....	4-9
4.3.5.3	Changing SOA Server URL to Use SSL Port	4-10
4.3.5.4	Configuring SSL for Oracle Identity Manager Utilities	4-11
4.4	Configuring SSL on Servers in the OAAM Domain	4-13
4.5	Configuring SSL for Oracle Unified Directory	4-14
4.6	Configuring SSL for Oracle HTTP Server	4-17
4.7	Securing IdM Components against the Poodle Vulnerability	4-17
4.7.1	Configuring OAM and OIM Domains with the TLSv1 Protocol.....	4-17
4.7.2	Configuring OUD with the TLSv1 Protocol	4-18
4.7.3	Configuring OHS with the TLSv1 Protocol	4-18
4.8	Completing SSL Configuration for Integrated IdM.....	4-18

5 Integrating Oracle Mobile Security Suite and Oracle Identity Manager

5.1	About the Oracle Mobile Security Suite and Oracle Identity Manager Integration	5-1
5.2	Oracle Mobile Security Suite and Oracle Identity Manager Integrated Architecture	5-2
5.3	Integrating Oracle Mobile Security Suite and Oracle Identity Manager	5-3
5.3.1	Oracle Mobile Security Suite and Oracle Identity Manager Integration Roadmap...	5-3
5.3.2	Oracle Mobile Security Suite and Oracle Identity Manager Integration Prerequisites	5-3
5.3.3	Setting Up Trust Between Oracle Mobile Security Suite and Oracle Identity Manager Domains	5-4
5.3.4	Wiring Oracle Mobile Security Manager and Oracle Identity Manager	5-6
5.4	Configuring Administrators for Oracle Identity Manager and Mobile Security Suite Administration	5-7
5.4.1	Setting Up Administrators	5-7
5.4.2	Configuring Help Desk Users.....	5-9
5.5	Integrating Oracle Mobile Security Suite in Upgrade Scenarios	5-10
5.6	Viewing Oracle Mobile Security Manager Console Pages in the Oracle Identity Manager Console	5-12

Part III External SSO Solutions

6 Integrating with Identity Federation

6.1	Background and Integration Overview	6-1
6.1.1	About Oracle Access Management Identity Federation	6-1
6.1.2	Deployment Options for Identity Federation.....	6-1
6.1.3	References	6-2
6.2	Integration with Access Manager 11gR2.....	6-2
6.2.1	Architecture	6-3
6.2.2	Overview of Integration Tasks	6-4
6.2.3	Prerequisites	6-4
6.2.4	Additional Setup	6-4
6.2.5	Register Oracle HTTP Server with Access Manager	6-5
6.2.6	Configure Oracle Identity Federation.....	6-5

6.2.6.1	Verify the User Data Store.....	6-6
6.2.6.2	Configure Oracle Identity Federation Authentication Engine	6-6
6.2.6.3	Configure Oracle Identity Federation SP Integration Module	6-7
6.2.7	Configure Access Manager	6-7
6.2.7.1	Configure OIFScheme.....	6-8
6.2.7.2	Register Oracle Identity Federation as a Trusted Access Manager Partner	6-8
6.2.7.2.1	Register Oracle Identity Federation for Use in SP Mode.....	6-8
6.2.7.2.2	Register Oracle Identity Federation for Use in Authentication Mode	6-9
6.2.8	Protecting a Resource with OIFScheme	6-9
6.2.9	Test the Configuration	6-9
6.2.9.1	Test SP Mode Configuration.....	6-9
6.2.9.2	Test Authentication Mode Configuration.....	6-10
6.3	Scripts for Integration Tasks.....	6-10
6.3.1	Perform the Preliminary Procedure.....	6-10
6.3.2	Additional Setup	6-11
6.3.3	Execute the Automated Procedure	6-11
6.3.3.1	Scope of the Automated Process	6-11
6.3.3.2	Copy the Scripts to the Access Manager Machine.....	6-11
6.3.3.3	Understand the inputs to the Scripts	6-12
6.3.3.4	Run the Scripts	6-12

Part IV Additional Identity Store Configuration

7 Configuring an Identity Store with Multiple Directories

7.1	Overview of Configuring Multiple Directories as an Identity Store.....	7-1
7.2	Configuring Multiple Directories as an Identity Store: Split Profile.....	7-2
7.2.1	Prerequisites	7-2
7.2.2	Repository Descriptions.....	7-3
7.2.3	Setting Up Oracle Internet Directory as a Shadow Directory	7-3
7.2.4	Directory Structure Overview - Shadow Join.....	7-4
7.2.5	Configuring Oracle Virtual Directory Adapters for Split Profile	7-6
7.2.6	Configuring a Global Consolidated Changelog Plug-in.....	7-7
7.2.7	Validating the Oracle Virtual Directory Changelog.....	7-8
7.3	Configuring Multiple Directories as an Identity Store: Distinct User and Group Populations in Multiple Directories	7-8
7.3.1	Directory Structure Overview for Distinct User and Group Populations in Multiple Directories	7-9
7.3.2	Configuring Oracle Virtual Directory Adapters for Distinct User and Group Populations in Multiple Directories	7-11
7.3.2.1	Create Enterprise Directory Adapters.....	7-11
7.3.2.2	Create Application Directory Adapters	7-13
7.3.3	Creating a Global Plug-in	7-15
7.4	Additional Configuration Tasks.....	7-15

Part V Appendices

A Verifying Adapters for Multiple Directory Identity Stores by Using ODSM

A.1	Verifying Oracle Virtual Directory Adapters for Split Profile by Using ODSM	A-1
A.1.1	Verifying User Adapter for Active Directory Server.....	A-1
A.1.2	Verifying Shadowjoiner User Adapter.....	A-2
A.1.3	Verifying JoinView Adapter	A-3
A.1.4	Verifying User/Role Adapter for Oracle Internet Directory	A-3
A.1.5	Verifying Changelog adapter for Active Directory Server.....	A-4
A.1.6	Verifying Changelog Adapter for Oracle Internet Directory	A-5
A.1.7	Configuring a Global Consolidated Changelog Plug-in.....	A-6
A.1.8	Validate Oracle Virtual Directory Changelog	A-6
A.2	Verifying Adapters for Distinct User and Group Populations in Multiple Directories by Using ODSM	A-6
A.2.1	User/Role Adapter A1.....	A-7
A.2.2	User/Role Adapter A2.....	A-7
A.2.3	Changelog Adapter C1	A-8
A.2.4	Changelog Adapter for Active Directory	A-8
A.2.5	Changelog Adapter C2	A-9
A.2.6	Verifying Oracle Virtual Directory Global Plug-in.....	A-10
A.2.7	Configuring a Global Consolidated Changelog Plug-in.....	A-10

B The idm.conf File

B.1	About the idm.conf File	B-1
B.1.1	The Default Access Zone	B-1
B.1.2	The External Access Zone.....	B-2
B.1.3	The Internal Services Zone	B-2
B.1.4	The Administrative Services Zone	B-2
B.2	Example idm.conf File.....	B-2

C Integrating Oracle Adaptive Access Manager with Access Manager

C.1	About Access Manager and Oracle Adaptive Access Manager Integration.....	C-2
C.2	Definitions, Acronyms, and Abbreviations	C-4
C.3	OAAM Basic Integration with Access Manager.....	C-11
C.3.1	Prerequisites for OAAM Basic Integration with Access Manager	C-12
C.3.2	Starting the Administration Server and Access Manager Managed Server	C-12
C.3.3	Configuring OAAM Basic Integration with Access Manager.....	C-12
C.4	OAAM Advanced Integration with Access Manager	C-17
C.4.1	Roadmap for OAAM Advanced Integration with Access Manager.....	C-17
C.4.2	Prerequisites for OAAM Advanced Integration with Access Manager	C-18
C.4.3	Restarting the Servers	C-20
C.4.4	Creating the OAAM Users and OAAM Groups	C-20
C.4.5	Importing the Oracle Adaptive Access Manager Snapshot	C-22
C.4.6	Validating Initial Configuration of Access Manager.....	C-23
C.4.7	Validating Initial Configuration of Oracle Adaptive Access Manager.....	C-23
C.4.8	Registering the WebGate with Access Manager 11g Using the Oracle Access Management Console	C-23
C.4.8.1	Prerequisites for WebGate Registration	C-24

C.4.8.2	Configure Oracle HTTP Server with WebGate	C-24
C.4.8.3	Register the WebGate as a Partner with Access Manager 11g Using the Oracle Access Management Console C-25	
C.4.8.4	Restarting the Oracle HTTP Server WebGate	C-25
C.4.8.5	Validating the WebGate Setup	C-25
C.4.9	Registering the OAAM Server as a Partner Application to Access Manager	C-26
C.4.10	Adding an Agent Password to the IAMSuiteAgent Profile	C-27
C.4.11	Updating the Domain Agent Definition If Using Domain Agent for IDM Domain Consoles C-28	
C.4.12	Verifying TAP Partner Registration.....	C-29
C.4.12.1	Verifying the Challenge URL.....	C-29
C.4.12.2	Adding the MatchLDAPAttribute Challenge Parameter in the TAPScheme ..	C-29
C.4.12.3	Validating the IAMSuiteAgent Setup	C-30
C.4.13	Setting Up Access Manager TAP Integration Properties in OAAM	C-31
C.4.14	Configuring the Integration to Use TAPScheme to Protect Identity Management Resources in the IAMSuiteAgent Application Domain C-34	
C.4.15	Configuring a Resource to be Protected with TAPScheme	C-35
C.4.15.1	Creating a New Resource under the Application Domain	C-35
C.4.15.2	Creating a New Authentication Policy that Uses TAPScheme to Protect the Resource C-36	
C.4.16	Validating the Access Manager and Oracle Adaptive Access Manager Integration.....	C-37
C.5	Access Manager and OAAM TAP Integration with DCC WebGate Using Tunneling .	C-37
C.5.1	Roadmap for Access Manager and OAAM TAP Integration with DCC WebGate	C-38
C.5.2	Integrating Access Manager with OAAM using TAP integration	C-38
C.5.3	Setting Up a DCC WebGate and Enabling Tunneling	C-38
C.5.4	Configuring Resources in the Application Domain of the DCC WebGate	C-39
C.5.5	Editing the TAP Authentication Scheme to Use the DCC WebGate.....	C-39
C.5.6	Configure an Authentication Scheme to Use the DCC WebGate (Optional)	C-40
C.6	Other Access Manager and OAAM Integration Configuration Tasks.....	C-40
C.6.1	Changing the Authentication Level of the TAPScheme Authentication Scheme ...	C-40
C.6.2	Setting Up Oracle Adaptive Access Manager and Access Manager Integration When Access Manager is in Simple Mode C-41	
C.6.2.1	Configuring Simple Mode Communication with Access Manager	C-41
C.6.2.2	Setting OAAM Properties for Access Manager for Simple Mode.....	C-41
C.6.3	Configuring Identity Context Claims in the Access Manager and OAAM TAP Integration C-42	
C.6.4	Enabling Oracle Adaptive Access Manager to Transfer Data to Access Manager over HTTP Post-Based Front Channel C-43	
C.6.5	Disabling OAAM Administration Console Protection	C-44
C.6.6	Disabling Step Up Authentication	C-44
C.6.7	Changing the Oracle Adaptive Access Manager Password Length Limit.....	C-44
C.6.8	Adding Customizations Using the OAAM Extensions Shared Library	C-45
C.6.9	Enabling the Single Login Page Flow	C-45
C.7	Resource Protection Scenario	C-45
C.7.1	Resource Protection Scenario: Changing Authentication Level of TAPScheme	C-45
C.7.2	Resource Protection Scenario: Removing OAAM Administration Console from Protected Higher Level Policy C-46	

C.7.3	Resource Protection Scenario: Creating a New Policy that Uses TAPScheme to Protect the Resource	C-47
C.7.4	Resource Protection Scenario: Creating a New OAAM User	C-47
C.7.5	Resource Protection Scenario: Login Flow.....	C-47
C.7.6	Resource Protection Scenario: Step Up Authentication Flow	C-50
C.8	Troubleshooting Common Problems.....	C-52
C.8.1	OAAM Basic Integration with Access Manager	C-52
C.8.1.1	Internet Explorer 7 and OAAM Basic Integration with Access Manager	C-52
C.8.1.2	Access Manager and Oracle Adaptive Access Manager Integration and Changes in the Console	C-53
C.8.1.3	OTP Challenge Not Supported in OAAM Basic integration with Access Manager ..	C-53
C.8.1.4	Using ConfigureOAAM WLST Command to Create the Data Source in OAAM Basic Integration with Access Manager	C-54
C.8.2	Login Failure	C-54
C.8.2.1	Login Page Does Not Display Error	C-54
C.8.2.2	Non-ASCII Credentials.....	C-55
C.8.2.3	Mixed Case Logins	C-55
C.8.2.4	Cookie Domain Definition	C-56
C.8.2.5	OAAM Test Login URL /oaam_server Fails After Access Manager and Oracle Adaptive Access Manager Integration	C-56
C.8.2.6	Login to a Protected Resource May Fail in an Access Manager Release 2 PS2 and Oracle Adaptive Access Manager Release 2 TAP Integrated Environment	C-56
C.8.3	Identity Store	C-57
C.8.3.1	Username Attribute Incorrect Setting.....	C-57
C.8.3.2	In the Access Manager and Oracle Adaptive Access Manager Integration TAP Could Not Modify User Attribute	C-57
C.8.3.3	No Synchronization Between Database and LDAP	C-58
C.8.4	Miscellaneous	C-58
C.8.4.1	Multiple Sessions Created for a Particular User Instead of a Unified Session .	C-58
C.8.4.2	Integration Failure Due to Network Delay.....	C-58
C.8.4.3	Changing the TAP Token Version to 2.1.....	C-59
C.8.4.4	Resource Protected by OAAMAdvanced Scheme Is Not Accessible in Access Manager 11.1.1.4.0 and OAAM 11.1.1.5.0 Integration	C-60
C.8.4.5	Additional Properties to Set If Using OAAMAdvanced Scheme.....	C-61
C.8.4.6	Accessing LDAP Protected Resource as a Test	C-61

D Using the idmConfigTool Command

D.1	About idmConfigTool.....	D-1
D.1.1	Components Supported by idmConfigTool	D-1
D.1.2	When to Use the Tool.....	D-2
D.1.3	Tasks performed by the Tool	D-2
D.1.4	Location of idmConfigTool	D-2
D.1.5	Webgate Types Supported	D-3
D.1.6	Single- and Cross-Domain Scenarios.....	D-3
D.2	Set Up Environment Variables.....	D-3
D.3	Syntax and Usage.....	D-4
D.3.1	Command Syntax	D-4

D.3.2	Requirements.....	D-5
D.3.3	Generated Files.....	D-6
D.3.4	Using the Properties File.....	D-6
D.3.4.1	About the properties File.....	D-6
D.3.4.2	List of Properties	D-6
D.3.5	Working with the idmConfigTool Log File	D-15
D.3.5.1	Searching the idmConfigTool Log File.....	D-16
D.3.5.2	Maintaining the idmConfigTool Log File	D-16
D.4	Command Options and Properties	D-16
D.4.1	preConfigIDStore Command	D-17
D.4.2	prepareIDStore Command	D-19
D.4.2.1	prepareIDStore mode=OAM	D-19
D.4.2.2	prepareIDStore mode=OIM.....	D-21
D.4.2.3	prepareIDStore mode=OAAM.....	D-23
D.4.2.4	prepareIDStore mode=WLS.....	D-24
D.4.2.5	prepareIDStore mode=WAS	D-26
D.4.2.6	prepareIDStore mode=APM.....	D-28
D.4.2.7	prepareIDStore mode=fusion	D-29
D.4.2.8	prepareIDStore mode=all.....	D-30
D.4.3	configPolicyStore Command	D-32
D.4.4	configOAM Command	D-33
D.4.5	configOIM Command	D-38
D.4.6	configOMSS Command	D-43
D.4.7	postProvConfig Command	D-45
D.4.8	upgradeLDAPUsersForSSO Command	D-46
D.4.9	validate IDStore Command.....	D-47
D.4.10	validate PolicyStore Command	D-48
D.4.11	validate OAM Command (11g)	D-49
D.4.12	validate OAM Command (10g)	D-50
D.4.13	validate OIM command	D-50
D.4.14	configOVD Command	D-51
D.4.15	ovdConfigUpgrade Command.....	D-53
D.4.16	disableOVDAccessConfig Command.....	D-53
D.4.17	upgradeOIMTo11gWebgate	D-54
D.5	Additional Tasks for OUD Identity Store in an HA Environment.....	D-54
D.5.1	Creating the Global ACI for Oracle Unified Directory	D-54
D.5.2	Creating Indexes on Oracle Unified Directory Replicas	D-57

E Enabling LDAP Synchronization in Oracle Identity Manager

E.1	Configuring LDAP Synchronization.....	E-1
E.1.1	Completing the Prerequisites for Enabling LDAP Synchronization.....	E-2
E.1.1.1	Preconfiguring Active Directory	E-4
E.1.1.2	Preconfiguring ODSEE	E-6
E.1.2	Configuring Changelog in OUD	E-10
E.1.3	Creating OVD Adapters	E-13
E.1.3.1	Creating Oracle Virtual Directory Adapters for Oracle Internet Directory and Active Directory	E-13

E.1.3.2	Creating Identity Virtualization Library (libOVD) Adapters and Integrating With Oracle Identity Manager	E-15
E.1.4	Enabling LDAP Synchronization	E-18
E.1.4.1	Modifying the MDS	E-18
E.1.4.2	Modifying the IT Resource	E-20
E.1.4.3	Seeding Reconciliation Jobs	E-21
E.1.4.4	Reverting from OVD to libOVD in LDAPSvc	E-23
E.2	Managing LDAP Synchronization	E-23
E.2.1	Running the LDAP Post-Configuration Utility	E-24
E.2.2	Verifying the LDAP Synchronization	E-28
E.2.3	Customizing and Filtering Users	E-28
E.2.3.1	Customizing User Creation Through Oracle Identity Manager With Different Custom Object Classes	E-28
E.2.3.2	Creating Users in Oracle Identity Manager and Not in LDAP When LDAP Synchronization is Enabled	E-30
E.2.4	Configuring LDAP Sync Using Plug-ins	E-31
E.2.4.1	Using the UserManagement Plug-In	E-31
E.2.4.1.1	Configuration Parameters	E-31
E.2.4.2	Using the Changelog Plug-In	E-33
E.2.4.2.1	Deploying the Release 11.1.1.4.0 Changelog Plug-In	E-33
E.2.4.2.2	Deploying Changelog Plug-Ins from Prior Releases	E-33
E.2.4.2.3	Configuration Parameters	E-34
E.2.5	Troubleshooting and Debugging OVD	E-36
E.2.6	Filtering Data in Incremental Reconciliation	E-37
E.2.7	Enabling SSL Between Identity Virtualization Library (libOVD) and the Directory Server	E-38
E.2.7.1	Enabling SSL Between Identity Virtualization Library (libOVD) and Microsoft Active Directory	E-38
E.2.7.2	Enabling SSL Between Identity Virtualization Library (libOVD) and iPlanet	E-39
E.2.7.3	Enabling SSL Between Identity Virtualization Library (libOVD) and OID	E-39
E.2.8	Provisioning Users and Roles Created Before Enabling LDAP Synchronization to LDAP	E-40
E.2.9	Disabling LDAP Synchronization	E-40
E.2.10	Managing Identity Virtualization Library (libOVD) Adapters	E-40
E.2.11	Enabling Access Logging for Identity Virtualization Library (libOVD)	E-43
E.2.12	Configuring LDAP Authentication When LDAP Synchronization is Enabled	E-43
E.2.13	Verifying the Value of pwdLockout in the Directory Password Policy	E-45
E.2.14	Fixing Permission Errors with OUD ACIs	E-45
E.2.14.1	Checking and Fixing ACIs With lastExternalChangelogCookie for OUD	E-45
E.2.14.2	Fixing External Changelog Cookie Expiration Issue When Performing Reconciliation with OUD	E-46
E.2.15	Disabling the LDAPAddMissingObjectClasses for Users and Roles	E-46
E.2.16	Setting Up LDAP Synchronization With HA Multi-Master Replication (MMR)	E-47

F Configuring Oracle Virtual Directory for Integration with Oracle Access Management Access Manager

F.1	Creating and Configuring Oracle Virtual Directory Adapters	F-1
F.1.1	Creating and Configuring an LDAP Adapter	F-2

F.1.1.1	Creating an LDAP Adapter.....	F-2
F.1.1.2	Configuring an LDAP Adapter	F-2
F.1.1.2.1	Configuring LDAP Adapter General Settings	F-2
F.1.1.2.2	Managing Certificate Authorities for LDAP Adapters Secured by SSL.....	F-9
F.1.2	Creating and Configuring a Database Adapter	F-10
F.1.2.1	Creating a Database Adapter	F-10
F.1.2.2	Configuring a Database Adapter	F-10
F.1.3	Creating and Configuring a Custom Adapter.....	F-12
F.1.3.1	Creating a Custom Adapter	F-12
F.1.3.2	Configuring Custom Adapters.....	F-12
F.2	Using the OAMPolicyControl Plug-In with Oracle Access Manager 10g.....	F-13
F.2.1	Configuration Parameters	F-14

Index

List of Figures

1-1	Oracle Identity Manager and LDAP	1-3
1-2	Basic Integration Topology with Multiple Administration Servers	1-10
1-3	Resource Protection and Credential Collection Flow	1-19
1-4	Integrating Access Manager and Oracle Identity Manager for Password Management	1-22
5-1	Logical Diagram Showing Oracle Identity Manager integrated with Oracle Mobile Security Suite 5-2	
6-1	Access Manager with Identity Federation	6-3
7-1	Directory Structure	7-4
7-2	Client View of the DIT	7-5
7-3	Adapter and Plug-in Configuration	7-5
7-4	Directory Structure	7-9
7-5	Client View of the DIT	7-10
7-6	Configuration Overview	7-10
C-1	Access Management User Name Page.....	C-48
C-2	Password Page with TextPad.....	C-48
C-3	Register Profile	C-48
C-4	Security Device Selection	C-49
C-5	Challenge Question Registration.....	C-49
C-6	OAAM Administration Console Cases Page: Accessing the Protected Resource.....	C-50
C-7	Access Management Login: Logging In to the Lower Risk Resource.....	C-50
C-8	Step Up Authentication: Log In to the Higher Protected Resource.....	C-51
C-9	Higher Protected Resource	C-52
C-10	TAPScheme Authentication Scheme.....	C-59

List of Tables

1-1	Oracle Fusion Middleware Integration Terminology.....	1-13
1-2	Links to Integration Procedures in This Guide	1-17
1-3	Links to Integration Procedures in Other Guides.....	1-18
2-1	Integration Flow for Access Manager and Oracle Identity Manager.....	2-3
2-2	Required Components for Integration Scenario.....	2-4
2-3	extendOAMPropertyFile Properties	2-7
2-4	preconfigOAMPropertyFile Properties	2-11
2-5	preconfigOIMPropertyFile Properties	2-15
2-6	preconfigWLSPropertyFile Properties.....	2-18
2-7	preconfigFAPropertyFile Properties.....	2-21
2-8	OAMconfigPropertyFile Properties File.....	2-24
2-9	OIMconfigPropertyFile Properties	2-29
2-10	Verifying Access Manager and Oracle Identity Manager Integration.....	2-39
3-1	Responsibilities for Each Component in Integration.....	3-2
3-2	Advanced Integration Terms	3-4
3-3	Integration Flow for Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager 3-11	
3-4	Access Manager, OAAM, and OIM Integration Required Components.....	3-12
3-5	Integration Flow for Access Manager and Oracle Adaptive Access Manager	3-15
3-6	Oracle Identity Manager Redirection.....	3-17
3-7	Configuring Oracle Identity Manager Property Values.....	3-18
3-8	Oracle Identity Manager Credentials.....	3-21
4-1	Roadmap for End-to-end IdM SSL.....	4-2
5-1	Setting Up Oracle Mobile Security Suite with Identity Manager	5-3
5-2	Required Components and Environment Configurations.....	5-4
5-3	Oracle Mobile Security Suite Screens.....	5-12
6-1	Deployment Options involving Oracle Access Manager.....	6-2
6-2	Inputs for the OAM-OIF 11gR1 Integration Scripts.....	6-12
A-1	Values in Parameters Table	A-8
A-2	Values in Parameters Table	A-9
B-1	Zones in the idm.conf File	B-1
C-1	Types of Access Manager and Oracle Adaptive Access Manager Integration.....	C-3
C-2	OAAM and Access Manager Integration Terms.....	C-5
C-3	Required Components for Integration.....	C-12
C-4	Roadmap for OAAM Advanced Integration with Access Manager	C-17
C-5	Required Components for Integration.....	C-19
C-6	TAP Partner Registration Parameters.....	C-27
C-7	OAAM CLI Properties.....	C-32
C-8	Integration for Access Manager and Oracle Adaptive Access Manager Using TAP with DCC C-38	
C-9	DCC WebGate Agent Profile Changes	C-39
C-10	Properties for Security Mode	C-42
D-1	Environment Variables for IdM Configuration Tool (idmConfigTool).....	D-3
D-2	Properties Used in IdMConfigtool properties Files.....	D-6
D-3	Properties of preConfigIDStore	D-17
D-4	prepareIDStore mode=OAM Properties	D-20
D-5	prepareIDStore mode=OIM Properties	D-22
D-6	prepareIDStore mode=OAAM Properties	D-23
D-7	prepareIDStore mode=WLS Properties.....	D-25
D-8	prepareIDStore mode=WAS Properties	D-27
D-9	prepareIDStore mode=APM Properties	D-28
D-10	prepareIDStore mode=fusion Properties	D-29
D-11	prepareIDStore mode=all Properties	D-30

D-12	Properties for ConfigPolicyStore	D-32
D-13	Properties of configOAM.....	D-33
D-14	Properties for configOIM.....	D-39
D-15	Properties for configOMSS	D-43
D-16	Properties for upgradeLDAPUsersForSSO	D-46
D-17	Properties for validate IDStore	D-47
D-18	Properties for validate polycystore	D-48
D-19	Properties for validate component=OAM11g	D-49
D-20	Properties for validate component=OAM10g	D-50
D-21	Properties for validate component=OIM11g	D-51
D-22	configOVD properties	D-51
D-23	ovdConfigUpgrade Properties.....	D-53
D-24	disableOVDAccessConfig Properties.....	D-54
E-1	Identity Virtualization Library (libOVD) Adapter Configuration Files	E-15
E-2	Parameters of the Property File	E-22
E-3	Parameters of the ldapconfig.props File.....	E-26
F-1	Properties in the krb5.conf File	F-5

Preface

This guide describes how you can integrate certain components in the Oracle Identity Management suite to provide a broad range of solutions for application environment including: integration with LDAP repositories, identity and access management, advanced login and password security, and identity federation.

Audience

This document is intended for administrators who wish to integrate Oracle Identity Management components using a simple topology without high availability features.

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 following documents in the documentation set:

- *Enterprise Deployment Guide for Oracle Identity and Access Management*
- *Administrator's Guide for Oracle Access Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
- *Oracle Fusion Middleware Third-Party Application Server Guide for Oracle Identity and 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.
<i>italic</i>	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

This preface provides a summary of new features and updates to Oracle Identity Management suite integration.

Updates in October 2016 Documentation Refresh for 11g Release 2 (11.1.2.3.0)

This revision of the *Integration Guide for Oracle Identity Management Suite* contains bug fixes and editorial corrections.

Updates in July 2016 Documentation Refresh for 11g Release 2 (11.1.2.3.0)

This revision of the *Integration Guide for Oracle Identity Management Suite* contains bug fixes and editorial corrections. Of particular interest:

- Added new section for configuring changelog in OUD.

See [Section E.1.2](#) for details.

Updates in January 2016 Documentation Refresh for 11g Release 2 (11.1.2.3.0)

This revision of the *Integration Guide for Oracle Identity Management Suite* contains bug fixes and editorial corrections. Of particular interest:

- Updated procedure to configure SSL on servers in the OAM domain.

See [Section 4.2](#) for details.

Updates in September 2015 Documentation Refresh for 11g Release 2 (11.1.2.3.0)

This revision of the *Integration Guide for Oracle Identity Management Suite* contains bug fixes and editorial corrections.

Updates in June 2015 Documentation Refresh for 11g Release 2 (11.1.2.3.0)

This revision of the *Integration Guide for Oracle Identity Management Suite* contains bug fixes and editorial corrections.

Updates and New Features for 11g Release 3 (11.1.2.3.0)

The *Integration Guide for Oracle Identity Management Suite* contains these new features:

- New `idmConfigTool` command option `configOMSS`.
For details, see [Section D.4.6](#).
- End-to-end SSL configuration for Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager.
For details, see [Chapter 4](#).
- Integrating Oracle Mobile Security Suite. For details, see [Chapter 5, "Integrating Oracle Mobile Security Suite and Oracle Identity Manager."](#)
- Steps in integrating Oracle Adaptive Access Manager with Oracle Access Management Access Manager revised for the updated and streamlined Oracle Access Management Console. For details, see [Appendix C, "Integrating Oracle Adaptive Access Manager with Access Manager"](#).

The following additional updates have been made to this document:

- Bugfixes and other corrections have been applied;
- the chapter for Oracle Identity Navigator is removed;
- Links have been added to key integration procedures that reside in other documents.

For details, see [Table 1-3](#).

Updates in February 2014 Documentation Refresh for 11g Release 2 (11.1.2.2.0)

This revision of the *Integration Guide for Oracle Identity Management Suite* contains bug fixes and editorial corrections.

Updates and New Features for 11g Release 2 (11.1.2.2.0)

The *Integration Guide for Oracle Identity Management Suite* contains these updates:

- Clarifications for use of `idmConfigTool` in an Oracle Unified Directory environment; changes to input parameters for some options.
For details, see [Appendix D](#).
- Added support for IdP mode identity federation.
For details, see [Section 4.1.2](#).
- The ability to use scripts to automate certain tasks for integrating Oracle Identity Federation and Oracle Access Manager.
For details, see [Section 4.2](#) and [Section 4.3](#).
- Bug fixes and corrections.

Updates in September 2013 Documentation Refresh for 11g Release 2 (11.1.2.1.0)

The *Integration Guide for Oracle Identity Management Suite* contains these updates in the documentation refresh:

- Bug fixes and corrections.

Updates in July 2013 Documentation Refresh for 11g Release 2 (11.1.2.1.0)

The *Integration Guide for Oracle Identity Management Suite* contains these updates in the documentation refresh:

- Bug fixes and corrections.

Updates in May 2013 Documentation Refresh for 11g Release 2 (11.1.2.1.0)

The *Integration Guide for Oracle Identity Management Suite* contains these updates in the documentation refresh:

- Usage of the `preConfigIDStore` option of `idmConfigTool` has been clarified. See Table 2-3.
- Description of the `IDSTORE_KEYSTORE_PASSWORD` parameter of `idmConfigTool` has been expanded. See Table 2-2.
- The OIM-related entries in the example `idm.conf` file have been corrected. See Appendix B.

New and Changed Features for 11g Release 2 (11.1.2.1.0)

The *Integration Guide for Oracle Identity Management Suite* contains these updates:

- The `prepareIDStore` command supports the WAS mode for configuration in the IBM WebSphere environment. See Section 2.4.2.5.
- New command parameters are added. See Table 2.2.
- Chapter 2, "Using the `idmConfigTool` Command," now contains usage notes for certain commands.

Updates in November 2012 Documentation Refresh for 11g Release 2 (11.1.2)

The *Integration Guide for Oracle Identity Management Suite* contains these updates in the documentation refresh:

- A description of the `idm.conf` configuration file has been added. See Appendix B.
- "Validating the Integration" and "Troubleshooting Common Problems" has been added to "Integrating Access Manager and Oracle Identity Manager". See Section 7.11 and Section 7.13.
- "Troubleshooting Tips" has been added to "Configuring Oracle Virtual Directory for Integration with Oracle Identity Manager." See Section 4.4.
- Additional parameters, needed to support the `preConfigIDStore` command for Oracle Unified Directory, have been included. See Section 2.4.1.

Updates in August 2012 Documentation Refresh for 11g Release 2 (11.1.2)

The *Integration Guide for Oracle Identity Management Suite* contains these updates in the documentation refresh:

- `idmConfigTool` support for Oracle Unified Directory. See Chapter 2.
- Integrating Oracle Access Management Access Manager 11g Release 2 (11.1.2) with Oracle Identity Federation 11g Release 1 (11.1.1). See Section 10.2.

New and Changed Features for 11g Release 2 (11.1.2)

11g Release 2 (11.1.2) includes these new features:

- The IdM Configuration Tool has been updated:
 - The tool supports 11g webgate by default
 - The tool supports cross-domain configuration for Oracle Access Management Access Manager and Oracle Identity Manager
 - A new command, `upgradeOIMTo11gWebgate`, has been added.

For details, see Chapter 2.

- Integration procedures have been revised. For details, see the chapters for the relevant components.

Other Significant Changes in this Document for 11g Release 2 (11.1.2)

This is a new book in 11g Release 2 (11.1.2). Some integrations described in this book were previously covered in the 11g Release 1 (11.1.1) *Oracle Access Manager Integration Guide*.

Part I

IdM Integration Topology

This part introduces the integration topologies supported by this document, and describes the tools used during integration.

This part contains the following chapter:

- [Chapter 1, "Introduction"](#)

Introduction

This chapter explains integration concepts for the Oracle Identity Management suite.

The chapter contains these topics:

- [Prerequisites to Integration](#)
- [Integration Topologies](#)
- [About Oracle Identity Management Components](#)
- [IdM Integration Quick Links](#)
- [Common Integration Scenarios](#)
- [System Requirements and Certification](#)
- [Using My Oracle Support for Additional Troubleshooting Information](#)

1.1 Prerequisites to Integration

Before using the procedures in this document to integrate Oracle Identity Management components, you must install and deploy the components. These prerequisites are explained in the following sections:

- [Understanding the Installation Roadmap](#)
- [Understanding Deployment Topologies](#)
- [About LDAP Synchronization in Oracle Identity Manager](#)
- [About Using Oracle Virtual Directory with Access Manager](#)
- [Common Environment Variables](#)

For details about installing Oracle Identity Management components, see:

- *Installation Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Quick Installation Guide for Oracle Identity and Access Management*

1.1.1 Understanding the Installation Roadmap

You will take (or may already have taken) one of these paths in your IdM deployment:

- Installation, followed by component integration, and ending with scale-out (HA)
- Installation, followed by scale-out, and ending with integration

With scale-out, you may already have performed some of the integration procedures described here; notes in the relevant sections can help you determine whether a procedure is needed.

The Introduction chapter in the *Installation Guide for Oracle Identity and Access Management* contains background on the IdM deployment procedure and describes the installation roadmap, prerequisites, and the installation and configuration workflow.

Oracle Fusion Middleware High Availability Solutions in the *High Availability Guide* explains the high availability solutions in Oracle Fusion Middleware, as well as the topologies and architecture of the various HA options.

1.1.2 Understanding Deployment Topologies

You must also understand the identity management topology and the environment in which the components will work together.

To learn more about the topology supported in this document, see [Section 1.2](#).

1.1.3 About LDAP Synchronization in Oracle Identity Manager

Enable LDAP synchronization in Oracle Identity Manager before starting this integration.

If you did not enable LDAP synchronization by using the OIM Configuration Wizard during installation, refer to [Appendix E, "Enabling LDAP Synchronization in Oracle Identity Manager"](#) for instructions.

The following topics provide an overview of the integration between LDAP identity store and Oracle Identity Manager:

- [The Identity Store](#)
- [Integration Between LDAP Identity Store and Oracle Identity Manager](#)

1.1.3.1 The Identity Store

Oracle Identity Manager provides the ability to integrate an LDAP-based identity store into Oracle Identity Manager architecture. You can connect and manage an LDAP-based identity store directly from Oracle Identity Manager. Using this feature, you can use advanced user management capabilities of Oracle Identity Manager, including request-based creation and management of identities, to manage the identities within the corporate identity store.

In this deployment architecture, user identity information is stored in Oracle Identity Manager database to support the relational functionality necessary for Oracle Identity Manager to function, as well as in the LDAP store. All data is kept in sync transparently without the need for provisioning actions and setting up policies and rules. Identity operations started within Oracle Identity Manager, such as user creation or modification, are run on both the stores in a manner that maintains transactional integrity. In addition, any changes in the LDAP store made outside of Oracle Identity Manager are pulled into Oracle Identity Manager and made available as a part of the identity context.

1.1.3.2 Integration Between LDAP Identity Store and Oracle Identity Manager

Oracle Identity Manager users and roles are stored in Oracle Identity Manager database. However, when a user, role, or role membership change takes place in Oracle Identity Manager, this information is propagated to LDAP identity store. If user, role,

or role membership change takes place in LDAP directly, then these changes are synchronized into Oracle Identity Manager. The synchronization involves:

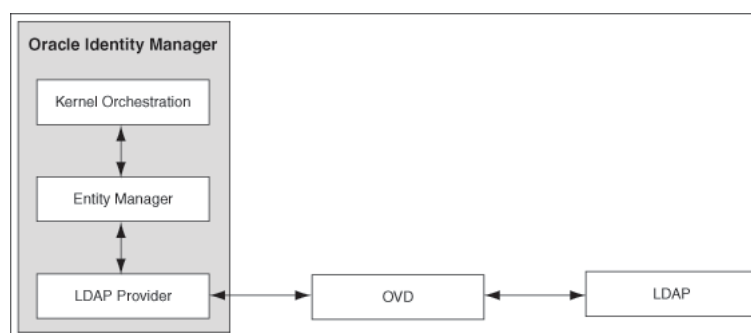
- Changes made in Oracle Identity Manager: User creation, modification, deletion, changes in enabled/disabled state and locked/unlocked states, and password changes are synchronized to LDAP.
- Role creation, modification, and deletion actions update the LDAP groups, including membership changes.
- Initial load of users, roles, and role memberships are synchronized.
- Direct changes to user profile in LDAP are reconciled to Oracle Identity Manager. However, a change to a user password made in LDAP is not reconciled to Oracle Identity Manager.
- Direct changes to roles and role memberships in LDAP are reconciled to Oracle Identity Manager.

When changes are made in the user and role data, the actual operation is performed with the help of the kernel handlers. These handlers go through an orchestration lifecycle of various stages, such as validation, preprocessing, action, and postprocessing.

Oracle Identity Manager kernel orchestration connects to the Entity Manager, which in turn connects to the LDAP provider. The LDAP provider connects to Oracle Virtual Directory (OVD) and Identity Virtualization Library (libOVD). OVD is an interface to various directory systems, such as Oracle Internet Directory, iPlanet, and Active Directory. The LDAP provider reaches the LDAP data by using OVD. libOVD is an LDAP virtualization layer (based on OVD) embedded in Fusion Middleware components, such as Oracle Identity Manager and Access Manager. It is not a standalone LDAP server like OVD.

Figure 1–1 shows the communication between Oracle Identity Manager and LDAP.

Figure 1–1 Oracle Identity Manager and LDAP



The integration configuration and synchronization of data between Oracle Identity Manager and the LDAP identity store are described in the following sections:

- [Configuring the Integration with LDAP](#)
- [Provisioning Data From Oracle Identity Manager to LDAP Identity Store](#)
- [Reconciliation From LDAP Identity Store to Oracle Identity Manager](#)

1.1.3.2.1 Configuring the Integration with LDAP Configuring the integration between Oracle Identity Manager and LDAP is performed after installing Oracle Identity Manager. When integrating LDAP with Oracle Identity Manager, you must create a

container to store reserved users, create a new user in Oracle Identity Manager to perform Oracle Identity Manager operations, and configure OVD (or libOVD) with a directory server to work with Oracle Identity Manager. These tasks are explained in the subsequent sections.

The post-configuration utility, as described in [Section E.2.1, "Running the LDAP Post-Configuration Utility"](#), enables the following scheduled jobs in Oracle Identity Manager. It updates the Last Change Number parameter of each job with the value found in the LDAP directory.

- LDAP User Create and Update Reconciliation
- LDAP User Delete Reconciliation
- LDAP Role Membership Reconciliation
- LDAP Role Hierarchy Reconciliation
- LDAP Role Create and Update Reconciliation
- LDAP Role Delete Reconciliation

In addition, you must enable these scheduled jobs after updating the Last Change Number parameter. To do so, see "Disabling and Enabling Jobs" in *Administering Oracle Identity Manager*.

See Also: "Managing Scheduled Tasks" for detailed information about scheduled jobs in *Administering Oracle Identity Manager*.

1.1.3.2.2 Provisioning Data From Oracle Identity Manager to LDAP Identity Store Oracle Identity Manager database stores the user and role information. When the user and role information is updated in Oracle Identity Manager, then the external repositories, such as the LDAP directory, must also be updated.

The LDAP changes are performed before Oracle Identity Manager changes. If Oracle Identity Manager changes fail, then the LDAP changes must be reverted to the original state. This is achieved by correcting an enable operation with a disable operation, a create operation with a delete operation, and a modification operation with another modification operation with the original values.

For instance, when a user is created, the validation processes are performed in the validation stage, such as password or any other policy validation. In the preprocessing stage, the user is created in LDAP first. Then, in the action stage, the user is to be created in Oracle Identity Manager. If there is an error in creating the user in Oracle Identity Manager, then the user must be deleted from LDAP because the corresponding user could not be created in Oracle Identity Manager. The operation to revert the change made is provided by the kernel handlers through the compensation method, which is predefined in Oracle Identity Manager.

Note: Each handler has predefined execute and compensate methods. The execute method runs any operation, such as creating a user. The compensate method is called when an error occurs to revert the operation performed by the execute method.

To synchronize data from Oracle Identity Manager to LDAP, the location of the LDAP must be known to Oracle Identity Manager. The information about the LDAP location is stored in Oracle Identity Manager as the Directory Server IT resource. This is a default IT resource provided by Oracle Identity Manager. The various parameters of

this IT resource, which you can specify while installing Oracle Identity Manager, allows the connection between Oracle Identity Manager and LDAP.

In order to identify the same entry in Oracle Identity Manager and LDAP, the Distinguished Name (DN) and GUID attributes are used. Each entry has the DN attribute in LDAP, which indicates the unique location of an entry in LDAP. The GUID attribute is a unique ID to identify the entry. The DN and GUID for users and roles are stored in columns in the users and role tables in Oracle Identity Manager database.

This section describes the following topics:

- [Managing Users](#)
- [Managing Roles](#)

1.1.3.2.3 Managing Users The following user operations can be performed to synchronize data from Oracle Identity Manager to LDAP:

- Create user
- Update user
- Delete user
- Enable user
- Disable user
- Lock user
- Unlock user
- Add role member
- Delete role member
- Change password

1.1.3.2.4 Managing Roles The following role operations can be performed to synchronize data from Oracle Identity Manager to LDAP:

- Create role
- Update role
- Delete role
- Add role to a member
- Add and Update role
- Remove role from a member
- Add role hierarchy
- Remove role hierarchy

1.1.3.2.5 Reconciliation From LDAP Identity Store to Oracle Identity Manager When changes in the identities are made directly in the LDAP identity store, the changes must be replicated to Oracle Identity Manager through authoritative source reconciliation. The identities include users and roles.

Reconciling users from LDAP to Oracle Identity Manager works with the general configuration of reconciliation, which includes the scheduled tasks for reconciliation.

See Also: "Managing Scheduled Tasks" for information about scheduler and scheduled tasks in *Administering Oracle Identity Manager*.

Note: Instead of using LDAP synchronization reconciliation jobs to reconcile users from LDAP to Oracle Identity Manager, if the Bulk Load utility is used, then subsequent operation on these users might fail if LDAP synchronization is enabled. To avoid this, all the users that are loaded in Oracle Identity Manager must be updated with correct GUID and DN values, and all these users in LDAP must be updated with an object class called orclIDXPerson.

For detailed information about the Bulk Load utility, see "Using the Bulk Load Utility" in *Developing and Customizing Applications for Oracle Identity Manager*.

The role reconciliation works only with the LDAP groups. Role reconciliation supports creation, updation, and deletion of roles. Role membership reconciliation supports creation and deletion of role memberships being driven from changes in an external LDAP directory.

Without roles and users being present in Oracle Identity Manager, role membership reconciliation will fail. Therefore, configure the LDAP synchronization scheduled jobs to run in the following order:

1. Fusion Applications Role Category Seeding

Note: Fusion Applications Role Category Seeding is a predefined scheduled task that is generated only when LDAP synchronization is enabled, along with other LDAP synchronization scheduled jobs. This job gets all distinct business categories in LDAP and creates them as OIM role categories.

For a list of the predefined scheduled jobs, see "Predefined Scheduled Tasks" in *Administering Oracle Identity Manager*.

2. LDAP Role Create and Update Reconciliation
3. LDAP Role Hierarchy Reconciliation
4. LDAP User Create and Update Reconciliation
5. LDAP Role Membership Reconciliation

For each of these jobs, except Fusion Applications Role Category Seeding, there is a parallel job to do the full reconciliation. All these jobs, except Fusion Applications Role Category Seeding, perform the reconciliation based on change logs, whereas full reconciliation jobs use the search base to do the reconciliation.

1.1.3.2.6 Consolidated LDAP Sync Full Reconciliation The LDAP Consolidated Full Reconciliation scheduled job runs the following jobs in order:

1. LDAP User Create and Update Full Reconciliation
2. LDAP Role Create and Update Full Reconciliation
3. LDAP Role Membership Full Reconciliation

4. LDAP Role Hierarchy Full Reconciliation

See Also: "LDAP Scheduled Tasks" in *Administering Oracle Identity Manager* for information about the LDAP Consolidated Full Reconciliation scheduled job

When you run the LDAP Consolidated Full Reconciliation scheduled job, the job status of the previous job and all event status for that particular job are checked because the next job must be run in a particular order. If any job fails to run, then the automatic run of the jobs stop, and error messages are logged in the diagnostic log.

Note: The LDAP User Delete Full Reconciliation and LDAP Role Delete Full Reconciliation jobs are not part of LDAP Consolidated Full Reconciliation. These scheduled jobs are disabled by default. They can be enabled by selecting the radio buttons and can be run individually.

You can also run the individual jobs by selecting the radio buttons on the LDAP Sync Consolidated Full Reconciliation job details page. The job details contain all the common parameters for the four full reconciliation jobs. In addition, you can specify the values for the following parameters of the LDAP Sync Consolidated Full Reconciliation scheduled job:

- **Reconciliation Search Base:** Search base for the full reconciliation of users or roles. This defines the location in the LDAP directory from which the LDAP search begins.
- **Reconciliation Role Search Filter:** Search filter for full reconciliation of roles. This filter allows certain role/group entries in the subtree of the LDAP directory and excludes others.
- **Reconciliation User Search Filter:** Search filter for full reconciliation of users. This filter allows certain user entries in the subtree of the LDAP directory and excludes others.

Based on the values entered for the Reconciliation Search Base and/or Reconciliation User Search Filter and Reconciliation Role Search Filter parameters, the user and role accounts are pulled into Oracle Identity Manager from LDAP when the LDAP Sync Consolidated Full Reconciliation job is run. As a result of this full reconciliation, the delete happens in the Oracle Identity Manager database for the deleted entries in LDAP from that particular node.

The Reconciliation Search Base and Reconciliation Search Filter parameters support the following use cases (sample parameters are shown):

- **Reconciling the user or role account from LDAP to Oracle Identity Manager database:**

This provides the option to perform fine-grained reconciliation of a particular user or role. The value of the Reconciliation Search Base parameter is:

```
"cn=sampleuser1,cn=users,cn=subrealm1,dc=us,dc=example,dc=com"
```

- **All users and roles or groups under the node are reconciled:**

The value of Reconciliation Search Base is:

```
"cn=subrealm1,dc=us,dc=example,dc=com"
```

Here, the user full reconciliation and role full reconciliation are triggered. Therefore, all the users and roles or groups under the tenant1 node are reconciled.

- **All users under the node are reconciled:**

The value of Reconciliation Search Base is:

```
"cn=users,cn=subrealm1,dc=us,dc=example,dc=com"
```

Here, all the users under the tenant1 node are reconciled.

- **All roles or groups under the node are reconciled:**

The value of the Reconciliation Search Base parameter is:

```
"cn=groups,cn=subrealm1,dc=us,dc=example,dc=com"
```

Here, all roles or groups under the tenant1 node are reconciled.

The Reconciliation Search Base and Reconciliation Search Filter parameters are not bound together for LDAPSvc Full reconciliation. Reconciliation Search Filter can be empty. Search Base can be used for provisioning or pushing entries from Oracle Identity Manager to LDAP, while Reconciliation Search Base can be used to perform full reconciliation from LDAP to Oracle Identity Manager database. If a value is not provided for Reconciliation Search Base, then the value for Search Base from the 'Directory Server' IT resource configuration is used for both provisioning and full reconciliation.

Sample values for the Reconciliation Search Base parameter:

```
"cn=subrealm1,dc=us,dc=example,dc=com"
```

Sample values for the Search Base parameter:

```
"dc=us,dc=example,dc=com"
```

Sample values for the Reconciliation User Search Filter and Reconciliation Role Search Filter parameters:

```
(objectclass=orclAPPIDPerson)  
(title=foobar)
```

Messages Logged For the LDAP Sync Consolidated Full Reconciliation Scheduled Job

The following is a list of messages for the LDAP Sync Consolidated Full Reconciliation scheduled job that are logged in the Oracle Identity Manager diagnostic log files:

```
LDAP Sync Full Reconciliation Scheduler job {0} is currently Running.  
LDAP Sync Full Reconciliation Scheduler job {0} is not currently Running. It has  
Stopped.  
LDAP Sync Full Reconciliation Scheduler job {0} is currently being Interrupted  
while running.  
LDAP Sync Full Reconciliation Scheduler job {0} is not currently Running. It has  
Failed.  
Error occurred while running the LDAP Sync User Full Reconciliation scheduler job.  
Please refer to the OIM Server logs for more details.  
LDAP Sync Full Reconciliation Scheduler job {0} is not currently Running. It has  
been Shutdown.  
LDAP Sync Full Reconciliation Scheduler job {0} is not currently Running.  
SQLException has occurred.  
All LDAPSvc Full Reconciliation jobs ran successfully and Stopped.
```

1.1.4 About Using Oracle Virtual Directory with Access Manager

Using Oracle Virtual Directory with Oracle Access Management Access Manager (Access Manager) is *optional*. However, if you plan to use Oracle Virtual Directory with Access Manager, then you must configure Oracle Virtual Directory for integration with Access Manager before starting the core integration procedures described in this publication.

Refer to [Appendix F, "Configuring Oracle Virtual Directory for Integration with Oracle Access Management Access Manager"](#) for instructions.

1.1.5 Common Environment Variables

This document uses shorthand notation to refer to common environment variables. For example, the Oracle Middleware Home directory is often referred to as `MW_HOME`.

For a list of common environment variables, see "Identifying Installation Directories" in the *Installation Guide for Oracle Identity and Access Management*.

1.2 Integration Topologies

Oracle Identity Management consists of a number of products, which can be used either individually or collectively. Two basic types of topology are available in Oracle Identity Management:

- Basic integration topology
This topology supports integration between suite components, in an environment where each component runs on a separate node.
- Enterprise integration topology
This topology supports integration between suite components in an enterprise environment. Each component may run on multiple nodes.

Topology Described in this Document

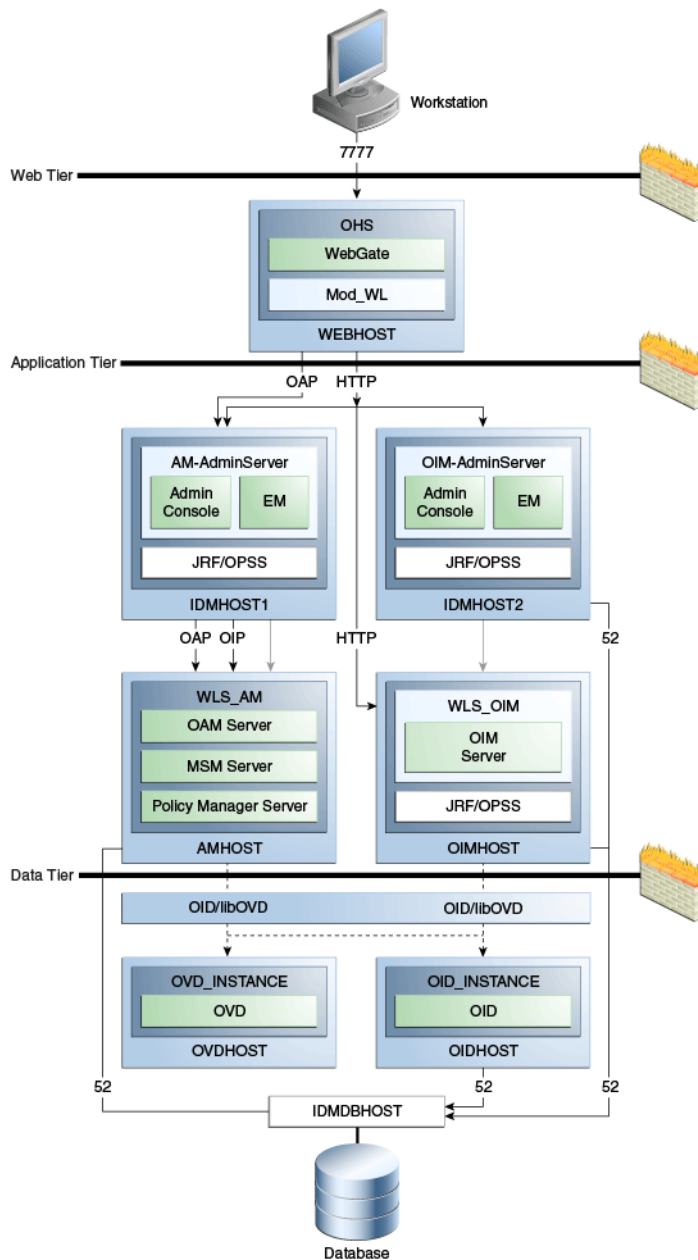
This book is dedicated to the first type, single-node integration topology. Use the procedures described in this book when deploying Oracle Identity Management in an environment where each component runs on its own node. You can also use the procedures to understand integration tools and techniques, and to understand the effects and benefits of integrating specific identity management components.

1.2.1 Basic Integration Topology

See Also: [Table 1-1](#) for definitions of acronyms used in this section.

[Figure 1-2](#) shows a basic integration topology where the IdM components Access Manager and Oracle Identity Manager are configured on separate WebLogic domains:

Figure 1–2 Basic Integration Topology with Multiple Administration Servers



Note that:

- All IdM components, including Access Manager server (AMHOST), the Oracle Identity Manager server (OIMHOST), and Oracle Internet Directory (OID) are configured in separate WebLogic domains, and each is administered by its own administration server.

Besides enhancing management of each component, this topology ensures you have flexibility when applying patches and upgrades. Patches for each component can be applied independently, with no version dependency on other components.

- For simplicity, some of the OMSS topology is omitted; for example the MSAS server which resides in the DMZ is not shown in the diagram. For complete details of OMSS architecture, see [Section 5.2](#).

- The BIP server and SOA Suite reside on the OIM domain; they are not shown in the diagram.
- The figure shows some representative ports only.

About SOA Suite for Oracle Identity Manager

The SOA Suite used by OIM must be installed in the same domain as OIM. However, if you use SOA Suite for other purposes, you should consider setting up a separate install of SOA Suite for running your own services, composites, and other SOA features for that purpose.

About Single Domain Architecture

In the single-domain architecture, Oracle Access Management Access Manager, Oracle Identity Manager, and Mobile Security Access Server are configured on the same WebLogic domain. While possible, such a topology is not practical in the current context for the reasons cited above, and is not recommended for IdM integration.

See Also: [Section 1.3](#) for an introduction to each IdM component.

1.2.1.1 The Three Tier Architecture

This architecture can be viewed as consisting of three layers or zones:

- The Web Tier consists of the HTTP server and handles incoming Web traffic.
- The Application Tier contains identity management applications for managing identities and access, including Oracle Identity Manager and Oracle Access Manager.
- The Data Tier, here considered to include the directory servers, hosts LDAPs and database.

1.2.1.2 Understanding the Web Tier

The web tier is in the DMZ Public Zone. The HTTP servers are deployed in the web tier.

Most Identity Management components can function without the web tier. However, the web tier is required to support enterprise level single sign-on using products such as Access Manager.

The web tier is structured as follows in the single-node topology:

- WEBHOST has Oracle HTTP Server, WebGate (an Access Manager component), and the mod_wl_ohs plug-in module installed. The mod_wl_ohs plug-in module enables requests to be proxied from Oracle HTTP Server to a WebLogic Server running in the application tier.
- WebGate, an Access Manager component in Oracle HTTP Server, uses Oracle Access Protocol (OAP) to communicate with Access Manager running on OAMHOST. WebGate and Access Manager are used to perform operations such as user authentication.

1.2.1.3 Understanding the Application Tier

The application tier is the tier where Java EE applications are deployed. Products such as Oracle Identity Manager, Oracle Mobile Security Suite, Oracle Access Management Identity Federation, and Oracle Enterprise Manager Fusion Middleware Control are among key Java EE components deployed in this tier.

The Identity Management applications in the application tier interact with the directory tier as follows:

- They leverage the directory tier for enterprise identity information.
- They leverage the directory tier (and sometimes the database in the data tier) for application metadata.
- Fusion Middleware Control Console provides administrative functions to the components in the application and directory tiers.
- Oracle WebLogic Server has built-in web server support. If enabled, the HTTP listener exists in the application tier as well.

1.2.1.4 Understanding the Data Tier

The data tier is the deployment layer where all the LDAP services reside. This tier includes products such as Oracle Internet Directory (OIDHOST), Oracle Virtual Directory (OVDHOST), Oracle Unified Directory, and Oracle Database (IDMDBHOST).

The data tier stores two types of information:

- Identity Information: Information about users and groups resides in the identity store.
- Oracle Platform Security Services (OPSS): Information about security policies and about configuration resides in the policy store.

Storing Policy Data

Policy information resides in a centralized policy store that is located within a database. You may store identity information in Oracle Internet Directory or in another directory.

Storing Identity Data

If you store the identity details in a directory other than Oracle Internet Directory you can use Oracle Virtual Directory to present all the identity data in a single consolidated view that Oracle Identity Management components can interpret. For details, see [Chapter 7](#).

Note: Oracle Identity Manager uses Oracle Virtual Directory server or libOVD to access third-party directories.

1.2.2 The Enterprise Integration Topology

Unlike the single-node topologies described in this document, an enterprise integration topology takes into account such features as high availability, failover, and firewalls, and is beyond the scope of this document.

See the *Enterprise Deployment Guide for Oracle Identity and Access Management*, which explains the concepts of the enterprise integration topology and provides implementation procedures.

1.2.3 Using Multiple Directories for an Identity Store

Although the integration scenarios in this document focus on a simple identity store topology consisting of an Oracle Internet Directory LDAP server, your site may have some user data in a third-party directory, such as Microsoft Active Directory, and other user data in Oracle Internet Directory.

To account for this topology, you can use Oracle Virtual Directory to present all the identity data in a single consolidated view that Oracle Identity Management components can interpret.

For configuration details, see [Chapter 7](#).

1.2.4 Integration Terminology

[Table 1–1](#) shows key terms and acronyms that are used to describe the architecture and topology of an Oracle Fusion Middleware environment:

Table 1–1 Oracle Fusion Middleware Integration Terminology

Term	Definition
IdM Configuration Tool	A command-line tool to verify the status of identity management components and to perform certain integration tasks.
Oracle Access Protocol (OAP)	A secure channel for communication between Webgates and Access Manager servers during authorization.
Oracle Fusion Middleware home	A Middleware home consists of the Oracle WebLogic Server home, and, optionally, one or more Oracle homes. A Middleware home can reside on a local file system or on a remote shared disk that is accessible through NFS.
Oracle HTTP Server (OHS)	Web server component for Oracle Fusion Middleware that provides a listener for Oracle WebLogic Server.
WebLogic Server home	A WebLogic Server home contains installed files necessary to host a WebLogic Server. The WebLogic Server home directory is a peer of other Oracle home directories underneath the Middleware home directory.
Oracle home	An Oracle home contains installed files necessary to host a specific product. For example, the Oracle Identity Management Oracle home contains a directory that contains binary and library files for Oracle Identity Management. An Oracle home resides within the directory structure of the Middleware home. Each Oracle home can be associated with multiple Oracle instances or Oracle WebLogic Server domains.
Oracle instance	An Oracle instance contains one or more system components, such as Oracle Web Cache, Oracle HTTP Server, or Oracle Internet Directory. The system components in an Oracle instance must reside on the same machine. An Oracle instance directory contains files that can be updated, such as configuration files, log files, and temporary files. An Oracle instance is a peer of an Oracle WebLogic Server domain. Both contain specific configurations outside of their Oracle homes. The directory structure of an Oracle instance is separate from the directory structure of the Oracle home. It can reside anywhere; it need not be within the Middleware home directory.

Table 1–1 (Cont.) Oracle Fusion Middleware Integration Terminology

Term	Definition
Oracle WebLogic Server domain	<p>A WebLogic Server domain is a logically related group of Java components. A WebLogic Server domain includes a special WebLogic Server instance called the Administration Server, which is the central point from which you configure and manage all resources in the domain. Usually, you configure a domain to include additional WebLogic Server instances called Managed Servers. You deploy Java components, such as Web applications, EJBs, and Web services, and other resources to the Managed Servers and use the Administration Server for configuration and management purposes only.</p> <p>Managed Servers in a WebLogic Server domain can be grouped together into a cluster.</p> <p>An Oracle WebLogic Server domain is a peer of an Oracle instance. Both contain specific configurations outside of their Oracle homes.</p> <p>The directory structure of an WebLogic Server domain is separate from the directory structure of the WebLogic Server home. It can reside anywhere; it need not be within the Middleware home directory.</p>
system component	<p>A system component is a manageable process that is not WebLogic Server. For example: Oracle HTTP Server, WebCache, and Oracle Internet Directory. Includes the JSE component.</p>
Java component	<p>A Java component is a peer of a system component, but is managed by the application server container. Generally refers to a collection of applications and resources, with generally a 1:1 relationship with a domain extension template. For example: SOA and WebCenter Spaces.</p>
Oracle Fusion Middleware farm	<p>Oracle Enterprise Manager Fusion Middleware Control is a Web browser-based, graphical user interface that you can use to monitor and administer an Oracle Fusion Middleware farm.</p> <p>An Oracle Fusion Middleware farm is a collection of components managed by Fusion Middleware Control. It can contain WebLogic Server domains, one or more Managed Servers and the Oracle Fusion Middleware system components that are installed, configured, and running in the domain.</p>
Oracle Identity Management	<p>The suite of identity and access management components in Oracle Fusion Middleware. See Section 1.3 for details.</p>
WebLogic Administration Server	<p>The Administration Server is the central point from which you configure and manage all resources in the WebLogic domain.</p>
WebLogic Managed Server	<p>The Managed Server is an additional WebLogic Server instance to host business applications, application components, Web services, and their associated resources. Multiple managed servers can operate within the domain. Certain Managed Servers in the domain are created specifically to host Oracle Fusion Middleware components.</p>

1.3 About Oracle Identity Management Components

This section provides a brief overview of IdM components whose integrations are described in this book, and explains the benefits of integration. Topics include:

- [Oracle Unified Directory](#)
- [Oracle Internet Directory](#)
- [Oracle Virtual Directory](#)
- [Oracle Access Management Access Manager](#)
- [Oracle Identity Manager](#)
- [Oracle Adaptive Access Manager](#)
- [Oracle Mobile Security Suite](#)
- [Oracle Access Management Identity Federation](#)

1.3.1 Oracle Unified Directory

Oracle Unified Directory is a comprehensive next generation directory service. It is designed to address large deployments and to provide high performance in a demanding environment.

The Oracle Unified Directory server is an LDAPv3-compliant directory server written entirely in Java. The directory server provides full LDAPv3 compliance, high performance and space effective data storage, and ease of configuration and administration.

Several procedures in this book feature Oracle Unified Directory as the repository for the identity store. For details, see [Section 2.3, "Configuring the Identity Store"](#).

1.3.2 Oracle Internet Directory

Oracle Internet Directory is a general purpose directory service that enables fast retrieval and centralized management of information about dispersed users and network resources. It combines Lightweight Directory Access Protocol (LDAP) Version 3 with the high performance, scalability, robustness, and availability of an Oracle Database.

Oracle Internet Directory can serve as the repository for the identity store, which contains user identities leveraged by identity management components and other applications.

For details about integration with Oracle Internet Directory, see:

- [Appendix E, "Enabling LDAP Synchronization in Oracle Identity Manager"](#)

1.3.3 Oracle Virtual Directory

Oracle Virtual Directory, an LDAP version 3 enabled service that provides virtualized abstraction of one or more enterprise data sources into a single directory view. Oracle Virtual Directory makes many directories appear to be one local repository, hiding the complexity of data location, format, and protocol from client applications.

For details about integration with Oracle Virtual Directory, see:

- [Appendix F, "Configuring Oracle Virtual Directory for Integration with Oracle Access Management Access Manager"](#)

1.3.4 Oracle Access Management Access Manager

Oracle Access Management Access Manager provides a full range of Web perimeter security functions that include Web single sign-on; authentication and authorization;

policy administration; auditing, and more. All existing access technologies in the Oracle Identity Management stack converge in Access Manager.

For details about integration with Access Manager, see:

- [Chapter 3, "Integrating Access Manager, OAAM, and OIM"](#)
- [Chapter 6, "Integrating with Identity Federation"](#)
- [Appendix C, "Integrating Oracle Adaptive Access Manager with Access Manager"](#)

1.3.4.1 A Note About IDMDomain Agents and Webgates

By default, the IDMDomain Agent is enabled in the Oracle HTTP Server deployment. If you migrate from IDMDomain Agent to WebGate Agent, note the following:

- The protection policies set up for IDMDomain can be reused for WebGate if your webgate uses the IDMDomain preferredHost.
- IDMDomain and WebGate can coexist. If the IDMDomain Agent discovers a WebGate Agent in the Oracle HTTP Server deployment, IDMDomain Agent becomes dormant.

See Also: Configuring Centralized Logout for the IDM Domain Agent in the *Administrator's Guide for Oracle Access Management*.

1.3.5 Oracle Identity Manager

Oracle Identity Manager is a powerful and flexible enterprise identity management system that automatically manages users' access privileges within enterprise IT resources. Oracle Identity Manager is designed from the ground up to manage user access privileges across all of a firm's resources, throughout the entire identity management lifecycle—from initial creation of access privileges to dynamically adapting to changes in business requirements.

For details about integration with Oracle Identity Manager, see [Chapter 3, "Integrating Access Manager, OAAM, and OIM"](#).

1.3.6 Oracle Adaptive Access Manager

Oracle Adaptive Access Manager is Oracle Identity Management's solution for web access real-time fraud detection and multifactor online authentication security for the enterprise. It provides:

- Real-time and batch risk analytics to combat fraud and misuse across multiple channels of access
- An extensive set of capabilities including device fingerprinting, real-time behavioral profiling and risk analytics
- Risk-based authentication methods including knowledge-based authentication (KBA) challenge infrastructure with Answer Logic and OTP Anywhere

See Also: "Introduction to Oracle Adaptive Access Manager" in *Administering Oracle Adaptive Access Manager*.

For details about integration with Oracle Adaptive Access Manager, see:

- [Chapter 3, "Integrating Access Manager, OAAM, and OIM"](#).
- [Appendix C, "Integrating Oracle Adaptive Access Manager with Access Manager"](#).

Note: Oracle Adaptive Access Manager integration with both OAM 10g and Access Manager 11g in coexistence mode and customizations such as single login page mode are beyond the scope of this document. For details, see *Developer's Guide for Oracle Adaptive Access Manager*.

1.3.7 Oracle Mobile Security Suite

Oracle Mobile Security Suite creates a secure enterprise workspace on mobile devices to isolate and protect corporate applications and data.

Oracle Mobile Security Suite and Access Manager are always installed together and integrated by default. It allows users to access corporate applications protected by Access Manager from the Mobile Workspace application while providing a unified administration console. Integration with Oracle Identity Manager enables you to allow mobile users, whose identities are governed by Oracle Identity Manager, to access corporate application with the single sign-on capabilities of Access Manager.

For details about integration with Oracle Mobile Security Suite, see [Chapter 5](#).

1.3.8 Oracle Access Management Identity Federation

To enhance support for federated authentication in cloud, web services, and B2B transactions, a SAML-based federation service is being introduced in a single access management server in 11g Release 2 (11.1.2). Oracle Access Management Identity Federation is an enterprise-level, carrier-grade service for secure identity information exchange between partners. Identity Federation protects existing IT investments by integrating with a wide variety of data stores, user directories, authentication providers and applications.

In this initial release Identity Federation is limited to Service Provider mode. Identity Provider mode still requires an Oracle Identity Federation 11gR1 installation.

For details about using the Identity Federation service with Access Manager, see [Chapter 6, "Integrating with Identity Federation"](#).

1.4 IdM Integration Quick Links

[Table 1–2](#) provides links to the integration procedures described in this document.

Table 1–2 *Links to Integration Procedures in This Guide*

Components to Integrate	Link
Post-install LDAP Synchronization with Oracle Identity Manager	Appendix E
Oracle Virtual Directory and Oracle Identity Manager	Appendix E
Oracle Virtual Directory and Access Manager	Appendix F
Access Manager and Oracle Identity Manager	Chapter 2
Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager	Chapter 3
Access Manager and Identity Federation	Chapter 6
Multi-Directory identity store	Chapter 7
Access Manager and Oracle Adaptive Access Manager	Appendix C
End-to-end SSL for IdM Components	Chapter 4

Integration Procedures in Other Documents

Table 1–3 lists key integration procedures that appear in other IdM documents:

Table 1–3 Links to Integration Procedures in Other Guides

Components to Integrate	Link
Oracle Privileged Account Manager (OPAM) and Oracle Identity Manager (OIM)	"Integrating with Oracle Identity Manager" in <i>Administering Oracle Privileged Account Manager</i> .
OPAM and OAM	"Integrating with Oracle Access Management Access Manager" in <i>Administering Oracle Privileged Account Manager</i> .
OIM and Oracle Identity Analytics (OIA)	"Integrating with Identity Analytics" in <i>Administering Oracle Identity Manager</i>

1.5 Common Integration Scenarios

This section describes common scenarios to integrate Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager and the resource protection and collection and password management benefits.

1.5.1 Resource Protection and Credential Collection Scenarios (OAAM Advanced Integration Using TAP)

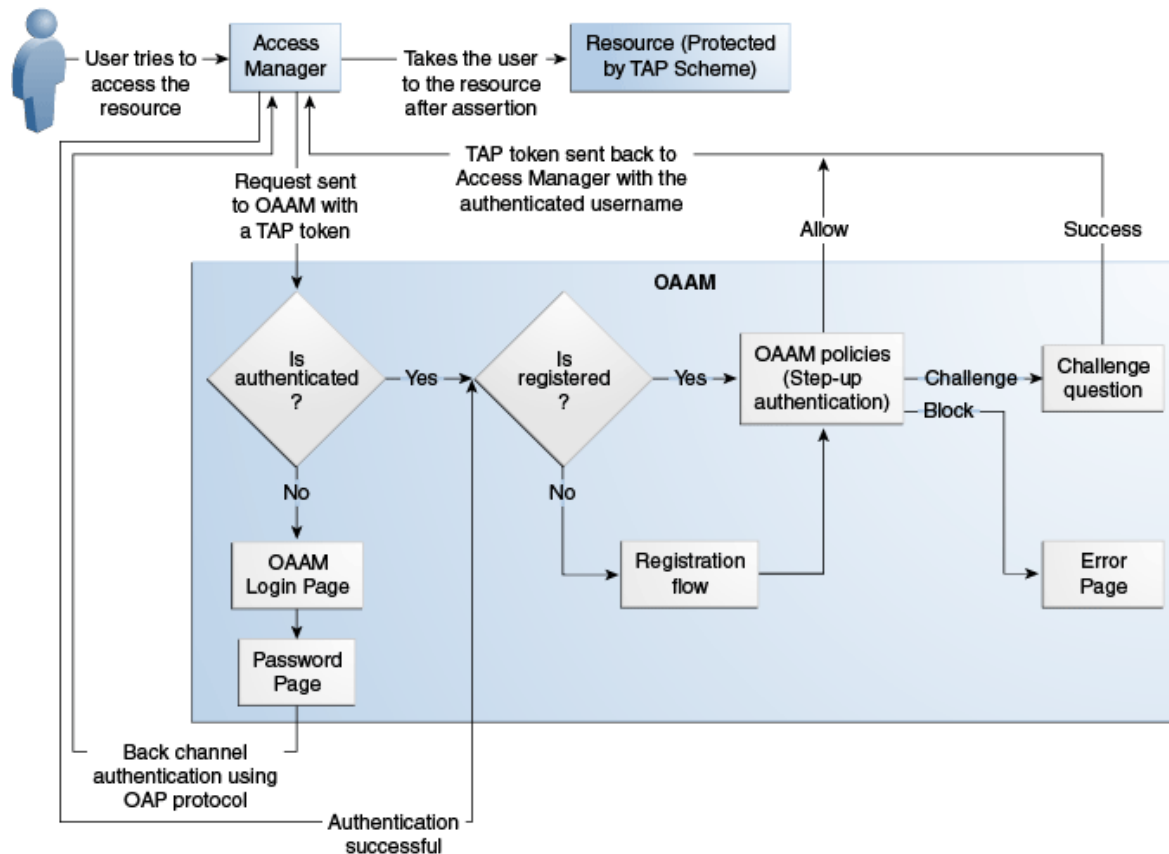
This section describes the process flow when a user tries to access a protected resource in an Access Manager and OAAM Advanced integration using Trusted Authentication Protocol (OAAM Advanced using TAP). OAAM Advanced using TAP is the supported OAAM Advanced integration with Access Manager. This integration type provides authentication schemes, virtual authenticators, fraud rules, knowledge-based authentication, challenge processor and shared library frameworks, and additional advanced security access features, such as OTP Anywhere and Step Up Authentication.

Step Up Authentication allows a user who has been authenticated for a resource at a specific authentication level to access resources at a relatively higher authentication level. When the user accesses a resource protected with an authentication level that is greater than the level of his current token, OAAM runs policies to determine how to further authenticate the user so he can gain the required level of authentication needed for access to the protected resource.

Figure 1–3 illustrates the following scenarios for Step Up Authentication:

- [Case 1: The User is Authenticated by Access Manager with Oracle Adaptive Access Manager Performing Step Up Authentication](#)
- [Case 2: User is Not Authenticated by Access Manager](#)
- [Case 3: User is Authenticated by Access Manager and Oracle Adaptive Access Manager Does Not Perform Step Up Authentication](#)

Figure 1–3 Resource Protection and Credential Collection Flow



Initial steps that pertain to all three cases are listed as follows:

1. A user tries to access a resource protected by Access Manager via TAPscheme configured with Oracle Adaptive Access Manager.
2. The Oracle Access Management WebGate intercepts the unauthenticated request and forwards the request to the OAAM Server with the encrypted TAP token.
Access Manager is forwarding the request to OAAM based on the challenge URL defined in the TAPScheme.
3. The OAAM Server checks for the current authentication status of the user from the TAP token. The TAP token contains the current authentication level. Depending on the value of the current authentication level, Oracle Adaptive Access Manager can determine whether the user is authenticated or not. Accordingly, the user is taken through one of the flows described in this section.

For information on authentication flows, see "Authentication Flow" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

1.5.1.1 Case 1: The User is Authenticated by Access Manager with Oracle Adaptive Access Manager Performing Step Up Authentication

In this scenario, the user is already authenticated when he recently accessed another resource with a lower authentication level. When the user tries to access a resource protected by the TAPscheme, Oracle Adaptive Access Manager does not show the user name and password pages because the user is already authenticated. However, the

following flows are executed in Oracle Adaptive Access Manager based on whether the user has registered or not in Oracle Adaptive Access Manager.

User has registered with Oracle Adaptive Access Manager

If the user is registered with Oracle Adaptive Access Manager, the process flow is as follows:

1. Oracle Adaptive Access Manager fingerprints the PC, notebook, mobile phone, smart phone, or other web-enabled machine used by the user.
2. Oracle Adaptive Access Manager runs the post-authentication rules, determines the risk score, and executes any actions or alerts that are specified in the policy.
3. If the risk score is sufficiently high, Oracle Adaptive Access Manager presents the user with a second challenge (KBA or OTP). In the Challenge flow, he is challenged with his registered challenge questions or one-time password.
4. If the Challenge flow is successful and the user has the appropriate profile registered, Oracle Adaptive Access Manager constructs the TAP token with the user name and sends it back to Access Manager. Access Manager asserts the token sent back. After asserting the token, Access Manager creates its cookie and continues the normal Single-Sign On flow in which it redirects the user to the protected resource.

User has not registered with Oracle Adaptive Access Manager

If the user has not registered with Oracle Adaptive Access Manager, the process flow is as follows:

1. If the user is not registered, he may be asked to register a virtual device, personal image, phrase, and challenge questions, and one-time password, if OTP has been configured. Registration is required depending on security requirements, which specify whether the registration is mandatory or optional.
2. Oracle Adaptive Access Manager fingerprints the PC, notebook, mobile phone, smart phone, or other web-enabled machine used by the user.
3. Oracle Adaptive Access Manager runs the post-authentication rules, determines the risk score, and executes any actions or alerts that are specified in the policy.
4. If the risk score is sufficiently high, Oracle Adaptive Access Manager blocks the user because it cannot challenge a user who does not have a registered profile (no KBA or OTP).
5. If there is no risk, the user is taken through profile registration and after that, Oracle Adaptive Access Manager constructs the TAP token with the user name and sends it back to Access Manager. Access Manager asserts the token sent back. After asserting the token, Access Manager creates its cookie and continues the normal Single-Sign On flow in which it redirects the user to the protected resource.

1.5.1.2 Case 2: User is Not Authenticated by Access Manager

If the user is not authenticated, the process flow is as follows.

1. The OAAM Server presents the user with the OAAM user name page.
2. The user submits his user name on the OAAM user name page.
3. Oracle Adaptive Access Manager fingerprints the PC, notebook, mobile phone, smart phone, or other web-enabled machine used by the user.

4. Oracle Adaptive Access Manager runs pre-authentication rules to determine if the user should be allowed to proceed to the OAAM password page.
5. If the user is allowed to proceed, the virtual authentication device rules are run to determine which virtual authenticator to display in the OAAM password page.
6. If the user has registered with Oracle Adaptive Access Manager, the OAAM Server displays the OAAM password page with either the personalized TextPad or KeyPad. If the user has not registered, Oracle Adaptive Access Manager displays the OAAM password page with the Generic TextPad.
7. The user submits his password on the OAAM password page and the credentials collected are verified against the identity store using the Oracle Access Management OAP API. After validation on the Access Manager side, Oracle Adaptive Access Manager runs the post-authentication rules.
8. Based on rules/risk score, Oracle Adaptive Access Manager might allow the user to proceed, challenge the user, or block the user.
 - If the user is allowed to proceed, then Oracle Adaptive Access Manager evaluates the Registration checkpoint depending on security requirements. If the user is not registered, he may be asked to register virtual device, personal image, phrase, challenge questions, and OTP, if configured.
 - If the user is to be challenged because the risk was sufficiently high, Oracle Adaptive Access Manager evaluates the Challenge checkpoint to determine whether to block him or present him with another challenge (KBA or OTP). If Challenge Choice has been configured and the user has more than one OTP type registered, the user can choose.
 - If the user is blocked, he cannot continue.
9. If authentication is successful and the user has the appropriate profile registered, Oracle Adaptive Access Manager constructs the TAP token with the user name and sends it back to Access Manager. Access Manager asserts the token sent back. After asserting the token, Access Manager creates its cookie and continues the normal Single-Sign On flow in which it redirects the user to the protected resource.

1.5.1.3 Case 3: User is Authenticated by Access Manager and Oracle Adaptive Access Manager Does Not Perform Step Up Authentication

If the user is already authenticated at a higher level than the level required to access the resource protected by TAPscheme, then the flow is not interrupted by Oracle Adaptive Access Manager and the user can directly access the protected resource.

1.5.2 Resource Protection and Credential Collection Scenario (OAAM Basic Integration)

This section describes the process flow when a user tries to access a protected resource in an Access Manager and OAAM Basic integration (OAAM Basic). This deployment provides login security and Knowledge Based Authentication (KBA). For details about OAAM Basic, see [Section C.3, "OAAM Basic Integration with Access Manager."](#)

The process flow is as follows:

1. A user tries to access a resource protected by Access Manager.
2. Oracle Access Management WebGate intercepts the request and forwards the request to the OAAM Server.
3. Access Manager calls the OAAM APIs to run pre-authentication rules to determine if the user should be allowed to proceed. Based on the rule result such as Allow, Block, or Deny, Access Manager displays the appropriate pages.

4. If the user is allowed to proceed, Access Manager displays the password page.
5. The user submits his password and the credentials collected from Access Manager are verified against the identity store.
6. Access Manager calls the OAAM APIs to run the post-authentication rules.
7. Based on the results (Register User, Register Question, Challenge, Allow, or Block), Access Manager displays the appropriate set of pages.

For example, if the result is Register User, as part of the user registration process (for first time login), the user is asked to select and answer three challenge questions.

For example, if the result is Challenge, Access Manager displays a challenge question page with the security question displayed.

1.5.3 Password Management Scenarios

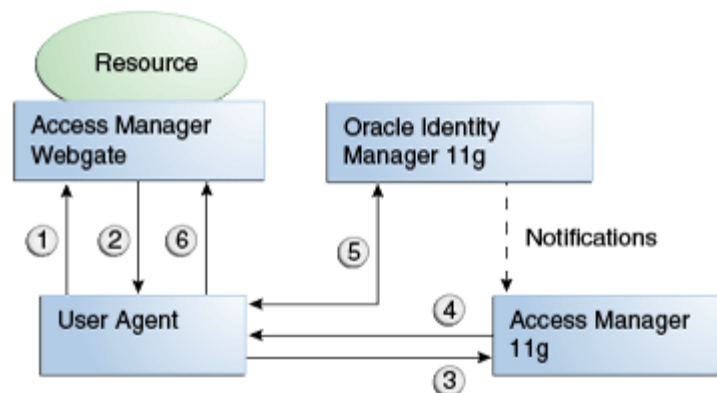
Common management scenarios supported by these deployment modes include:

- [Access Manager Integrated with Oracle Identity Manager](#)
- [Self-Registration](#)
- [Password Change](#)
- [Forgot Password](#)
- [Account Lock and Unlock](#)
- [Challenge Setup](#)
- [Challenge Reset](#)

1.5.3.1 Access Manager Integrated with Oracle Identity Manager

Figure 1–4 shows how password management is achieved when Access Manager and Oracle Identity Manager are integrated.

Figure 1–4 Integrating Access Manager and Oracle Identity Manager for Password Management



The flow of interactions between the components is as follows:

1. A user tries to access a resource protected by Access Manager.
2. The Oracle Access Management WebGate intercepts the (unauthenticated) request.

3. WebGate redirects the user to the Access Manager login service, which performs validation checks.
4. If Access Manager finds any password management trigger conditions, such as password expiry, it redirects users to Oracle Identity Manager.
5. Oracle Identity Manager interacts with the user to establish the user's identity and carry out the appropriate action, such as resetting the password.
6. Access Manager logs the user in by means of auto-login, and redirects the user to the Access Manager-protected resource which the user was trying to access in Step 1.

1.5.3.2 Self-Registration

In this scenario, the user does not have an account but tries to access an Access Manager-protected resource. An Oracle Access Management 11g WebGate intercepts the request, detects that the user is not authenticated, and redirects the user to the Oracle Access Management Credential Collector (or 10g authenticating WebGate), which shows the Access ManagerLogin page containing a **Register New Account** link.

On selecting this link, the user is securely redirected to the Oracle Identity Manager Self Registration URL. Oracle Identity Manager interacts with the user to provision his account.

Self-Registration Flow

The Welcome Page is an unprotected page from which the self-registration/account creation can be initiated. This page contains two links, in addition to any introductory text or branding information. The links are:

- Register New Account - This is an unprotected URL to the corresponding application's registration wizard
- Login - This is a protected URL which serves as the landing page to which the user is directed after successfully completing the login.

Note: Any application protected by a single sign-on system with the self-registration requirement is expected to support a self-registration page. The options are:

- Self-registration using the default self-registration page or a customized version of the page.
This is the most common option and is covered here.
 - Self-registration using anonymous pages in other applications.
If the application dictates that the user be automatically logged in at the end of the registration process, it can implement this by using the Oracle Platform Security Services APIs.
-

See Also: *Oracle Fusion Middleware Security Overview* for more information about Oracle Platform Security Services.

The account creation flow is as follows:

1. The user (using his browser) accesses the application's welcome page, which contains a **Register New Account** link.

2. The user clicks the **Register New Account** link, which takes the user to a self-registration page provided by the application.
3. The user interacts with the application to self-register.
4. On completion, the application performs an auto-login for the user.

The protected application is expected to send an SPML request to Oracle Identity Manager to create the user. After this, the application could choose to do one of the following:

- The application may choose not to auto-login the user. The application redirects the user to the protected landing page URL. Access Manager then shows the login page and takes the user through the login flow.
- If there is no approval associated with the request, the application can make use of the Oracle Platform Security Services (OPSS) APIs to conduct an auto-login to the specific landing page URL and respond with a redirect request with that URL (along with the SSO cookie). This takes the user directly to the landing page without bringing up the login page.
- Auto-login cannot be done if approval is needed. The application determines which profile to use at the time of SPML request. The application needs to respond with an appropriate page indicating that the request has been submitted.

1.5.3.3 Password Change

The Change Password flow enables users to change their password.

Password Change Flow with Access Manager and Oracle Identity Manager

In this situation, the user successfully logs into Access Manager but is required to immediately change the password. The user is not authorized to access protected resources until the password is changed and challenges have been set up.

On successful login, Access Manager detects if the triggering condition is in effect and redirects the user to the Oracle Identity Manager **Change Password** URL. Oracle Identity Manager facilitates the user password change or challenge set-up and resets the triggering condition.

On completion, Oracle Identity Manager redirects the user to the protected resource.

This situation is triggered in the following cases:

- The `Change Password upon Login` flag is on. This occurs:
 - when a new user is created
 - when the administrator resets a user's password
- The password has expired.

This flow describes the situation where a user logs in to an Access Manager-protected application for the first time, and is required to change password before proceeding.

The following describes the Change Password flow:

1. Using a browser, the user tries to access an application URL that is protected by Access Manager.
2. Oracle Access Management WebGate (SSO Agent) intercepts the request and redirects the user to the Access Manager Login Page.
3. The user submits credentials, which are validated by Access Manager.

4. Access Manager next determines if any of the First Login trigger conditions are valid. If so, Access Manager redirects the user to the Oracle Identity Manager Change Password URL.
5. Oracle Access Management WebGate (SSO Agent) intercepts the request, determines that Oracle Identity Manager is protected by the Anonymous Authentication Policy, and allows the user request to proceed.
6. Oracle Identity Manager interacts with the user to enable the user to change his password. On completion, Oracle Identity Manager updates the attributes that triggered the First Login flow. Oracle Identity Manager then performs a user auto-login.
7. Oracle Identity Manager notifies Access Manager of the successful first login.
8. Oracle Identity Manager redirects the user to the application URL the user tried to access in step 1.

1.5.3.4 Forgot Password

The Forgot Password flow allows users to reset their password after successfully answering all challenge questions.

Forgot Password Flow for Access Manager/Oracle Identity Manager Integration

In this scenario, the user is at the Access Manager Login page and clicks the **Forgot Password** link. Access Manager redirects the user to the Oracle Identity Manager **Forgot Password** URL, and passes the destination URL to which Oracle Identity Manager must redirect upon a successful password change as a query parameter (backURL).

Oracle Identity Manager asks the user the challenge questions. Upon providing the correct responses, the user is allowed to specify a new password.

On completion, Oracle Identity Manager redirects the user to the protected resource.

The Forgot Password flow is as follows:

1. Using a browser, the user tries to access an application URL that is protected by Access Manager.
2. The Oracle Access Management WebGate (SSO Agent) intercepts the request and redirects the user to the Access Manager Login Page.
3. The user clicks on the **Forgot Password** link on the Access Manager Login page, which sends the user to the Oracle Identity Manager **Forgot Password** URL.
4. Oracle Identity Manager interacts with the user to enable the user to reset the password. On completion, Oracle Identity Manager performs a user auto-login.
5. Oracle Identity Manager redirects the user to the application URL to which access was attempted in step 1.

Forgot Password Flow for Access Manager/Oracle Identity Manager/Oracle Adaptive Access Manager Integration

With Oracle Adaptive Access Manager and Oracle Identity Manager integration, the Forgot Password feature is made available as a link from the OAAM password page. The flow starts when the user is at the OAAM password page and clicks the **Forgot your password** link.

The process flow is as follows:

1. Using a browser, the user tries to access an application URL that is protected by Access Manager via an authentication scheme.
2. The Oracle Access Management WebGate (SSO Agent) intercepts the request and forwards the request to the OAAM Server for login.
3. OAAM Server presents the user with the OAAM user name page where the user submits his user name.
4. Oracle Adaptive Access Manager fingerprints the user device (a desktop computer, laptop computer, PDA, cell phone, kiosk, or other web enabled device) and runs the pre-authentication rules to check if the user is a member of a blacklisted country, device, IP, ISP, or users group or if he is using WEBZIP. If he is in a blacklisted group or using WEBZIP, he is blocked and cannot proceed.
5. If the user is allowed to proceed, virtual authentication device rules are run to determine which virtual authentication device to display on the password page.
6. OAAM Server displays the OAAM password page with the virtual authentication device.
7. The user clicks the **Forgot your password** link on the OAAM password page.

Note: The Forgot your password link is not available to unregistered users logging in for the first time. They will have to reset their password on the first logon.

8. OAAM Server runs the Forgot Password checkpoint.
9. Oracle Adaptive Access Manager presents the user with a challenge page.
 - If the user is unregistered, the user is blocked and cannot access the protected resource.
 - If the user is registered, he is challenged by OTP or KBA depending on the deployment. If challenge choice has been configured and the user has more than one OTP challenge type registered, he is given a choice of which OTP challenge type he wants OAAM to challenge him.
10. If the challenge is successful, Oracle Adaptive Access Manager makes calls to Oracle Identity Manager for the Password Policy text.
11. The user is redirected to the Password Reset page where the Password Policy text is shown.
12. The user enters the new password and confirms the new password by entering it again.
13. Oracle Adaptive Access Manager collects the user name and password and sends OAP API calls to Access Manager.
14. Access Manager makes LDAP calls to the identity store configured with Access Manager to validate credentials.
15. Oracle Adaptive Access Manager calls Oracle Identity Manager to update the repository with the new password.
16. After authentication, Oracle Adaptive Access Manager evaluates Post-Authentication checkpoint policies. Based on the outcome of the policy Oracle Adaptive Access Manager might challenge the user, check the registration of the user, or block the user.

- If the outcome of Post-Authentication is Allow then Oracle Adaptive Access Manager evaluates the Registration checkpoint to determine which pieces of user information is pending registration. Based on the types of registration it takes the user through the Registration flow.
 - If there is enough risk involved, the outcome of Post-Authentication may be Challenge. Oracle Adaptive Access Manager evaluates the Challenge checkpoint to determine if the user should be blocked or challenged with one of the registered challenge mechanism (KBA or OTP depending on the configuration) by taking the user through the Challenge flow.
 - If the outcome of Post-Authentication is Block then the user would be blocked and he will not be able to access the protected resource.
17. Oracle Adaptive Access Manager interacts with the user during the required flows and if the user is successful, Access Manager sets the OAM cookie, the user is logged in, and a single sign-on session is created.

1.5.3.5 Account Lock and Unlock

Access Manager keeps track of login attempts and locks the account when the count exceeds the established limit.

When an account is locked, Access Manager displays the Help Desk contact information and Forgot Password link, or similar.

If contacted by the end user, the Help Desk unlocks the account using the Oracle Identity Manager administrative console. Oracle Identity Manager then notifies Access Manager about the changes. If the end user decides to use the Forgot Password link instead of contacting the Help Desk, Oracle Identity Manager interacts with the user. Upon completion, the user is allowed to reset the password.

Account Lock and Unlock Flow

When the number of unsuccessful user login attempts exceeds the value specified in the password policy, the user account is locked. Any login attempt after the user account has been locked displays a page that provides information about the account unlocking process, which will need to be customized to reflect the process (Help Desk information and Forgot Password link, or similar) that is followed by your organization.

The following describes the account locking/unlocking flow:

1. Using a browser, a user tries to access an application URL that is protected by Access Manager.
2. Oracle Access Management WebGate (SSO Agent) intercepts the request and redirects the user to the Access Manager login page.
3. The user submits credentials that fail Access Manager validation. Access Manager renders the login page and asks the user to resubmit his or her credentials.
4. The user's unsuccessful login attempts exceed the limit specified by the policy. Access Manager locks the user account and redirects the user to the Access Manager Account Lockout URL. The resulting page displays the Help Desk contact information and Forgot Password link.
5. If the user contacts the Help Desk over the telephone and asks an administrator to unlock the account, then:
 - a. Oracle Identity Manager notifies Access Manager of the account unlock event.

Challenge Setup Flow for Access Manager-Oracle Identity Manager-Oracle Adaptive Access Manager Integration

In this scenario, the user is successfully authenticated but is required to register challenge questions. The user is not authorized to access protected resources until the challenge questions have been registered.

Note: When adding Oracle Adaptive Access Manager to existing Oracle Identity Manager deployments, you will need to forego all the existing questions and answers that are registered in Oracle Identity Manager. Instead, users are asked to register the challenge questions again in Oracle Adaptive Access Manager on the next login.

1. Using a browser, the user tries to access an application URL that is protected by Access Manager.
2. Oracle Access Management WebGate intercepts the (unauthenticated) request.
3. Oracle Access Management WebGate redirects the user to the OAAM Server and passes a redirect URL.
4. Oracle Adaptive Access Manager presents the user with the OAAM user name page.
5. The user submits his user name on the OAAM user name page.
6. Oracle Adaptive Access Manager fingerprints the user device (a desktop computer, laptop computer, PDA, cell phone, kiosk, or other web enabled device) and runs pre-authentication rules to determine if the user should be allowed to proceed to the OAAM password page.
7. If the user is allowed to proceed, the OAAM Server displays the OAAM password page with the strong authenticator specified by the virtual authentication device rules.
8. The user submits his password on the OAAM password page.
9. During authentication, Oracle Adaptive Access Manager calls Access Manager to validate the credentials.
10. After authentication, Oracle Adaptive Access Manager checks if the user has registered challenge questions.
11. If the user has not registered for challenges, Oracle Adaptive Access Manager interacts with the user to set up the challenges (select challenge questions and register answers and/or set up an OTP profile).
12. If the registration is successful Oracle Adaptive Access Manager redirects the user to the Access Manager protected resource.

1.5.3.7 Challenge Reset

Challenge Reset enables users to reset their challenge registration.

The flow is as follows:

1. Using a browser, the user tries to access an application URL that is protected by Access Manager.
2. Oracle Access Management WebGate intercepts the (unauthenticated) request.
3. Oracle Access Management WebGate redirects the user to the OAAM Server and passes a redirect URL.

4. The OAAM Server presents the user with the OAAM user name page.
5. The user submits his user name on the OAAM user name page.
6. Oracle Adaptive Access Manager fingerprints the user device (a desktop computer, laptop computer, PDA, cell phone, kiosk, or other web enabled device) and runs pre-authentication rules to determine if the user should be allowed to proceed to the OAAM password page.
7. If the user is allowed to proceed, the OAAM Server displays the OAAM password page with the strong authenticator specified by the virtual authentication device rules.
8. The user submits his password on the OAAM password page.
9. During authentication, Oracle Adaptive Access Manager calls Access Manager to validate the credentials.
10. If authentication is successful and the user has questions registered, but he wants to reset his challenge questions, the user clicks the Reset Challenge link.

Note: The integrator would need to have added a link to the protected application that would take users to the OAAM User Preference pages (or in some cases, directly to the OAAM Question Reset page). Adding the link allows users to manage their OAAM registration.

11. The user is redirected to Oracle Adaptive Access Manager User Preferences/Question Registration page where he can reset challenge questions.

1.5.4 Manage Mobile Security Accounts and Applications Using Identity Self-Service

The Manage Mobile Security Account flow enables users to manage their mobile security accounts and applications. The flow between Oracle Mobile Security Suite and Oracle Mobile Security Suite-integrated components is as follows:

1. The user enrolls his mobile devices in Oracle Mobile Security Suite.
2. Oracle Mobile Security Suite provisions applications to the users based on his roles.
3. The user logs in to the Oracle Identity Manager Self Service Console to:
 - view his devices
 - perform operations, such as lock, wipe, or reset passcode for his device or workspace
4. The Oracle Mobile Security Suite taskflows embedded in the Oracle Identity Manager Console invokes Oracle Mobile Security Suite to obtain information on the devices and perform operations on them.

1.6 System Requirements and Certification

Refer to the system compatibility, requirements and certification documentation for information about hardware and software requirements, platforms, databases, and other information.

The compatibility documentation describes compatibility and interoperability considerations that may arise when you install, patch, or upgrade Oracle Fusion

Middleware 11g components. For details, see *Interoperability and Compatibility Guide for Oracle Identity and Access Management*.

The system requirements document covers information such as hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches.

The certification document covers supported installation types, platforms, operating systems, databases, JDKs, directory servers, and third-party products.

For the latest requirements and certification documentation refer to the table "Oracle Fusion Middleware Certification Matrices" in the *Interoperability and Compatibility Guide for Oracle Identity and Access Management*.

1.7 Using My Oracle Support for Additional Troubleshooting Information

You can use My Oracle Support (formerly MetaLink) to help resolve Oracle Fusion Middleware problems. My Oracle Support contains several useful troubleshooting resources, such as:

- Knowledge base articles
- Community forums and discussions
- Patches and upgrades
- Certification information

Note: You can also use My Oracle Support to log a service request.

You can access My Oracle Support at <https://support.oracle.com>.

Part II

Core Integrations

This part describes integrations between certain IdM components.

This part contains the following chapters:

- [Chapter 2, "Integrating Access Manager and Oracle Identity Manager"](#)
- [Chapter 3, "Integrating Access Manager, OAAM, and OIM"](#)
- [Chapter 4, "Configuring SSL for Integrated IdM Components"](#)
- [Chapter 5, "Integrating Oracle Mobile Security Suite and Oracle Identity Manager"](#)

Integrating Access Manager and Oracle Identity Manager

This chapter provides step-by-step instructions for integrating Oracle Access Management Access Manager (Access Manager) and Oracle Identity Manager (Enterprise Edition). The exact details in this chapter may differ depending on your specific deployment. Adapt information as required for your environment.

The integration instructions assume Identity Management components have been configured on separate Oracle WebLogic domains, as discussed in "[Basic Integration Topology](#)." For prerequisite and detailed information on how the components were installed and configured in this example integration, see *Installation Guide for Oracle Identity and Access Management*.

If you are deploying Oracle Identity Management components in an enterprise integration topology, as discussed in "[The Enterprise Integration Topology](#)," see *Enterprise Deployment Guide for Oracle Identity and Access Management* for implementation procedures. If you are planning to design and deploy a high availability environment for Access Manager and Oracle Identity Manager, see *High Availability Guide* for concepts and configuration steps.

This chapter contains these sections:

- [About Oracle Identity Manager and Access Manager Integration](#)
- [Configuring LDAP Synchronization](#)
- [Configuring the Identity Store](#)
- [Configuring Access Manager for Oracle Identity Manager Integration](#)
- [Integrating Access Manager with Oracle Identity Manager](#)
- [Configuring Oracle HTTP Server to Front-End Resources on Oracle Identity Manager](#)
- [Deleting the IAMSuiteAgent Security Provider from WebLogic](#)
- [Validating the Integration](#)
- [Functionally Testing the Access Manager and Oracle Identity Manager Integration](#)
- [Troubleshooting Common Problems](#)

2.1 About Oracle Identity Manager and Access Manager Integration

This section contains the following topics:

- [Integrating Oracle Identity Manager with Access Manager](#)

- [Access Manager and Oracle Identity Manager Single-Node Integration Topology](#)
- [Access Manager and Oracle Identity Manager Integration Prerequisites](#)

2.1.1 Integrating Oracle Identity Manager with Access Manager

This integration scenario enables you to manage identities with Oracle Identity Manager and control access to resources with Oracle Access Management Access Manager. Oracle Identity Manager is a user provisioning and administration solution that automates user account management, whereas Access Manager provides a centralized and automated single sign-on (SSO) solution.

In the Oracle Access Management Access Manager (Access Manager) and Oracle Identity Manager (OIM) integration, users have the capability to:

- Create and reset the password without assistance for expired and forgotten passwords
- Recover passwords using challenge questions and answers
- Set up challenge questions and answers
- Perform self-service registration
- Perform self-service profile management
- Access multiple applications securely with one authentication step

For more information about password management flows when Access Manager and Oracle Identity Manager are integrated, see [Section 1.5.3, "Password Management Scenarios."](#)

2.1.2 Access Manager and Oracle Identity Manager Single-Node Integration Topology

You must configure Oracle Identity Management components in separate WebLogic Server domains (split domain topology), as discussed in [Section 1.2.1, "Basic Integration Topology,"](#) and separate Oracle Middleware homes. Otherwise, attempts to patch or upgrade one product may be blocked by a version dependency on a component shared with another. When you install Oracle Identity Management components in a single WebLogic Server domain, there is a risk that the component (libraries, jars, utilities, and custom plug-ins) you are installing into the domain might not be compatible with other components, thereby resulting in problems across your entire domain.

Access Manager uses a database for policy data and a directory server for identity data. This integration scenario assumes a single directory server. The directory server must also be installed in a separate domain and a separate Middleware home as well.

Note: The instructions in this chapter assume that you will use Oracle Unified Directory as the identity store. Other component configurations are possible. Refer to ["Configuring the Identity Store"](#) for more information about supported LDAP servers.

2.1.3 Access Manager and Oracle Identity Manager Integration Roadmap

[Table 2–1](#) lists the high-level tasks for integrating Access Manager and Oracle Identity Manager with Oracle Unified Directory.

Depending on your installation path, you may already have performed some of the integration procedures listed in this table. For details on the installation roadmap, see [Section 1.1.1, "Understanding the Installation Roadmap."](#)

Table 2–1 Integration Flow for Access Manager and Oracle Identity Manager

No.	Task	Information
1	Verify that all required components have been installed and configured prior to integration.	For more information, see Access Manager and Oracle Identity Manager Integration Prerequisites .
2	Configure LDAP synchronization for Oracle Identity Manager if LDAP synchronization was not enabled during OIM installation.	For more information, see Configuring LDAP Synchronization .
3	Configure the identity store by extending the schema.	For information, see Extending Directory Schema for Access Manager .
4	Configure the identity store with the users required by Access Manager.	For information, see Creating Users and Groups for Access Manager .
5	Configure the identity store with the users required by Oracle Identity Manager.	For information, see Creating Users and Groups for Oracle Identity Manager .
6	Configure the identity store with the users required by Oracle WebLogic Server	For more information, see Creating Users and Groups for Oracle WebLogic Server .
7	Stop the Oracle WebLogic Server managed servers for Access Manager and Oracle Identity Manager	For information, see "Stopping the Stack" in <i>Installation Guide for Oracle Identity and Access Management</i> .
8	Extend Access Manager to support Oracle Identity Manager	For information, see Configuring Access Manager for Oracle Identity Manager Integration .
9	Integrate Access Manager and Oracle Identity Manager	For information, see Integrating Access Manager with Oracle Identity Manager .
10	Configure the WebGate on the Oracle HTTP Server (OHS) to point to the 11g OAM Server	For information, see Configuring Oracle HTTP Server to Front-End Resources on Oracle Identity Manager .
11	Delete IAMSuiteAgent (the IDM Domain Agent) and restart the Oracle WebLogic Server Administration and Managed Servers.	For information, see Deleting the IAMSuiteAgent Security Provider from WebLogic .
12	Test the integration.	For information, see Functionally Testing the Access Manager and Oracle Identity Manager Integration .

2.1.4 Access Manager and Oracle Identity Manager Integration Prerequisites

In the following sections it is assumed that the required components, as listed in [Table 2–2](#), have already been installed, including any dependencies, and the environment already configured prior to the integration. For more information about the integration topologies, see [Section 1.2, "Integration Topologies."](#)

Table 2–2 Required Components for Integration Scenario

Component	Information
Oracle HTTP Server with 11g WebGate or 10g WebGate	<p>Oracle HTTP Server with 11g WebGate or 10g WebGate is installed.</p> <p>For information about the installation and registration of the 10g WebGates for use with Access Manager 11g, see "Registering and Managing 10g WebGates with Access Manager 11g" in <i>Administrator's Guide for Oracle Access Management</i>.</p> <p>For information about the installation and registration of the 11g WebGate for use with Access Manager 11g, see "Installing and Configuring Oracle HTTP Server 11g WebGate for OAM" in <i>Oracle Fusion Middleware Installing Webgates for Oracle Access Manager</i>.</p> <p>The Oracle HTTP Server (OHS) profile must have been updated before the Oracle Identity Manager administration pages can launch correctly after the integration with Access Manager is completed. For more information, see Configuring Oracle HTTP Server to Front-End Resources on Oracle Identity Manager.</p>
Oracle SOA Suite	<p>Oracle Identity Manager requires Oracle SOA Suite 11g Release 1 (11.1.1.9.0), which is exclusive to Oracle Identity and Access Management.</p> <p>SOA Suite is a prerequisite for Oracle Identity Manager and must be installed in the same domain as Oracle Identity Manager. If you use SOA Suite for other purposes, a separate install must be set up for running your own services, composites, BPEL processes, and so on.</p> <p>For more information see <i>Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite</i></p>
Oracle Unified Directory	<p>Oracle Unified Directory is installed.</p> <p>The instructions in this chapter assume that you will use Oracle Unified Directory as the identity store. Other component configurations are possible. Refer to "Configuring the Identity Store" for more information about supported LDAP servers.</p> <p>For information on Oracle Unified Directory, see <i>Administering Oracle Unified Directory</i>.</p>
Access Manager	<p>Access Manager is already installed.</p> <p>For information on the configuration, see "Configuring Oracle Access Management" in <i>Installation Guide for Oracle Identity and Access Management</i>.</p>
Oracle Identity Manager	<p>Oracle Identity Manager is already installed and configured with the Enable OIM for Suite integration option selected. Ensure that you have followed the steps for the LDAP directory that you want to configure. See "Configuring Oracle Identity Manager Server" in <i>Installation Guide for Oracle Identity and Access Management</i>.</p> <p>For information on the installation of Oracle Identity Manager, see "Installing and Configuring Oracle Identity and Access Management" and "Configuring Oracle Identity Manager" in <i>Installation Guide for Oracle Identity and Access Management</i>.</p>

Table 2–2 (Cont.) Required Components for Integration Scenario

Component	Information
wlfullclient.jar file	Oracle Identity Manager uses the <code>wlfullclient.jar</code> library for certain operations. Oracle does not ship this library, so you must create this library manually as a post-configuration step of Oracle Identity Manager configuration. This file must be present before performing the integration steps. If this file does not exist the IDM Configuration Tool will not be able to connect to the database properly. For information on the creation of the <code>wlfullclient.jar</code> , see "Post-Configuration Steps" in <i>Installation Guide for Oracle Identity and Access Management</i> .

2.2 Configuring LDAP Synchronization

LDAP synchronization is a requirement for Access Manager and Oracle Identity Manager integration.

If you selected the **Enable OIM for Suite integration** option during the Oracle Identity Manager Server configuration, LDAP synchronization has been enabled, Oracle Identity Manager is integrated with Oracle Unified Directory and users and groups created in Oracle Identity Manager will synchronize automatically with Oracle Unified Directory. You still need to run the LDAP Post-Configuration Utility to enable all the LDAP synchronization-related incremental Reconciliation Scheduler jobs, which are disabled by default. The LDAP Post-Configuration Utility also retrieves the last change number from the Directory Server and updates all the LDAP Sync Incremental Reconciliation jobs. For instructions on running the LDAP Post-Configuration Utility, see [Section E.2.1, "Running the LDAP Post-Configuration Utility."](#)

If you did not enable LDAP synchronization during Oracle Identity Manager Server configuration, you must manually configure LDAP Synchronization following the instructions in [Section E.1, "Configuring LDAP Synchronization."](#)

2.3 Configuring the Identity Store

If you are integrating Access Manager with Oracle Identity Manager, you must extend the Access Manager schema to support Oracle Identity Manager and seed the identity store with users and groups for use by Access Manager, Oracle Identity Manager, and Oracle WebLogic Server.

This section contains the following topics:

- [Extending Directory Schema for Access Manager](#)
- [Creating Users and Groups for Access Manager](#)
- [Creating Users and Groups for Oracle Identity Manager](#)
- [Creating Users and Groups for Oracle WebLogic Server](#)
- [Creating Readonly user, ReadWrite user and Superuser for Oracle Fusion Applications](#)

Supported LDAP Servers are Oracle Internet Directory, Oracle Unified Directory, Oracle Virtual Directory (used as virtualization), Oracle Directory Server Enterprise Edition, and Active Directory.

For information on Oracle Unified Directory, Oracle Internet Directory, Oracle Virtual Directory (used as virtualization), Oracle Directory Server Enterprise Edition, and Active Directory, refer to the following:

- For information on Oracle Unified Directory, see *Administering Oracle Unified Directory*.
- For information on Oracle Internet Directory, see *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.
- For information on Oracle Virtual Directory, see *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.
- For information on Oracle Directory Server Enterprise Edition, see *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Server Enterprise Edition*.
- For information on Active Directory, see *Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management*.

The IdM configuration tool (`idmConfigTool`) supports a number of tasks to assist in installing, configuring, and integrating Oracle Identity Management (IdM) components. You can use the IdM Configuration Tool only if Oracle Internet Directory (OID) or Oracle Unified Directory (OUD) is used as the identity store or if standalone Oracle Virtual Directory (OVD) is used for virtualization. The IDM Configuration Tool does not support Oracle Directory Server Enterprise Edition (ODSEE) or Active Directory (AD) where they are used as the identity store. In these cases, you must perform manual configuration steps. For `preconfigIDStore`, and `prepareIDStore mode=OIM, OAM` and `WLS` commands in `idmConfigTool`, the equivalent manual steps are documented for AD and ODSEE in the following sections:

- [Section E.1.1.1, "Preconfiguring Active Directory"](#)
- [Section E.1.1.2, "Preconfiguring ODSEE"](#)

Note: Ensure that the Access Manager and Oracle Identity Manager Administration servers and LDAP server are up and running before running the `idmConfigTool` command. For more information, see "Starting the Stack" in *Installation Guide for Oracle Identity and Access Management*.

2.3.1 Extending Directory Schema for Access Manager

Before you can use your LDAP directory as an identity store, you must preconfigure it by using the IDM Configuration Tool. This extends the schema in the LDAP directory to include the object classes required by the Access Manager, Oracle Identity Manager, and WebLogic Server. Once it has been extended users are seeded into the directory for later use.

1. If you are using Oracle Unified Directory as the identity store, retrieve the Oracle Unified Directory keystore password from the `admin-keystore.pin` file located at:

```
OID_ORACLE_INSTANCE/OUD/config
```

The keystore password is required for Oracle Unified Directory identity stores. You will use this value when you create the properties file in Step 2.

2. Create a properties file called `extendOAMPropertyFile` with contents similar to the following example. The `extendOAMPropertyFile` file must contain configuration information specific to your environment. You will use this file to configure the LDAP identity store when you run the `idmConfigTool` command.

Do not include any blank lines when creating the file.

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
```

```

IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_DIRECTORYTYPE: OUD
IDSTORE_ADMIN_PORT : 4444
IDSTORE_KEYSTORE_FILE : /u01/config/instances/oud1/OUd/config/admin-keystore
IDSTORE_KEYSTORE_PASSWORD : 4VYGtJLG61V50jDWKe94e601x7tgLFs

```

Table 2–3 provides descriptions of the parameters in the `extendOAMPropertyFile` configuration file example.

Table 2–3 *extendOAMPropertyFile Properties*

Property	Description
IDSTORE_HOST	Identity store host name. <ul style="list-style-type: none"> If your identity store is in Oracle Internet Directory or Oracle Unified Directory, then <code>IDSTORE_HOST</code> points directly to the Oracle Internet Directory or Oracle Unified Directory host. If your identity store is fronted by Oracle Virtual Directory, then <code>IDSTORE_HOST</code> points to the Oracle Virtual Directory host, which should be <code>IDSTORE.example.com</code>.
IDSTORE_PORT	Identity store port.
IDSTORE_BINDDN	An administrative user in the identity store directory.
IDSTORE_USERNAMEATTRIBUTE	Username attribute used to set and search for users in the identity store. If the user DN is <code>cn=orcladmin, cn=Users, dc=us, dc=example, dc=com</code> , this property should be set to <code>cn</code> .
IDSTORE_LOGINATTRIBUTE	Login attribute of the identity store that contains the user's login name. This is the attribute the user uses for login, for example <code>uid</code> or <code>email</code> .
IDSTORE_USERSEARCHBASE	Location in the directory where users are stored. This property tells the directory where to search for users.
IDSTORE_GROUPSEARCHBASE	Location in the directory where groups (or <i>roles</i>) are stored. This property tells the directory where to search for groups or roles.

Table 2–3 (Cont.) extendOAMPropertyFile Properties

Property	Description
IDSTORE_SEARCHBASE	<p>Location in the directory where users and groups are stored.</p> <p>This property is the parent location that contains the USERSEARCHBASE and the GROUPSEARCHBASE.</p> <p>For example:</p> <pre>IDSTORE_SEARCHBASE: cn=oracleAccounts, dc=example,dc=com IDSTORE_USERSEARCHBASE: cn=Users,cn=oracleAccounts,dc=example,dc=com IDSTORE_GROUPSEARCHBASE: cn=Groups,cn=oracleAccounts,dc=example,dc=com</pre>
IDSTORE_SYSTEMIDBASE	<p>Location of a container in the directory where system operations users are stored.</p> <p>This is so they are kept separate from enterprise users stored in the main user container.</p> <p>There are only a few system operations users. One example is the Oracle Identity Manager reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.</p>
IDSTORE_DIRECTORYTYPE	<p>Identity store directory type.</p> <p>OULD if your identity store is in Oracle Unified Directory and you are accessing it directly rather than through OVD.</p> <p>If you are not using Oracle Unified Directory, you can leave out this parameter.</p>
IDSTORE_ADMIN_PORT	<p>Administration port of your Oracle Unified Directory instance. If you are not using Oracle Unified Directory, you can leave out this parameter.</p>
IDSTORE_KEYSTORE_FILE	<p>Location of the Oracle Unified Directory Keystore file. It is used to enable communication with Oracle Unified Directory using the Oracle Unified Directory administration port. It is called admin-keystore and is located in <code>OULD_ORACLE_INSTANCE/OULD/config</code>. If you are not using Oracle Unified Directory, you can leave out this parameter. This file must be located on the same host that the <code>idmConfigTool</code> command is running on. The command uses this file to authenticate itself with OUD.</p>
IDSTORE_KEYSTORE_PASSWORD	<p>Encrypted password of the Oracle Unified Directory keystore. This value can be found in the file <code>OULD_ORACLE_INSTANCE/OULD/config/admin-keystore.pin</code>. If you are not using Oracle Unified Directory, you can leave out this parameter.</p>

3. Set the environment variables required for the `idmconfigtool` command. For information on setting environment variables, see [Section D.2, "Set Up Environment Variables."](#)

4. Change the directory to the `IAM_ORACLE_HOME/idmtools/bin` directory:

```
cd IAM_ORACLE_HOME/idmtools/bin
```


You will be running the `idmConfigTool` command from the `IAM_ORACLE_HOME/idmtools/bin` directory.

5. Configure the identity store by running the `idmConfigTool` command with the `-preConfigIDStore` command option.

`IAM_ORACLE_HOME/idmtools/bin`

Note: The `-preConfigIDStore` command option supports Oracle Internet Directory, Oracle Unified Directory, and Oracle Virtual Directory.

On Linux, the command syntax is:

```
idmConfigTool.sh -preConfigIDStore input_file=configfile
```

On Windows, the command syntax is:

```
idmConfigTool.bat -preConfigIDStore input_file=configfile
```

For example:

```
idmConfigTool.sh -preConfigIDStore input_file=extendOAMPropertyFile
```

For information on `preConfigIDStore`, see [Section D.4.1, "preConfigIDStore Command."](#)

When the command runs, you are prompted to enter the password of the account used to connect to the identity store.

Sample command output, when running the command against Oracle Unified Directory, is shown as follows:

```
Enter ID Store Bind DN password :
Dec 30, 2014 1:01:52 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1/oam/server/oim-intg/ldif/ojd/schema/ojd_oam_pwd_schema_add.ldif
.
.
.
This tool has completed its operation. Details have been logged to
automation.log
```

6. Check the log file for any errors or warnings and correct them. The file with the name `automation.log` is created in the directory from where you run the `idmconfigtool`. The tool is reentrant and can be safely called again.

In addition to creating users, `idmConfigTool` creates following groups:

- `OrclPolicyAndCredentialWritePrivilegeGroup`
- `OrclPolicyAndCredentialReadPrivilegeGroup`

2.3.2 Creating Users and Groups for Access Manager

Use the IDM Configuration Tool to seed the identity store with the users required by Access Manager.

The `idmConfigTool` command creates:

- The oamLDAP user under `cn=systemids,dc=example,dc=com`. The oamLDAP user is used to connect to LDAP from Access Manager.
- The oamadmin user under `cn=Users,dc=example,dc=com`. The oamadmin user is the administrator of the Oracle Access Management Console.
- The OAMAdministrators group. `idmConfigTool` assigns the oamadmin user to this group.

To seed the identity store, proceed as follows:

1. If you are using Oracle Unified Directory as the identity store, perform these steps:

- a. Copy the Oracle Unified Directory Keystore file `admin-keystore` from the Oracle Unified Directory server to the OAM Admin Server machine. The file is located in the following directory on the Oracle Unified Directory server:

```

    OUD_ORACLE_INSTANCE/OU/Config
  
```

You will use the path on the local machine when you create the properties file in Step 2.

- b. Retrieve the Oracle Unified Directory keystore password from the `admin-keystore.pin` file located at:

```

    OUD_ORACLE_INSTANCE/OU/Config
  
```

The keystore password is required for Oracle Unified Directory identity stores. You will use this value when you create the properties file in Step 2.

2. Create a properties file called `preconfigOAMPropertyFile` with contents similar to the following. The `preconfigOAMPropertyFile` file must contain configuration information specific to your environment. This file will be used to create the required users and groups for Access Manager when you run the `idmConfigTool` command.

Do not include any blank lines when creating the file.

```

IDSTORE_HOST : idstore.example.com
IDSTORE_PORT : 389
IDSTORE_BINDDN : cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN:OAMAdministrators
IDSTORE_OAMSOFTWAREUSER:oamLDAP
IDSTORE_OAMADMINUSER:oamadmin
IDSTORE_DIRECTORYTYPE: OUD
IDSTORE_ADMIN_PORT : 4444
IDSTORE_KEYSTORE_FILE : <path to file copied from oud install>
IDSTORE_KEYSTORE_PASSWORD : 4VYGtJLG61V50jDWKe94e601x7tgLFs
  
```

[Table 2-4](#) provides descriptions of the parameters in the `preconfigOAMPropertyFile` configuration file example.

Table 2–4 *preconfigOAMPropertyFile Properties*

Properties	Description
IDSTORE_HOST	Identity store host name. <ul style="list-style-type: none"> ■ If your identity store is in Oracle Internet Directory or Oracle Unified Directory, then point IDSTORE_HOST to Oracle Internet Directory or Oracle Unified Directory, even if you are fronting Oracle Internet Directory with Oracle Virtual Directory. ■ If you are using a directory other than Oracle Internet Directory or Oracle Unified Directory, specify the Oracle Virtual Directory host.
IDSTORE_PORT	Identity store port.
IDSTORE_BINDDN	An administrative user in the identity store directory.
IDSTORE_USERNAMEATTRIBUTE	Username attribute used to set and search for users in the identity store. For example, if the user DN is <code>cn=orcladmin,cn=Users,dc=us,dc=example,dc=com</code> , this property should be set to <code>cn</code> .
IDSTORE_LOGINATTRIBUTE	Login attribute of the identity store that contains the user's login name. This is the attribute the user uses for login, for example <code>uid</code> or <code>email</code> .
IDSTORE_USERSEARCHBASE	Location in the directory where users are stored. This property tells the directory where to search for users.
IDSTORE_GROUPSEARCHBASE	Location in the directory where groups (or <i>roles</i>) are stored. This property tells the directory where to search for groups or roles.
IDSTORE_SEARCHBASE	Location in the directory where users and groups are stored. This property is the parent location that contains the <code>USERSEARCHBASE</code> and the <code>GROUPSEARCHBASE</code> .
POLICYSTORE_SHARES_IDSTORE	true if your policy and identity stores are in the same directory. If not, it is set to false.
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	Group used to allow access to the Oracle Access Management Administration Console.
IDSTORE_OAMSOFTWAREUSER	Directory user that Access Manager will use to interact with the directory or LDAP server. This user is created by the tool.
IDSTORE_OAMADMINUSER	User you want to create as your Oracle Access Management Administrator. This user is created by the tool.

Table 2–4 (Cont.) preconfigOAMPropertyFile Properties

Properties	Description
IDSTORE_DIRECTORYTYPE	Identity store directory type. OUD if your identity store is in Oracle Unified Directory and you are accessing it directly rather than through OVD. If you are not using Oracle Unified Directory, you can leave out this parameter.
IDSTORE_ADMIN_PORT	Administration port of your Oracle Unified Directory instance. If you are not using Oracle Unified Directory, you can leave out this parameter.
IDSTORE_KEYSTORE_FILE	Location of the Oracle Unified Directory Keystore file. It is used to enable communication with Oracle Unified Directory using the Oracle Unified Directory administration port. It is called admin-keystore and is located in <code>OUD_ORACLE_INSTANCE/OUDD/config</code> . If you are not using Oracle Unified Directory, you can leave out this parameter. This file must be located on the same host that the idmConfigTool command is running on. The command uses this file to authenticate itself with OUD.
IDSTORE_KEYSTORE_PASSWORD	Encrypted password of the Oracle Unified Directory keystore. This value can be found in the file <code>OUD_ORACLE_INSTANCE/OUDD/config/admin-keystore.pin</code> . If you are not using Oracle Unified Directory, you can leave out this parameter.

3. Set the environment variables required for the `idmconfigtool` command. For information on setting environment variables, see [Section D.2, "Set Up Environment Variables."](#)

4. Change the directory to the `IAM_ORACLE_HOME/idmtools/bin` directory:

```
cd IAM_ORACLE_HOME/idmtools/bin
```

You will be running the `idmConfigTool` command from the `IAM_ORACLE_HOME/idmtools/bin` directory.

5. Configure the identity store by running the `idmConfigTool` command with the `-prepareIDStore mode=OAM` command option.

On Linux, the command syntax is:

```
idmConfigTool.sh -prepareIDStore mode=OAM input_file=configfile
```

On Windows, the command syntax is:

```
idmConfigTool.bat -prepareIDStore mode=OAM input_file=configfile
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=OAM input_file=preconfigOAMPropertyFile
```

For information on `prepareIDStore mode=OAM`, see [Section D.4.2.1, "prepareIDStore mode=OAM."](#)

The command prompts you to enter the password for the account used to connect to the identity store. You are then prompted to create passwords for the following three accounts:

- **oblixanonymous**
The Oblix anonymous user account. It is the public user.
- **oamadmin**
The OAM administrator account. It is used to log in to the Oracle Access Management Console.
- **oamLDAP**
The OAM LDAP account. It is used to connect to Access Manager to the identity store for authentication.

Sample command output, when running the command against Oracle Unified Directory, is shown as follows:

```
Enter ID Store Bind DN password :
*** Creation of Oblix Anonymous User ***
Dec 30, 2014 1:53:55 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1//idmtools/templates/oud/oam_10g_anonymous_user_template.ldif
Enter User Password for oblixanonymous:
Confirm User Password for oblixanonymous:
*** Creation of oamadmin ***
Dec 30, 2014 1:54:46 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1//idmtools/templates/oud/oam_user_template.ldif
Enter User Password for oamadmin:
Confirm User Password for oamadmin:
*** Creation of oamLDAP ***
Dec 30, 2014 1:55:19 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1//idmtools/templates/oud/oim_user_template.ldif
Enter User Password for oamLDAP:
Confirm User Password for oamLDAP:
Dec 30, 2014 1:55:57 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1//idmtools/templates/common/oam_user_group_read_acl_template.ldif
.
.
.
*** Creation of CO ***
Dec 30, 2014 1:55:58 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1//idmtools/templates/common/orgunit_template.ldif
*** Creation of People ***
Dec 30, 2014 1:55:58 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1//idmtools/templates/common/orgunit_template.ldif
*** Creation of vgoLocator ***
Dec 30, 2014 1:55:58 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1//idmtools/templates/common/orgunit_template.ldif
*** Creation of default vgoLocator ***
Dec 30, 2014 1:55:58 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1//idmtools/templates/common/esso_default.ldif
*** Creation of ESSO acl ***
```

```
Dec 30, 2014 1:55:58 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1//idmtools/templates/oud/esso_acl.ldif
The tool has completed its operation. Details have been logged to
automation.log
```

6. The automation.log file is created in the directory where you ran the tool. Check the log file for any errors or warnings and correct them. The tool is reentrant and can be safely called again.

2.3.3 Creating Users and Groups for Oracle Identity Manager

Use the IDM Configuration Tool to create the following users:

- oimLDAP

System user in LDAP under `cn=systemids,dc=example,dc=com` and associated with the OIMAdministrators group.

A system user is required for performing operations in Oracle Unified Directory or Oracle Internet Directory on behalf of Oracle Identity Manager.

The IDM Configuration Tool creates this user in the system container and gives it the permissions appropriate for controlling all the containers Oracle Identity Manager communicates with. Oracle Unified Directory or Oracle Internet Directory uses these credentials to connect to the backend directories.

The oimLDAP user credentials are used for communication to LDAP from Oracle Identity Manager.

- xelsysadm

Oracle Identity Manager System Administrator in LDAP

To seed the identity store with the xelsysadm user and assign it to an Oracle Identity Manager administrative group and create the oimLDAP system user with the appropriate permissions, proceed as follows:

Note: Skip this step if you have created the users already as part of the manual configuration of LDAP synchronization. For details, see [Section E.1.1, "Completing the Prerequisites for Enabling LDAP Synchronization."](#)

1. If you are using Oracle Unified Directory as the identity store, perform these steps:
 - a. Copy the Oracle Unified Directory Keystore file `admin-keystore` from the Oracle Unified Directory server to the OIM Admin Server machine. The file is located in the following directory on the Oracle Unified Directory server:

```
OID_ORACLE_INSTANCE/OID/config
```

You will use the path on the local machine when you create the properties file in Step 2.

- b. Retrieve the Oracle Unified Directory keystore password from the `admin-keystore.pin` file located at:

```
OID_ORACLE_INSTANCE/OID/config
```

The keystore password is required for Oracle Unified Directory identity stores. You will use this value when you create the properties file in Step 2.

2. Create a properties file called `preconfigOIMPropertyFile` with contents similar to the following. The `preconfigOIMPropertyFile` file must contain configuration information specific to your environment. This file will be used to create the required users and groups for Oracle Identity Manager when you run the `idmConfigTool` command.

Do not include any blank lines when creating the file.

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_OIMADMINUSER: oimLDAP
IDSTORE_OIMADMINGROUP: OIMAdministrators
IDSTORE_DIRECTORYTYPE: OUD
IDSTORE_ADMIN_PORT : 4444
IDSTORE_KEYSTORE_FILE : <path to file copied from oud install>
IDSTORE_KEYSTORE_PASSWORD : 4VYGtJLG61V50jDWKe94e601x7tgLFs
```

Table 2–5 provides descriptions of the parameters in the `preconfigOIMPropertyFile` configuration file example.

Table 2–5 *preconfigOIMPropertyFile Properties*

Properties	Description
IDSTORE_HOST	Identity store host name. <ul style="list-style-type: none"> ■ If your identity store is in Oracle Internet Directory or Oracle Unified Directory, then point <code>IDSTORE_HOST</code> directly to the Oracle Internet Directory or Oracle Unified Directory host. ■ If your identity store is fronted by Oracle Virtual Directory, then point <code>IDSTORE_HOST</code> to the Oracle Virtual Directory host, which should be <code>IDSTORE.example.com</code>.
IDSTORE_PORT	Identity store port.
IDSTORE_BINDDN	An administrative user in the identity store directory.
IDSTORE_USERNAMEATTRIBUTE	Username attribute used to set and search for users in the identity store.
IDSTORE_LOGINATTRIBUTE	Login attribute of the identity store which contains the user's login name.
IDSTORE_USERSEARCHBASE	Location in your identity store where users are placed.
IDSTORE_GROUPSEARCHBASE	Location in your identity store where groups are placed.
IDSTORE_SEARCHBASE	Location in the directory where users and groups are stored.
POLICYSTORE_SHARES_IDSTORE	true if your policy and identity stores are in the same directory. If not, it is set to false.
IDSTORE_SYSTEMIDBASE	Location in your directory where the Oracle Identity Manager reconciliation user is placed.

Table 2–5 (Cont.) preconfigOIMPropertyFile Properties

Properties	Description
IDSTORE_OIMADMINUSER	User that Oracle Identity Manager uses to connect to the identity store.
IDSTORE_OIMADMINGROUP	Group you want to create to hold your Oracle Identity Manager administrative users.
IDSTORE_DIRECTORYTYPE	Identity store directory type. OUD if your identity store is in Oracle Unified Directory and you are accessing it directly rather than through OVD. If you are not using Oracle Unified Directory, you can leave out this parameter.
IDSTORE_ADMIN_PORT	Administration port of your Oracle Unified Directory instance. If you are not using Oracle Unified Directory, you can leave out this parameter.
IDSTORE_KEYSTORE_FILE	Location of the Oracle Unified Directory Keystore file. It is used to enable communication with Oracle Unified Directory using the Oracle Unified Directory administration port. It is called admin-keystore and is located in <code>OUD_ORACLE_INSTANCE/OUd/config</code> . If you are not using Oracle Unified Directory, you can leave out this parameter. This file must be located on the same host that the <code>idmConfigTool</code> command is running on. The command uses this file to authenticate itself with OUD.
IDSTORE_KEYSTORE_PASSWORD	Encrypted password of the Oracle Unified Directory keystore. This value can be found in the file <code>OUD_ORACLE_INSTANCE/OUd/config/admin-keystore.pin</code> . If you are not using Oracle Unified Directory, you can leave out this parameter.

3. Set the environment variables required for the `idmconfigtool` command. For information on setting environment variables, see [Section D.2, "Set Up Environment Variables."](#)

4. Change the directory to the `IAM_ORACLE_HOME/idmtools/bin` directory:

```
cd IAM_ORACLE_HOME/idmtools/bin
```

You will be running the `idmConfigTool` command from the `IAM_ORACLE_HOME/idmtools/bin` directory.

5. Configure the identity store by using the `idmConfigTool` command with the `-prepareIDStore mode=OIM` command option.

On Linux, the command syntax is:

```
idmConfigTool.sh -prepareIDStore mode=OIM input_file=configfile
```

On Windows, the command syntax is:

```
idmConfigTool.bat -prepareIDStore mode=OIM input_file=configfile
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=OIM input_file=preconfigOIMPropertyFile
```

For information on `prepareIDStore mode=OIM`, see [Section D.4.2.2, "prepareIDStore mode=OIM."](#)

When the command runs, you are prompted to enter the password of the account used to connect to the identity store. The command also asks you to create passwords for the following two accounts:

- IDSTORE_OIMADMINUSER
- xelsysadm. This value should match the value you create as part of the Oracle Identity Manager configuration.

Sample command output, when running the command against Oracle Unified Directory, is shown as follows:

```
Enter ID Store Bind DN password :
***Creation of oimLDAP***
Jan 28, 2015 9:27:00 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO:-> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1/idmtools/templates/oud/oim_user_template.ldif
Enter User Password for oimLDAP:
Confirm User Password for oimLDAP:
***Add password reset privilege to oimLDAP***
Jan 28, 2015 9:27:01 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO:-> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1/idmtools/templates/oud/add_pwd_reset_privilege.ldif
.
.
.
***Creation of Xel Sys Admin User***
Jan 28, 2015 9:27:01 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1/idmtools/templates/oud/idm_xelsysadmin_user.ldif
Enter User Password for xelsysadm:
Confirm User Password for xelsysadm:
Jan 28, 2015 9:27:01 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1/idmtools/templates/oud/oud_set_lockout_failure_count.ldif
The tool has completed its operation. Details have been logged to
automation.log
```

6. The automation.log file is created in the directory where you run the tool. Check the log file for any errors or warnings and correct them. The tool is reentrant and can be safely called again.

2.3.4 Creating Users and Groups for Oracle WebLogic Server

To enable single sign-on for your administration consoles, you must ensure that there is a user in your identity store who has the permissions to log in to your Oracle WebLogic Administration Console and Oracle Enterprise Manager Fusion Middleware Control. Use the IDM Configuration Tool to seed the identity store with the users required by WebLogic Server as follows.

The following steps create a domain administrator for WebLogic (weblogic_idm), whose credentials will be used to add Oracle Identity Manager resource policies to the Access Manager configuration when the configOIM command is run.

1. Create a properties file called preconfigWLSPropertyFile with contents similar to the following. The preconfigWLSPropertyFile file must contain configuration information specific to your environment. This file will be used to create the required users and groups for Oracle WebLogic Server when you run the idmConfigTool command.

Do not include any blank lines when creating the file.

```

IDSTORE_HOST : idstore.example.com
IDSTORE_PORT : 389
IDSTORE_BINDDN : cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_WLSADMINUSER: weblogic_idm
IDSTORE_WLSADMINGROUP: wlsadmingroup
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
    
```

Table 2–6 provides descriptions of the parameters in the `preconfigWLSPropertyFile` configuration file example.

Table 2–6 *preconfigWLSPropertyFile Properties*

Properties	Description
IDSTORE_HOST	Identity store host name. <ul style="list-style-type: none"> ▪ If your identity store is in Oracle Internet Directory or Oracle Unified Directory, then point IDSTORE_HOST to Oracle Internet Directory or Oracle Unified Directory, even if you are fronting Oracle Internet Directory with Oracle Virtual Directory. ▪ If you are using a directory other than Oracle Internet Directory or Oracle Unified Directory, specify the Oracle Virtual Directory host (which should be <code>IDSTORE.example.com</code>.)
IDSTORE_PORT	Identity store port.
IDSTORE_BINDDN	Administrative user in the identity store directory.
IDSTORE_USERNAMEATTRIBUTE	Username attribute used to set and search for users in the identity store.
IDSTORE_LOGINATTRIBUTE	Login attribute of the identity store that contains the user's login name.
IDSTORE_WLSADMINUSER	Identity store administrator for Oracle WebLogic Server.
IDSTORE_WLSADMINGROUP	Identity store administrator group for Oracle WebLogic Server.
IDSTORE_USERSEARCHBASE	Location in the directory where users are stored.
IDSTORE_GROUPSEARCHBASE	Location in the directory where groups are stored.
IDSTORE_SEARCHBASE	Location in the directory where users and groups are stored.
POLICYSTORE_SHARES_IDSTORE	true if your policy and identity stores are in the same directory. If not, it is set to false.

2. Set the environment variables required for the `idmconfigtool` command. For information on setting environment variables, see [Section D.2, "Set Up Environment Variables."](#)

3. Change the directory to the `IAM_ORACLE_HOME/idmtools/bin` directory:

```
cd IAM_ORACLE_HOME/idmtools/bin
```

You will be running the `idmConfigTool` command from the `IAM_ORACLE_HOME/idmtools/bin` directory.

4. Configure the identity store by using the `idmConfigTool` with the `-prepareIDStore mode=WLS` command option.

On Linux, the command syntax is:

```
idmConfigTool.sh -prepareIDStore mode=WLS input_file=configfile
```

On Windows, the command syntax is:

```
idmConfigTool.bat -prepareIDStore mode=WLS input_file=configfile
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=WLS input_file=preconfigWLSPropertyFile
```

For information on `-prepareIDStore mode=WLS`, see [Section D.4.2.4, "prepareIDStore mode=WLS."](#)

The command prompts you to enter the password for the account used to connect to the identity store. You are then prompted to create a password for the following account:

- WebLogic administrative user (`weblogic_idm`)

Sample command output, when running the command against Oracle Unified Directory, is shown as follows:

```
Enter ID Store Bind DN password :
*** Creation of Weblogic Admin User ***
Dec 10, 2014 1:43:30 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1/idmtools/templates/oud/oam_user_template.ldif
Enter User Password for weblogic_idm:
Confirm User Password for weblogic_idm:
Dec 10, 2014 1:44:12 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1/idmtools/templates/oud/weblogic_admin_group.ldif
Dec 10, 2014 1:44:12 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /scratch/user1/Oracle/middleware/Oracle_
IDM1/idmtools/templates/common/group_member_template.ldif
The tool has completed its operation. Details have been logged to
automation.log
```

5. The `automation.log` file is created in the directory where you run the tool. Check the log file for any errors or warnings and correct them. The tool is reentrant and can be safely called again.

2.3.5 Creating Readonly user, ReadWrite user and Superuser for Oracle Fusion Applications

Oracle Fusion Applications requires several users and groups to be created in the Identity Store. Use the IDM Configuration Tool to seed the identity store with the `readOnly` user, `readWrite` user, and `superuser` and create the following groups:

- `orclFAGroupReadPrivilegeGroup`
- `orclFAGroupWritePrivilegeGroup`
- `orclFAUserReadPrivilegeGroup`

- orclFAUserWritePrefsPrivilegeGroup
- orclFAUserWritePrivilegeGroup

In addition to creating the users and groups, idmConfigTool assigns the readOnly user to the orclFAGroupReadPrivilegeGroup, orclFAUserReadPrivilegeGroup and orclFAUserWritePrefsPrivilegeGroup groups and assigns the readWrite user to the orclFAUserWritePrivilegeGroup and orclFAGroupWritePrivilegeGroup groups.

The following steps create users and groups and add the readOnly and readWrite users to their appropriate groups.

1. If you are using Oracle Unified Directory as the identity store, perform these steps:

- a. Copy the Oracle Unified Directory Keystore file admin-keystore from the Oracle Unified Directory server to the OIM Admin Server machine. The file is located in the following directory on the Oracle Unified Directory server:

```

OULD_ORACLE_INSTANCE/OULD/config

```

You will use the path on the local machine when you create the properties file in Step 2.

- b. Retrieve the Oracle Unified Directory keystore password from the admin-keystore.pin file located at:

```

OULD_ORACLE_INSTANCE/OULD/config

```

The keystore password is required for Oracle Unified Directory identity stores. You will use this value when you create the properties file in Step 2.

2. Create a preconfigFAPropertyFile properties file with contents similar to the following. The preconfigFAPropertyFile file must contain configuration information specific to your environment. This file will be used to create the required users and add them to the appropriate groups when you run the idmConfigTool command.

Do not include any blank lines when creating the file.

```

IDSTORE_HOST : idstore.example.com
IDSTORE_PORT : 389
IDSTORE_BINDDN : cn=directory manager
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_SSL_ENABLED: false
IDSTORE_READONLYUSER: IDROUser
IDSTORE_READWRITEUSER: IDRWUser
IDSTORE_SUPERUSER: weblogic_fa
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_ADMIN_PORT : 4444
IDSTORE_KEYSTORE_FILE : <path to file copied from oud install>
IDSTORE_KEYSTORE_PASSWORD : 4VYGtJLG61V50jDWKe94e601x7tgLFs

```

[Table 2–7](#) provides descriptions of the parameters in the configuration file example.

Table 2–7 *preconfigFAPPropertyFile Properties*

Properties	Description
IDSTORE_HOST	Host name of the LDAP identity store directory (corresponding to the IDSTORE_DIRECTORYTYPE). If your identity store is in Oracle Internet Directory or Oracle Unified Directory, then IDSTORE_HOST points directly to the Oracle Internet Directory or Oracle Unified Directory host. If the Identity Store is fronted by Oracle Virtual Directory, then IDSTORE_HOST points to the Oracle Virtual Directory host, which is IDSTORE.example.com.
IDSTORE_PORT	Port number of the LDAP identity store (corresponding to the IDSTORE_DIRECTORYTYPE).
IDSTORE_BINDDN	Administrative user in the identity store directory.
IDSTORE_USERNAMEATTRIBUTE	Username attribute used to set and search for users in the identity store. Set to part of the user DN. For example, if the user DN is cn=orcladmin, cn=Users, dc=us, dc=example, dc=com, this property is set to cn.
IDSTORE_LOGINATTRIBUTE	Login attribute of the identity store which contains the user's login name. This is the attribute the user uses for login.
IDSTORE_USERSEARCHBASE	Location in the directory where users are stored. This property tells the directory where to search for users.
IDSTORE_SEARCHBASE	Search base for users and groups contained in the identity store. Parent location that contains the USERSEARCHBASE and the GROUPSEARCHBASE.
IDSTORE_GROUPSEARCHBASE	The location in the directory where groups (or roles) are stored. This property tells the directory where to search for groups or roles.
POLICYSTORE_SHARES_IDSTORE	Denotes whether the policy store and identity store share the directory. Always true in Release 11g. Valid values: true, false
IDSTORE_SSL_ENABLED	Whether SSL to the identity store is enabled. Valid values: true false
IDSTORE_READONLYUSER	User with read-only permissions to the identity store.
IDSTORE_READWRITEUSER	User with read-write permissions to the identity store.
IDSTORE_SUPERUSER	The Oracle Fusion Applications superuser in the identity store.

Table 2–7 (Cont.) preconfigFAPropertyFile Properties

Properties	Description
IDSTORE_SYSTEMIDBASE	Location of a container in the directory where system operations users are stored so that they are kept separate from enterprise users stored in the main user container. There are only a few system operations users. One example is the Oracle Identity Manager reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.
IDSTORE_ADMIN_PORT	Administration port of your Oracle Unified Directory instance. If you are not using Oracle Unified Directory, you can leave out this parameter.
IDSTORE_KEYSTORE_FILE	Location of the Oracle Unified Directory Keystore file. It is used to enable communication with Oracle Unified Directory using the Oracle Unified Directory administration port. It is called admin-keystore and is located in <code>OID_ORACLE_INSTANCE/OU/OU/config</code> . If you are not using Oracle Unified Directory, you can leave out this parameter. This file must be located on the same host that the <code>idmConfigTool</code> command is running on. The command uses this file to authenticate itself with OUD.
IDSTORE_KEYSTORE_PASSWORD	Encrypted password of the Oracle Unified Directory keystore. This value can be found in the file <code>OID_ORACLE_INSTANCE/OU/OU/config/admin-keystore.pin</code> . If you are not using Oracle Unified Directory, you can leave out this parameter.

3. Set the environment variables required for the `idmconfigtool` command. For information on setting environment variables, see [Section D.2, "Set Up Environment Variables."](#)

4. Change the directory to the `IAM_ORACLE_HOME/idmtools/bin` directory:

```
cd IAM_ORACLE_HOME/idmtools/bin
```

You will be running the `idmConfigTool` command from the `IAM_ORACLE_HOME/idmtools/bin` directory.

5. Configure the identity store by using the `idmConfigTool` with the `-prepareIDStore mode=fusion` command option.

On Linux, the command syntax is:

```
idmConfigTool.sh -prepareIDStore mode=fusion input_file=configfile
```

On Windows, the command syntax is:

```
idmConfigTool.bat -prepareIDStore mode=fusion input_file=configfile
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=fusion input_file=preconfigFAPropertyFile
```

For information on `-prepareIDStore mode=fusion`, see [Section D.4.2.7, "prepareIDStore mode=fusion."](#)

The command prompts you to enter the password for the account used to connect to the identity store. You are then prompted to create passwords for the following three accounts:

- IDROUser
User with read-only permissions to the identity store.
 - IDRWUser
User with read-write permissions to the identity store.
 - weblogic_fa
The Oracle Fusion Applications superuser in the identity store.
6. The `automation.log` file is created in the directory where you run the tool. Check the log file for any errors or warnings and correct them. The tool is reentrant and can be safely called again.

2.4 Configuring Access Manager for Oracle Identity Manager Integration

Before integrating Oracle Identity Manager with Access Manager 11g, you must configure Access Manager 11g for Access Manager and Oracle Identity Manager integration.

1. Create a properties file called `OAMconfigPropertyFile` with contents similar to the following:

Note: If you already have an identity store in place that is different from the default created by this tool, add the `OAM11G_IDSTORE_NAME` parameter to the properties file and set the value to the name of that identity store.

Do not include any blank lines when creating the file.

```
WLSHOST: adminvhn.example.com
WLSPORT: 7001
WLSADMIN: weblogic
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_OAMSOFTWAREUSER: oamLDAP
IDSTORE_OAMADMINUSER: oamadmin
IDSTORE_DIRECTORYTYPE: OUD
POLICYSTORE_SHARES_IDSTORE: true
PRIMARY_OAM_SERVERS: oamhost1.example.com:5575
WEBGATE_TYPE: ohsWebgate11g
ACCESS_GATE_ID: Webgate_IDM
OAM11G_IDM_DOMAIN_OHS_HOST: sso.example.com
OAM11G_IDM_DOMAIN_OHS_PORT: 443
OAM11G_IDM_DOMAIN_OHS_PROTOCOL: http
OAM11G_WG_DENY_ON_NOT_PROTECTED: false
OAM11G_IMPERSONATION_FLAG: false
```

```
OAM_TRANSFER_MODE: Open
OAM11G_OAM_SERVER_TRANSFER_MODE: open
OAM11G_IDM_DOMAIN_LOGOUT_URLS:
/console/jsp/common/logout.jsp,/em/targetauth/emaslogout.jsp,/oamssso/logout.htm
l,/cgi-bin/logout.pl
OAM11G_SERVER_LOGIN_ATTRIBUTE: uid
COOKIE_DOMAIN: .example.com
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
OAM11G_SSO_ONLY_FLAG: true
OAM11G_OIM_INTEGRATION_REQ: true
OAM11G_SERVER_LBR_HOST: sso.example.com
OAM11G_SERVER_LBR_PORT: 443
OAM11G_SERVER_LBR_PROTOCOL: http
COOKIE_EXPIRY_INTERVAL: 120
OAM11G_OIM_OHS_URL: http://sso.example.com:443/
SPLIT_DOMAIN: true
```

The `OAMconfigPropertyFile` file must contain configuration information specific to your environment. This file will be used to configure Access Manager 11g for Access Manager and Oracle Identity Manager integration when you run the `idmconfigtool` command.

Table 2–8 provides descriptions of the parameters in the `OAMconfigPropertyFile` configuration file example.

Table 2–8 OAMconfigPropertyFile Properties File

Properties	Description
WLSHOST	Administration server host name. This will be the virtual name.
WLSPORT	Administration server port.
WLSADMIN	WebLogic Server administrative user account you use to log in to the WebLogic Server administration console.
IDSTORE_HOST	Identity store host name. If using a directory server other than Oracle Internet Directory or Oracle Unified Directory, specify the Oracle Virtual Directory host and port.
IDSTORE_PORT	Identity store port.
IDSTORE_BINDDN	An administrative user in Oracle Internet Directory or Oracle Unified Directory. If using a directory server other than Oracle Internet Directory or Oracle Unified Directory, specify an Oracle Virtual Directory administrative user.
IDSTORE_USERNAMEATTRIBUTE	Username attribute used to set and search for users in the identity store.
IDSTORE_LOGINATTRIBUTE	Login attribute of the identity store which contains the user's login name.
IDSTORE_USERSEARCHBASE	Container under which Access Manager searches for the users.
IDSTORE_SEARCHBASE	Location in the directory where users and groups are stored.
IDSTORE_GROUPSEARCHBASE	Location in the directory where groups are stored.

Table 2–8 (Cont.) OAMconfigPropertyFile Properties File

Properties	Description
IDSTORE_OAMSOFTWAREUSER	User you use to interact with the LDAP server.
IDSTORE_OAMADMINUSER	User you use to access your Oracle Access Management Administration Console.
IDSTORE_DIRECTORYTYPE	Identity store directory type.
PRIMARY_OAM_SERVERS	<p>Comma-separated list of your Access Manager servers and the proxy ports they use.</p> <p>To determine the proxy ports your Access Manager servers:</p> <ol style="list-style-type: none"> 1. Log in to the Oracle Access Management administration console at <code>http://admin.example.com:7001/oamconsole</code> 2. At the top of the Oracle Access Management Console, click Configuration. 3. In the Configuration console, click Server Instances. 4. In the page that appears, click Search, then double-click the target instance to display its configuration. For example, WLS_OAM1. <p>The proxy port is shown as Port.</p>
WEBGATE_TYPE	<p>WebGate agent type you want to create.</p> <p>Valid values are <code>ohsWebgate11g</code> if WebGate version 11 is used, or <code>ohsWebgate10g</code> if WebGate version 10 is used.</p>
ACCESS_GATE_ID	Name you want to assign to the WebGate. Do <i>not</i> change the property value shown above.
OAM11G_IDM_DOMAIN_OHS_HOST	Load balancer that is in front of Oracle HTTP Server (OHS) in a high-availability configuration.
OAM11G_IDM_DOMAIN_OHS_PORT	Load balancer port.
OAM11G_IDM_DOMAIN_OHS_PROTOCOL	Protocol to use when directing requests to the load balancer.
OAM11G_WG_DENY_ON_NOT_PROTECTED	Set to deny on protected flag for 10g WebGate. Valid values are <code>true</code> and <code>false</code> .
OAM11G_IMPERSONATION_FLAG	<p>Enables or disables the impersonation feature in the OAM Server.</p> <p>Valid values are <code>true</code> (enable) and <code>false</code> (disable). The default is <code>false</code>.</p> <p>If you are using impersonalization, you must manually set this value to <code>true</code>.</p>
OAM_TRANSFER_MODE	Security mode in which the access servers function.
OAM11G_OAM_SERVER_TRANSFER_MODE	Security mode for the Access Manager servers.
OAM11G_IDM_DOMAIN_LOGOUT_URLS	Set to the various logout URLs.
OAM11G_SERVER_LOGIN_ATTRIBUTE	Set to <code>uid</code> ensures that when users log in their username is validated against the <code>uid</code> attribute in LDAP.

Table 2–8 (Cont.) OAMconfigPropertyFile Properties File

Properties	Description
COOKIE_DOMAIN	Domain in which the WebGate functions.
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	Account to administer role security in identity store.
OAM11G_SSO_ONLY_FLAG	Configures Access Manager 11g as authentication only mode or normal mode, which supports authentication and authorization. Default value is true. If set to true, the Access Manager 11g server operates in authentication only mode, where all authorizations return true by default without any policy validations. In this mode, the server does not have the overhead of authorization handling. This is recommended for applications which do not depend on authorization policies and need only the authentication feature of the Access Manager server. If set to false, the server runs in default mode, where each authentication is followed by one or more authorization requests to the Access Manager server. WebGate allows the access to the requested resources or not, based on the responses from the Access Manager server.
OAM11G_OIM_INTEGRATION_REQ	Specifies whether to integrate with Oracle Identity Manager or configure Access Manager in stand-alone mode. Set to true for integration.
OAM11G_SERVER_LBR_HOST	OAM Server fronting your site. This and the following two parameters are used to construct your login URL.
OAM11G_SERVER_LBR_PORT	Load balancer port.
OAM11G_SERVER_LBR_PROTOCOL	URL prefix. The default value is http.
COOKIE_EXPIRY_INTERVAL	Cookie expiration period.
OAM11G_OIM_OHS_URL	URL of the load balancer or Oracle HTTP Server (OHS) fronting the OIM server.
SPLIT_DOMAIN	Set to true is required to suppress the double authentication of Oracle Access Management administration console.

2. Set the environment variables required for the `idmconfigtool` command. For information on setting environment variables, see [Section D.2, "Set Up Environment Variables."](#)

3. Change the directory to the `IAM_ORACLE_HOME/idmtools/bin` directory:

```
cd IAM_ORACLE_HOME/idmtools/bin
```

You will be running the `idmConfigTool` command from the `IAM_ORACLE_HOME/idmtools/bin` directory.

4. Configure the identity store by using the `idmConfigTool` command with the `-configOAM` command option.

On Linux, the command syntax is:

```
idmConfigTool.sh -configOAM input_file=configfile
```

On Windows, the command syntax is:

```
idmConfigTool.bat -configOAM input_file=configfile
```

For example:

```
idmConfigTool.sh -configOAM input_file=OAMconfigPropertyFile
```

For information on the `configOAM` command option, see [Section D.4.4, "configOAM Command."](#)

Before running this command, ensure that the Access Management Domain Administration Server is running.

When the command runs, it prompts you to enter the password of the account used to connect to the identity store. It also asks you to create passwords for the following three accounts:

- OAM11G_WLS_ADMIN_PASSWD
- IDSTORE_PWD_OAMSOFTWAREUSER
- IDSTORE_PWD_OAMADMINUSER

Sample command output, when running the command against Oracle Unified Directory, is shown as follows:

```
Enter ID Store Bind DN password:
Enter User Password for OAM11G_WLS_ADMIN_PASSWD:
Confirm User Password for OAM11G_WLS_ADMIN_PASSWD:
Enter User Password for IDSTORE_PWD_OAMSOFTWAREUSER:
Confirm User Password for IDSTORE_PWD_OAMSOFTWAREUSER:
Enter User Password for IDSTORE_PWD_OAMADMINUSER:
Confirm User Password for IDSTORE_PWD_OAMADMINUSER:
The tool has completed its operation. Details have been logged to
automation.log
```

5. Check the log file for any errors or warnings and correct them. The tool is reentrant and can be safely called again.
6. Restart OAM Administration Server.

For information on restarting the WebLogic Administration Server, see "Restarting Servers" in *Installation Guide for Oracle Identity and Access Management*.

2.5 Integrating Access Manager with Oracle Identity Manager

Integrate Oracle Identity Manager with Access Manager as follows.

Note: Before running `configOIM`, ensure that:

- The `configOAM` command was successful.
 - The Oracle Access Management Admin Server had been restarted.
 - The OIM Admin and OAM Admin Servers are running.
-
-

1. Retrieve the random global passphrase for SIMPLE security mode communication with Access Manager.

By default, Access Manager is configured to use the `OPEN` security mode. If you want to use the installation default of `OPEN` mode, you can skip this step.

If you want `idmConfigTool` to change the security mode to `SIMPLE` mode and propagate changes to the WebGates, you must provide the global passphrase when prompted by the Access Manager and Oracle Identity Manager integration script. Artifacts generated for `SIMPLE` mode use the global passphrase. If you do not remember your global passphrase, you can retrieve it by using the `displaySimpleModeGlobalPassphrase()` command as follows:

- a. Ensure that the Oracle Access Management Console is running.
- b. On the computer hosting the Oracle Access Management Console, connect to the WebLogic Scripting Tool. For example:

```
$ORACLE_IDM_HOME/common/bin/wlst.sh
wls:/offline> connect()
```

where `$ORACLE_IDM_HOME` represents the base installation directory path.

- c. Respond to the prompts as shown:

```
Please enter your username [weblogic] :
Please enter your password [weblogic] :
Please enter your server URL [t3://localhost:7001] :
wls:/base_domain/serverConfig>
```

- d. Enter the following command to change the location to the read-only domainRuntime tree:

```
wls:/base_domain/serverConfig>domainRuntime()
```

- e. View the global passphrase by entering the following command:

```
wls:/base_domain/domainRuntime> displaySimpleModeGlobalPassphrase()
```

- f. Make a note of this passphrase and exit WLST by using the exit command:

```
wls:/base_domain/domainRuntime> exit()
```

2. Create a properties file named `OIMconfigPropertyFile` with contents similar to the following:

Do not include any blank lines when creating the file.

```
LOGINURI: /${app.context}/adfAuthentication
LOGOUTURI: /oamssso/logout.html
AUTOLOGINURI: None
ACCESS_SERVER_HOST: OAMHOST1.example.com
ACCESS_SERVER_PORT: 5575
ACCESS_GATE_ID: Webgate_IDM
COOKIE_DOMAIN: .example.com
COOKIE_EXPIRY_INTERVAL: 120
OAM_TRANSFER_MODE: Open
WEBGATE_TYPE: ohsWebgate11g
OAM_SERVER_VERSION: 11g
OAM11G_WLS_ADMIN_HOST: wlsadmin.example.com
OAM11G_WLS_ADMIN_PORT: 17001
OAM11G_WLS_ADMIN_USER: weblogic
SSO_ENABLED_FLAG: true
IDSTORE_PORT: 389
IDSTORE_HOST: idstore.example.com
IDSTORE_DIRECTORYTYPE: OUD
```

```

IDSTORE_ADMIN_USER: cn=oamLDAP,cn=systemids,dc=example,dc=com
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
MDS_DB_URL: jdbc:oracle:thin:@DBHOST:PORT:SID
MDS_DB_SCHEMA_USERNAME: idm_mds
WLSHOST: adminvhn.example.com
WLSPORT: 7001
WLSADMIN: weblogic
DOMAIN_NAME: IDM_Domain
OIM_MANAGED_SERVER_NAME: WLS_OIM1
DOMAIN_LOCATION: ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain
IDSTORE_WLSADMINUSER: weblogic_idm
OIM_MSM_REST_SERVER_URL: <Oracle Mobile Security Manager server URL>

```

The `OIMconfigPropertyFile` file must contain configuration information specific to your environment. This file will be used for Access Manager and Oracle Identity Manager integration.

If you are not integrating OIM with OMSS, you can leave out the `OIM_MSM_REST_SERVER_URL` parameter.

[Table 2–9](#) provides descriptions of the parameters in the `OIMconfigPropertyFile` configuration file example.

Table 2–9 OIMconfigPropertyFile Properties

Properties	Description
WLSHOST, WLSPORT, WLSADMIN	In the split domain topology where Oracle Identity Manager and Access Manager are in different domains, WLSHOST, WLSPORT, WLSADMIN are related to Oracle Identity Manager.
ACCESS_SERVER_PORT	Access Manager OAP port.
ACCESS_GATE_ID	ACCESS_GATE_ID must be the same as the ACCESS_GATE_ID value that you provided in the properties file for the <code>configOAM</code> command. (See Section 2.4 , which covers configuring the identity store using the <code>idmConfigTool</code> with the <code>-configOAM</code> command.)
OAM_TRANSFER_MODE	OAM_TRANSFER_MODE must be the same as the OAM_TRANSFER_MODE value that you provided in the properties file for the <code>configOAM</code> command. (See Section 2.4 , which covers configuring the identity store using the <code>idmConfigTool</code> with the <code>-configOAM</code> command.)
WEBGATE_TYPE	Set to <code>ohsWebgate11g</code> if WebGate version 11 is used, or <code>ohsWebgate10g</code> if WebGate version 10 is used.
OAM_SERVER_VERSION	Set to <code>10g</code> if using Oracle Access Manager 10g, or <code>11g</code> if using Access Manager 11g.
OAM11G_WLS_ADMIN_HOST, OAM11G_WLS_ADMIN_PORT, and OAM11G_WLS_ADMIN_USER.	Set <code>OAM11G_WLS_ADMIN_HOST</code> , <code>OAM11G_WLS_ADMIN_PORT</code> , and <code>OAM11G_WLS_ADMIN_USER</code> . <code>OAM11G_WLS_ADMIN_HOST</code> , <code>OAM11G_WLS_ADMIN_PORT</code> , and <code>OAM11G_WLS_ADMIN_USER</code> properties are related to Access Manager. For information about split domain integration topology, see Chapter 1, "Introduction."
IDSTORE_PORT	Oracle Unified Directory or Oracle Internet Directory port if you are using Oracle Unified Directory or Oracle Internet Directory as your identity store. If not, set it to your Oracle Virtual Directory port.

Table 2–9 (Cont.) OIMconfigPropertyFile Properties

Properties	Description
IDSTORE_HOST	Oracle Unified Directory or Oracle Internet Directory host or load balancer name if you are using Oracle Unified Directory or Oracle Internet Directory as your identity store. If not, set it to your Oracle Virtual Directory host or load balancer name.
IDSTORE_DIRECTORYTYPE	OVD if you are using Oracle Virtual Directory server to connect to either a non-OID directory, Oracle Internet Directory or Oracle Unified Directory. OID if your identity store is in Oracle Internet Directory and you are accessing it directly rather than through Oracle Virtual Directory. OUD if your identity store is in Oracle Unified Directory and you are accessing it directly rather than through OVD.
IDSTORE_ADMIN_USER	Complete LDAP DN of the administrator of the identity store directory. This should be the same user specified for IDSTORE_OAMSOFTWAREUSER (if specified).
MDS_DB_URL	Single instance database. The string following the '@' symbol must have the correct values for your environment. SID must be the actual SID, <i>not</i> a service name. If you are using a single instance database, then set MDS_URL to: jdbc:oracle:thin:@DBHOST:1521:SID.
MDS_DB_SCHEMA_USERNAME	MDS schema which Oracle Identity Manager is using.
OIM_MSM_REST_SERVER_URL	Oracle Mobile Security Manager server URL. https://host:port. The MSM URL is seeded in Oracle Identity Manager and the system property OMSS_Enabled is set. OIM_MSM_REST_SERVER_URL enables the Mobile Security Manager task flows in the Oracle Identity Manager console. If not set, configOIM will continue the configuration without configuring the Mobile Security Manager.
WLSPASSWORD	The WebLogic Server administrator password. Note: This property is required for Mobile Security Manager and Oracle Identity Manager integration.
IDSTORE_WLSADMINUSER	Value of the user which should be the same value as provided while running prepareIdStore mode=wls command.

3. Set the environment variables required for the idmconfigtool command. For information on setting environment variables, see [Section D.2, "Set Up Environment Variables."](#)

4. Change the directory to the `IAM_ORACLE_HOME/idmtools/bin` directory:

```
cd IAM_ORACLE_HOME/idmtools/bin
```

You will be running the `idmConfigTool` command from the `IAM_ORACLE_HOME/idmtools/bin` directory.

5. Configure the identity store by using `idmConfigTool` with the `-configOIM` command.

On Linux, the command syntax is:

```
idmConfigTool.sh -configOIM input_file=configfile
```

On Windows, the command syntax is:

```
idmConfigTool.bat -configOIM input_file=configfile
```

For example:

```
idmConfigTool.sh -configOIM input_file=OIMconfigPropertyFile
```

For information on the `configOIM` command option, see [Section D.4.5, "configOIM Command."](#)

When the command executes you will be prompted for:

- Access Gate Password
- Single Sign-On (SSO) Keystore Password
- Global Passphrase
- Idstore Admin Password
- MDS Database schema password
- Admin Server User Password
- Password to be used for Oracle Access Management administrative user
- Password for `IDSTORE_WLS_ADMIN_USER` as provided during the `prepareIdStore mode=wls` command

Sample command output, when running the command against Oracle Unified Directory, is shown as follows:

```
Enter oam11g domain admin user password :
Enter sso access gate password :
Enter mds db schema password :
Enter idstore admin password :
Enter admin server user password :
Enter IDSTORE_WLS_ADMIN_USER Password :
Seeding OIM Resource Policies into OAM...
Resources Seeded!!
***** Seeding OAM Passwds in OIM *****
Completed loading user inputs for - CSF Config
Completed loading user inputs for - Dogwood Admin WLS
Connecting to t3://adminvhn.example.com:7001

Connection to domain runtime mbean server established
Seeding credential :SSOAccessKey
***** *****
***** Activating OAM Notifications *****
Completed loading user inputs for - MDS DB Config
Initialized MDS resources
Jan 28, 2015 10:43:06 PM oracle.mds
NOTIFICATION: MDS-10013: transfer operation started.
Jan 28, 2015 10:43:06 PM oracle.mds
NOTIFICATION: MDS-10014: transfer is completed. Total number of documents
successfully processed : 1, total number of documents failed : 0.
Upload to DB completed
Releasing all resources
Notifications activated.
***** *****
***** Seeding OAM Config in OIM *****
Completed loading user inputs for - OAM Access Config
Validated input values
Initialized MDS resources
Jan 28, 2015 10:43:06 PM oracle.mds
```

```
NOTIFICATION: MDS-10013: transfer operation started.
Jan 28, 2015 10:43:06 PM oracle.mds
NOTIFICATION: MDS-10014: transfer is completed. Total number of documents
successfully processed : 1, total number of documents failed : 0.
Download from DB completed
Releasing all resources
Updated /u01/app/oracle/product/fmw/iam/server/oamMetadata/db/oim-config.xml
Initialized MDS resources
Jan 28, 2015 10:43:06 PM oracle.mds
NOTIFICATION: MDS-10013: transfer operation started.
Jan 28, 2015 10:43:06 PM oracle.mds
NOTIFICATION: MDS-10014: transfer is completed. Total number of documents
successfully processed : 1, total number of documents failed : 0.
Upload to DB completed
Releasing all resources
OAM configuration seeded. Please restart oim server.
*****
***** Configuring Authenticators in OIM WLS *****
Completed loading user inputs for - LDAP connection info
Connecting to t3://adminvhn.example.com:7001
Connection to domain runtime mbean server established
Starting edit session
Edit session started
Connected to security realm.
Validating provider configuration
Validated desired authentication providers
Destroyed Authentication Provider:
Security:Name=myrealmOIMAuthenticationProvider
Created OAMIDAsserter successfully
OAMIDAsserter is already configured to support 11g webgate
Created OIMSignatureAuthenticator successfully
Created OUDAuthenticator successfully
Setting attributes for OUDAuthenticator
All attributes set. Configured inOUDAuthenticatornow
LDAP details configured in OUDAuthenticator
Control flags for authenticators set successfully
Reordering of authenticators done successfully
Saving the transaction
Transaction saved
Activating the changes
Changes Activated. Edit session ended.
Connection closed successfully
*****
The tool has completed its operation. Details have been logged to
automation.log
```

6. Check the log file for errors and correct them if necessary. The tool is reentrant and can be safely called again.
7. Restart the Oracle Identity Manager managed server and the WebLogic Administration Server.

For information, see "Starting or Stopping the Oracle Stack" in *Installation Guide for Oracle Identity and Access Management*.

2.6 Configuring Oracle HTTP Server to Front-End Resources on Oracle Identity Manager

The Oracle HTTP Server (OHS) profile must be edited so that the OHS server points to the OIM server that is being protected by Access Manager. The `oim.conf` profile template file is located here:

```
$IAM_HOME/server/setup/templates/oim.conf
```

Note: WebGate installation and configuration is required.

The Oracle HTTP Server with 11g WebGate must be installed. For information, see "Installing and Configuring Oracle HTTP Server 11g WebGate for OAM" in *Oracle Fusion Middleware Installing Webgates for Oracle Access Manager*.

For information about installing Oracle HTTP Server with a 10g WebGate, see "Registering and Managing 10g WebGates with Access Manager 11g" and "Configuring Apache, OHS, IHS for 10g WebGates" in *Administrator's Guide for Oracle Access Management*.

1. Add the following entry to the `oim.conf` file, if it is not already present:

```
<Location /reqsvc>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicHost <OIM managed server host>
  WebLogicPort <OIM managed server port>
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>
```

2. Edit the `oim.conf` file to include the following lines:

```
<Location /identity>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicHost <OIM managed server host>
  WebLogicPort <OIM managed server port>
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>
```

```
<Location /sysadmin>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicHost <OIM managed server host>
  WebLogicPort <OIM managed server port>
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>
```

```
<Location /oam>
  SetHandler weblogic-handler
  WLCookieName jsessionid
  WebLogicHost <OAM managed server host>
  WebLogicPort <OAM managed server port>
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>
```

```
<Location /admin>
```

```

SetHandler weblogic-handler
WebLogicHost <OIM managed server host>
WebLogicPort <OIM managed server port>
WLCookieName oimjsessionid
WLOGFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# oim self and advanced admin webapp consoles (canonic webapp)
<Location /oim>
SetHandler weblogic-handler
WebLogicHost <OIM managed server host>
WebLogicPort <OIM managed server port>
WLCookieName oimjsessionid
WLOGFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# SOA Callback webservice for SOD
<Location /sodcheck>
SetHandler weblogic-handler
WebLogicHost <OIM managed server host>
WebLogicPort <OIM managed server port>
WLCookieName oimjsessionid
WLOGFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# Callback webservice for SOA. SOA calls this when a request is
approved/rejected
# Provide the SOA Managed Server Port
<Location /workflowservice>
SetHandler weblogic-handler
WebLogicHost <OIM managed server host>
WebLogicPort <OIM managed server port>
WLCookieName oimjsessionid
WLOGFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# xlWebApp - Legacy 9.x webapp (struts based)
<Location /xlWebApp>
SetHandler weblogic-handler
WLCookieName oimjsessionid
WebLogicHost <OIM managed server host>
WebLogicPort <OIM managed server port>
WLOGFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# Nexaweb WebApp - used for workflow designer and DM
<Location /Nexaweb>
SetHandler weblogic-handler
WLCookieName oimjsessionid
WebLogicHost <OIM managed server host>
WebLogicPort <OIM managed server port>
WLOGFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# used for FA Callback service.
<Location /callbackResponseService>
SetHandler weblogic-handler
WLCookieName oimjsessionid
WebLogicHost <OIM managed server host>
WebLogicPort <OIM managed server port>

```

```

WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# spml xsd profile
<Location /spml-xsd>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicHost <OIM managed server host>
  WebLogicPort <OIM managed server port>
  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

<Location /HTTPClnt>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicHost <OIM managed server host>
  WebLogicPort <OIM managed server port>
  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

```

3. Copy the oim.conf file to the OHS moduleconf location:

```
INSTANCE_LOCATION/config/OHS/ohs1/moduleconf/
```

4. Restart the OHS instance. For information on restarting the OHS instance, see "Restarting Oracle HTTP Server Instances" in *Oracle Fusion Middleware Administrator's Guide for Oracle HTTP Server*.

2.7 Deleting the IAMSuiteAgent Security Provider from WebLogic

The IAMSuiteAgent is installed out of the box when you install Access Manager. It is preconfigured to provide single-sign on for the IdM domain consoles, Oracle Identity Manager, Oracle Adaptive Access Manager, and other Identity Management servers created during domain creation. It is like a WebGate, but it only protects internal URLs provided by various products in the Identity and Access Management Suite.

Because this environment uses an OHS 11g WebGate to handle single sign-on, the IAMSuiteAgent is no longer necessary, so you must remove it. To do so:

1. Log in to the Oracle WebLogic Administration Console using the URL:
`http://admin.example.com/console`.
2. Click **Lock and Edit** from the Change Center.
3. Select **Security Realms** from the left pane and click **myrealm**.
4. Click the **Providers** tab and then the **Authentication** tab.
5. In the list of authentication providers, select **IAMSuiteAgent**.
6. Click **Delete** to delete IAMSuiteAgent.
7. Click **Yes** to confirm the deletion.
8. Click **Activate Changes** from the Change Center.
9. Restart WebLogic Administration Server and all running Managed Servers.

For information on restarting the servers, see "Restarting Servers" in *Installation Guide for Oracle Identity and Access Management*.

2.8 Validating the Integration

This section provides steps for validating the integrated environment. Performing the following sanity checks can help you avoid some common issues that could be encountered during runtime.

In this release, Oracle Identity Manager is integrated with Access Manager when the `idmconfig` command is run with the `configOIM` option. After the command is run, the following configuration settings and files are updated:

- The SSOConfig section in the `oim-config.xml` file, stored in the OIM Metadata store. See [Section 2.8.1, "Validate Oracle Identity Manager SSOConfig."](#)
- The realm security providers in `OIM_DOMAIN_HOME/config.xml`. See [Section 2.8.2, "Validate Security Provider Configuration."](#)
- The OIM domain credential store in `OIM_DOMAIN_HOME/config/fmwconfig/cwallet.sso`. See [Section 2.8.3, "Validate Oracle Identity Manager Domain Credential Store."](#)
- The orchestration event-handlers required for SSO integration in `Eventhandler.xml`, stored in the OIM Metadata store. See [Section 2.8.4, "Validate Event Handlers for SSO."](#)
- The SSO logout configuration in `OIM_DOMAIN_HOME/config/fmwconfig/jps-config.xml`. See [Section 2.8.5, "Validate SSO Logout Configuration."](#)

2.8.1 Validate Oracle Identity Manager SSOConfig

To validate the SSOConfig settings in `oim-config.xml`:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control.
2. Select **Weblogic Domain**, then right-click the domain name.
3. Open System Mbean Browser and search for the SSOConfig Mbean.

For more information, see "Getting Started Using the Fusion Middleware Control MBean Browsers" in *Administrator's Guide*.

4. Verify the following attribute settings are correct after running `idmconfig configOIM`. Update any values as needed:
 - `SsoEnabled` attribute is set to `true`.
 - If using TAP communication, the `TapEndpointURL` attribute is present.
 - If using Oracle Access Protocol (OAP) communication, the following attributes are present: `AccessGateID`, `AccessServerHost`, `AccessServerPort`, `CookieDomain`, `CookieExpiryInterval`, `NapVersion`, `TransferMode`, `WebgateType`.
 - If `Version` is set to 11g, verify the `TapEndpointURL` attribute is set to a valid URL. Validate the URL by accessing in a web browser.
 - If `Version` is set to 10g, verify the other attributes are configured correctly.

2.8.2 Validate Security Provider Configuration

To validate the Oracle Identity Manager security provider configuration:

1. In Oracle WebLogic Administration Console, navigate to the **OIM domain**.
2. Navigate to **Security Realms > myrealm** and then click the **Providers** tab.

3. Confirm the Authentication Providers are configured as follows.

Authentication Provider	Control Flag
OAMIDasserter	REQUIRED
OIMSignatureAuthenticator	SUFFICIENT
LDAP Authenticator	SUFFICIENT
DefaultAuthenticator	SUFFICIENT
DefaultIdentityAsserter	Not applicable

4. The LDAP Authenticator name may vary depending on which LDAP provider you are using. For example for Oracle Unified Directory, it is OUDAuthenticator. Verify it is configured correctly by selecting **Users and Groups** tab, and confirming the LDAP users are listed in **Users** tab.

To validate the Access Manager security provider configuration:

1. In Oracle WebLogic Administration Console, navigate to the **OAM domain**.
2. Navigate to **Security Realms > myrealm**. Then, click the **Providers** tab.
3. Confirm the Authentication Providers are configured as follows.

Authentication Provider	Control Flag
OAMIDasserter	REQUIRED
DefaultAuthenticator	SUFFICIENT
LDAP Authenticator	SUFFICIENT
DefaultIdentityAsserter	Not applicable

4. The LDAP authenticator varies depending upon the LDAP provider being used. Verify that it is configured correctly by clicking the **Users and Groups** tab, and confirming that the LDAP users are listed in **Users** tab.

2.8.3 Validate Oracle Identity Manager Domain Credential Store

All passwords and credentials used during communication between Oracle Identity Manager and Access Manager are stored in the domain credential store.

To validate the passwords and credentials used to communicate:

1. Login to Oracle Enterprise Manager Fusion Middleware Control and select **WebLogic Domain**.
2. Right-click the *domain name*. Navigate to **Security**, then **Credentials**.
3. Expand the **oim** instance. Verify the following credentials:
 - **SSOAccessKey**: OPEN mode only
 - **SSOKeystoreKey**: SIMPLE mode only
 - **SSOGobalPP**: SIMPLE mode only
 - **OIM_TAP_PARTNER_KEY**

2.8.4 Validate Event Handlers for SSO

A set of event handlers is uploaded to the Oracle Identity Manager MDS in order to support session termination after a user status change. These event handlers notify Access Manager when a user status is changed, which then terminates the user session. They are uploaded to MDS as part of `EventHandlers.xml` file, located at `/db/ssointg/EventHandlers.xml`.

To confirm all event handlers are configured correctly, export the `EventHandlers.xml` file using Oracle Enterprise Manager Fusion Middleware Control:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control.
2. Navigate to **Identity and Access > OIM > oim(11.1.2.0.0)**.
3. Right-click and navigate to **System MBean Browser**.
4. Under **Application Defined MBeans**, navigate to **Oracle.mds.lcm > Server:oim_server1 > Application:OIMAppMetadata > MDSAppRuntime > MDSAppRuntime**.

For more information, see "Getting Started Using the Fusion Middleware Control MBean Browsers" in *Administrator's Guide*.

5. Click the **Operations** tab, and then, click **exportMetadata**.
6. In **toLocation**, enter `/tmp` or the name of another directory. This is the directory where the file will be exported.
7. In the **docs** field, click **Edit** and then **Add** and enter the complete file location as the Element:

```
/db/oim-config.xml
/db/ssointg/EventHandlers.xml
```

8. Select **false** for **excludeAllCust**, **excludeBaseDocs**, and **excludeExtendedMetadata**.
9. Click **Invoke** to export the files specified in the **docs** field to the directory specified in the **toLocation** field.

For more information, see "Deploying and Undeploying Customizations" in *Developing and Customizing Applications for Oracle Identity Manager*.

2.8.5 Validate SSO Logout Configuration

Oracle Identity Manager logout is configured to use single logout after the integration is complete. After a user logs out from Oracle Identity Manager, they are logged out from all the Access Manager protected applications as well.

To verify the configuration of single logout, do the following:

1. From your present working directory, move to the following directory:
`OIM_DOMAIN_HOME/config/fmwconfig`
2. Open the `jps-config.xml` file.
3. Ensure the `<propertySet name="props.auth.uri.0">` element in the `jps-config.xml` file contains entries similar to the following example:

```
<propertySet name="props.auth.uri.0">
  <property name="logout.url" value="/oamssso/logout.html"/>
  <property name="autologin.url" value="None"/>
  <property name="login.url.BASIC"
```

```

value="/${app.context}/adfAuthentication"/>
    <property name="login.url.FORM"
value="/${app.context}/adfAuthentication"/>
    <property name="login.url.ANONYMOUS"
value="/${app.context}/adfAuthentication"/>
</propertySet>

```

2.9 Functionally Testing the Access Manager and Oracle Identity Manager Integration

The final task is to verify the integration by performing, in order, the steps shown in [Table 2–10](#).

Table 2–10 Verifying Access Manager and Oracle Identity Manager Integration

Step	Description	Expected Result
1	<p>Log in to the Oracle Access Management Administration Console as the <code>weblogic_idm</code> user using the URL:</p> <p><code>http://admin_server_host:admin_server_port/oamconsole</code></p>	Provides access to the administration console.
2	<p>Access the Oracle Identity Manager administration page with the URL:</p> <ul style="list-style-type: none"> ■ For Oracle Identity Self Service: <p><code>http://hostname:port/identity/faces/home</code></p> ■ For Oracle Identity System Administration: <p><code>http://hostname:port/sysadmin/faces/home</code></p> <p>where <code>hostname:port</code> can be for either Oracle Identity Manager or OHS, depending on whether a Domain Agent or WebGate is used.</p>	<p>The Oracle Access Management login page from the Access Manager managed server should display.</p> <p>Verify the links for "Forgot Password", "Self Register" and "Track Registration" features appear in the login page. Verify that each link works. For more information about these features, see Section 1.5.3, "Password Management Scenarios."</p>
3	Log in as <code>xelsysadm</code> (Oracle Identity Manager administrator).	The Oracle Identity Manager Admin Page should be accessible.
4	<p>Create a new user using Oracle Identity Self Service.</p> <p>Close the browser and try accessing the OIM Identity Page. When prompted for login, provide valid credentials for the newly-created user.</p>	<p>You should be redirected to Oracle Identity Manager and be required to reset the password.</p> <p>After resetting the password and setting the challenge question, user should be automatically logged into the application. Auto-login should work.</p>

Table 2–10 (Cont.) Verifying Access Manager and Oracle Identity Manager Integration

Step	Description	Expected Result
5	Close the browser and access Oracle Identity Self Service.	The Oracle Access Management login page from the Access Manager managed server should display. Verify the links for "Forgot Password", "Self Register" and "Track Registration" features appear in the login page. Verify that each link works. For more information about these features, see Section 1.5.3, "Password Management Scenarios."
6	Verify the lock/disable feature works by opening a browser and logging in as a test user. In another browser session, log in as an administrator, then lock the test user account.	The user must be redirected back to the login page while accessing any of the links.
7	Verify the SSO logout feature works by logging into Oracle Identity Self Service as test user or system administrator.	Upon logout from the page, you are redirected to the SSO logout page.

2.10 Troubleshooting Common Problems

This section describes common problems you might encounter in an Oracle Identity Manager and Access Manager integrated environment and explains how to solve them. It is organized by common problem types and contains the following topics:

- [Single Sign-On Issues](#)
- [Auto-Login Issues](#)
- [Session Termination Issues](#)
- [Account Self-Locking Issues](#)
- [Miscellaneous Issues](#)

In addition to this section, review the *Oracle Fusion Middleware Error Messages Reference* for information about the error messages you may encounter.

For information about additional troubleshooting resources, see [Section 1.7, "Using My Oracle Support for Additional Troubleshooting Information."](#)

2.10.1 Single Sign-On Issues

This section describes common problems and solutions relating to single sign-on in the integrated environment. Using single sign-on, a user can access Oracle Identity Manager resources after being successfully authenticated by Access Manager. When accessing any Oracle Identity Manager resource protected by Access Manager, the user is challenged for their credentials by Access Manager using the Oracle Access Management Console login page.

This section discusses the following single sign-on issues:

- [Checking HTTP Headers](#)
- [User is Redirected to Wrong Login Page](#)
- [Login Fails](#)
- [Oracle Access Management Console Login Page Does Not Display](#)

- [Authenticated User is Redirected to Oracle Identity Manager Login Page](#)
- [User is Redirected to Oracle Identity Manager Login Page](#)
- [New User is Not Redirected to Change Password](#)
- [User is Redirected in a Loop](#)

2.10.1.1 Checking HTTP Headers

Checking the HTTP headers may provide diagnostic information about login issues. You can collect information from the HTTP headers for troubleshooting issues. This can be done by enabling HTTP tracing in the web browser, logging into Access Manager as a new user, and examining the headers for useful information.

2.10.1.2 User is Redirected to Wrong Login Page

After accessing an Oracle Identity Manager resource using OHS (for example, `http://OHS_HOST:OHS_PORT/identity`), the user is redirected to the Oracle Identity Manager login page instead of the Oracle Access Management Console login page.

Cause

The Access Manager WebGate is not deployed or configured properly.

Solution

Confirm the `httpd.conf` file contains the following entry at the end:

```
include "<ORACLE_WEBTIER_INST_HOME>/config/OHS/ohs1/webgate.conf"
```

where `webgate.conf` contains the 11g WebGate configuration.

If this entry is not found, review the 11g WebGate configuration steps to verify none were missed. For more information, see *Oracle Fusion Middleware Installing Webgates for Oracle Access Manager and Administrator's Guide for Oracle Access Management*.

2.10.1.3 Login Fails

User login fails with the following error:

```
An incorrect Username or Password was specified.
```

Cause

Access Manager is responsible for user authentication but authentication has failed. The identity store configuration may be wrong.

Solution

Check the identity store is configured correctly in the Oracle Access Management Console.

To resolve this problem:

1. Login to Oracle Access Management Console.
2. Navigate to **Configuration > User Identity Stores > OAMIDStore**.
3. Verify the Default Store and System Store configuration.
4. Click **Test Connection** to verify the connection.

2.10.1.4 Oracle Access Management Console Login Page Does Not Display

User is not directed to the Oracle Access Management Console to login and the following error message displays:

Oracle Access Manager Operation Error.

Cause 1

The OAM Server is not running.

Solution 1

Start the OAM Server.

Cause 2

The WebGate is not correctly deployed on OHS and is not configured correctly for the 10g or 11g Agent located on the OAM Server.

An error message displays, for example: The AccessGate is unable to contact any Access Servers.

The issue may be with the SSO Agent.

Solution 2

To resolve this problem:

1. Run `oamtest.jar` (`ORACLE_HOME/oam/server/tester`) and test the connection by specifying AgentID.

The AgentID can be found in `ObAccessClient.xml`, located in the `webgate/config` directory in the `WEBSERVER_HOME`. For example:

```
<SimpleList>
    <NameValPair
        ParamName="id"
        Value="IAMAG_11g"></NameValPair>
</SimpleList>
```

If the Tester fails to connect, this confirms a problem exists with the SSO Agent configuration (password/host/port) on the OAM Server.

2. Re-create the 10g or 11g SSO Agent and then reconfigure the WebGate to use this Agent.

Follow the instructions in *Administrator's Guide for Oracle Access Management*.

2.10.1.5 Authenticated User is Redirected to Oracle Identity Manager Login Page

User authenticated using the Oracle Access Management Console but is redirected to the Oracle Identity Manager login page to enter credentials.

Cause 1

The security providers for the OIM domain are not configured correctly in Oracle WebLogic Server.

Solution 1

Verify the WebLogic security providers are configured correctly for the OIM domain security realm. Check the LDAP Authenticator setting. For more information, see [Section 2.8.2, "Validate Security Provider Configuration."](#)

Cause 2

OAMIDasserter is not configured correctly in Oracle WebLogic Server.

Solution 2

To resolve this problem:

1. Log in to Oracle WebLogic Server Administration Console.
2. Navigate to **Common** tab and verify **Active Types** contains the correct header for the WebGate type:
 - OAM_REMOTE_USER, for an 11g WebGate.
 - ObSSOCookie, for a 10g WebGate.

2.10.1.6 User is Redirected to Oracle Identity Manager Login Page

Access Manager relies upon Oracle Identity Manager for password management. If the user logs in for the first time or if the user password is expired, Access Manager redirects the user to the Oracle Identity Manager First Login page.

From the Access Manager login screen, user should be able to navigate to the Oracle Identity Manager Forgot Password flow, the Self-Registration or Track Registration flows.

Cause

If there is any deviation or error thrown when performing these flows, the configuration in oam-config.xml (*OAM_DOMAIN_HOME*/config/fmwconfig) is incorrect.

Solution

Verify the contents of oam-config.xml resembles the following example. Specifically, that HOST and PORT corresponds to the OHS (or any supported web server) configured to front-end Oracle Identity Manager resources.

```
Setting Name="IdentityManagement" Type="htf:map">
    <Setting Name="IdentityServiceConfiguration" Type="htf:map">
        <Setting Name="IdentityServiceProvider"
Type="xsd:string">oracle.security.am.engines.idm.provider.OracleIdentityServicePro
vider</Setting>
        <Setting Name="AnonymousAuthLevel" Type="xsd:integer">0</Setting>
        <Setting Name="IdentityServiceEnabled"
Type="xsd:boolean">true</Setting>
        <Setting Name="IdentityServiceProviderConfiguration"
Type="htf:map">
            <Setting Name="AccountLockedURL"
Type="xsd:string">/identity/faces/accountlocked</Setting>
            <Setting Name="ChallengeSetupNotDoneURL"
```

```

Type="xsd:string"/>/identity/faces/firstlogin</Setting>

    <Setting Name="DateFormatPattern"
Type="xsd:string">yyyy-MM-dd'T'HH:mm:ss'Z'</Setting>

    <Setting Name="ForcedPasswordChangeURL"
Type="xsd:string"/>/identity/faces/firstlogin</Setting>

    <Setting Name="IdentityManagementServer"
Type="xsd:string">OIM-SERVER-1</Setting>

    <Setting Name="PasswordExpiredURL"
Type="xsd:string"/>/identity/faces/firstlogin</Setting>

    <Setting Name="LockoutAttempts" Type="xsd:integer">5</Setting>

    <Setting Name="LockoutDurationSeconds"
Type="xsd:long">31536000</Setting>

</Setting>

</Setting>

<Setting Name="RegistrationServiceConfiguration" Type="htf:map">

    <Setting Name="RegistrationServiceProvider"
Type="xsd:string">oracle.security.am.engines.idm.provider.DefaultRegistrationServiceProvider</Setting>

    <Setting Name="RegistrationServiceEnabled"
Type="xsd:boolean">true</Setting>

    <Setting Name="RegistrationServiceProviderConfiguration"
Type="htf:map">

        <Setting Name="ForgotPasswordURL"
Type="xsd:string"/>/identity/faces/forgotpassword</Setting>

        <Setting Name="NewUserRegistrationURL"
Type="xsd:string"/>/identity/faces/register</Setting>

        <Setting Name="RegistrationManagementServer"
Type="xsd:string">OIM-SERVER-1</Setting>

        <Setting Name="TrackUserRegistrationURL"
Type="xsd:string"/>/identity/faces/trackregistration</Setting>

    </Setting>

</Setting>

<Setting Name="ServerConfiguration" Type="htf:map">

    <Setting Name="OIM-SERVER-1" Type="htf:map">

        <Setting Name="Host"
Type="xsd:string">myhost1.example.com</Setting>

        <Setting Name="Port" Type="xsd:integer">7777</Setting>
    </Setting>
    </Setting>

```

```

        <Setting Name="SecureMode" Type="xsd:boolean">false</Setting>
    </Setting>
    </Setting>
</Setting>

```

2.10.1.7 New User is Not Redirected to Change Password

A new user created in Oracle Identity Manager logs into Oracle Identity Manager for the first time and is not redirected to the First Login Page and prompted to change their password.

Cause

The Oracle Virtual Directory adapters (either OVD or libOVD, depending on the setup) are not configured correctly.

Solution

Locate the corresponding adapters.or_xml file and verify that the oamEnabled attribute is set to true for both the UserManagement and changelog adapters. For example:

```
<param name="oamEnabled" value="true" />
```

Next, verify that IdentityServiceEnabled is set to true in oam-config.xml (see [Section 2.10.1.5, "Authenticated User is Redirected to Oracle Identity Manager Login Page"](#)). For example:

```
<Setting Name="IdentityServiceEnabled" Type="xsd:boolean">true</Setting>
```

2.10.1.8 User is Redirected in a Loop

A new user attempts to access Oracle Identity Manager Self-Service and after successful authentication, the user is redirected in a loop. The service page does not load and the browser continues spinning or refreshing.

Cause

OHS configuration setting for WLCookieName for front-ending identity is incorrect.

Solution

Check the OHS configuration for front-ending identity and verify that WLCookieName directive is set to oimjsessionid. If not, set this directive as oimjsessionid for each Oracle Identity Manager resource Location entry. For example:

```

<Location /identity>
    SetHandler weblogic-handler
    WLCookieName oimjsessionid
    WebLogicHost myhost1.example.com
    WebLogicPort 8003
    WLogFile "$
Unknown macro: {ORACLE_INSTANCE}
/diagnostics/logs/mod_wl/oim_component.log"

```

</Location>

2.10.2 Auto-Login Issues

The auto-login feature enables user login to Oracle Identity Manager after the successful completion of the Forgot Password or Forced Change Password flows, without prompting the user to authenticate using the new password.

Communication between Oracle Identity Manager and Access Manager can be configured to use Oracle Access Protocol (OAP) or TAP channels. Debugging auto-login issues is simplified if you determine which channel is being used. Determine the channel by examining the Oracle Identity Manager `SSOConfig` MBean (version attribute) using the System MBean Browser in Oracle Enterprise Manager Fusion Middleware Control. For more information, see "Using the System MBean Browser" in *Administrator's Guide*.

Depending upon the Access Manager version being used, the following applies:

- If the version is 10g, the Oracle Access Protocol (OAP) channel is used during auto-login. See [Section 2.10.2.1, "TAP Protocol Issues."](#)

After a password is reset in Oracle Identity Manager and in LDAP through LDAP-synchronization, Oracle Identity Manager will auto-login the user by redirecting to the requested resource.

- If the version is 11g, the TAP channel is used during auto-login. See [Section 2.10.2.2, "Oracle Access Protocol \(OAP\) Issues."](#)

After a password is reset in Oracle Identity Manager and in LDAP through LDAP synchronization, Oracle Identity Manager redirects the user to the Access Manager TAP endpoint URL (`SSOConfig: TAPEndpointUrl`). Access Manager will auto-login the user by redirecting to the requested resource.

Note: In an 11g R2 Oracle Identity Manager and Access Manager integrated environment, the TAP protocol is configured for auto-login by default.

2.10.2.1 TAP Protocol Issues

Check the OIM Server and Access Manager Server logs for any of the following error messages.

2.10.2.1.1 404 Not Found Error After resetting the password, user is redirected to a 404 Not Found error page.

Cause

The Access Manager TAP endpoint URL (`SSOConfig: TAPEndpointUrl`) is configured incorrectly.

Solution

Verify that `TAPEndpointUrl` is correctly configured in Oracle Identity Manager `SSOConfig` and is accessible. For example:

```
http://OAM_HOST:OAM_PORT/oam/server/dap/cred_submit
```

Or

```
http://OHS_HOST:OHS_PORT/oam/server/dap/cred_submit
```

where Access Manager is front-ended by OHS.

2.10.2.1.2 System Error After resetting the password, user is redirected to Access Manager `TapEndpointUrl` (configured in Oracle Identity Manager `SSOConfig`), and the following error displays in the UI:

System error. Please re-try your action. If you continue to get this error, please contact the Administrator.

Cause 1

A message similar to the following displays in the Access Manager Server logs:

```
Sep 19, 2012 4:29:45 PM EST> <Warning> <oracle.oam.engine.authn>
<BEA-000000> <DAP Token not received>
<Sep 19, 2012 4:29:45 PM EST> <Error> <oracle.oam.binding> <OAM-00002>
<Error occurred while handling the request.
java.lang.NullPointerException
at
oracle.security.am.engines.enginecontroller.token.DAPTokenEncIssuerImpl.issue(DAPT
okenEncIssuerImpl.java:87)
```

Solution 1

This error could be due to mis-configuration in `TAPResponseOnlyScheme` in Access Manager. Verify `oam-config.xml` (located at `OAM_DOMAIN_HOME/config/fmwconfig`) contains the following entry:

```
<Setting Name="DAPModules" Type="htf:map">
    <Setting Name="7DASE52D" Type="htf:map">
        <Setting Name="MAPPERCLASS"
Type="xsd:string">oracle.security.am.engine.authn.internal.executor.DAPAttributeMa
pper</Setting>
        <Setting Name="MatchLDAPAttribute" Type="xsd:string">uid</Setting>
        <Setting Name="name" Type="xsd:string">DAP</Setting>
    </Setting>
</Setting>
```

The value of `MatchLDAPAttribute` should be `uid`. If not, change the value.

To resolve the problem:

1. Login to Oracle Access Management Console.
2. Navigate to `TapResponseOnlyScheme`. Add the following as Challenge parameter:
`MatchLDAPAttribute=uid`
3. Save the changes.

Cause 2

The following error displays in the Access Manager Server logs:

```
javax.crypto.BadPaddingException: Given final block not properly padded
```

This may occur if `OIM_TAP_PARTNER_KEY` is not include in the OIM credential map in the credential store, or if an invalid key is present.

Solution 2

Reregister Oracle Identity Manager as a TAP partner with Access Manager by rerunning the `idmConfigTool -configOIM` option. After the `-configOIM` option is run, you must restart the complete OIM domain.

Cause 3

After resetting the password, if auto-login is not successful, the OIM server logs contain the following error:

```
Error occured while retrieving TAP partner key from Credential store
```

Solution 3

To resolve the problem:

1. Using Fusion Middleware Control, verify the `OIM_TAP_PARTNER_KEY` generic credential is present in the OIM credential map in the credential store.
2. If `OIM_TAP_PARTNER_KEY` is present, verify that LDAP synchronization is configured correctly, and that the password is reset in LDAP provider. Check this by issuing an `ldapbind` command with the user and the new/reset password.

Cause 4

After resetting the password, if auto-login is not successful, the OIM server logs have the following error:

```
Error occured while retrieving DAP token from OAM due to invalid TAP partner key
```

The `OIM_TAP_PARTNER_KEY` present in the OIM credential map of credential store is not valid.

Solution 4

Reregister Oracle Identity Manager as a TAP partner with Access Manager by rerunning `idmConfigTool -configOIM` option. After the `-configOIM` option is run, you must restart the complete OIM domain.

2.10.2.2 Oracle Access Protocol (OAP) Issues

Check the OIM Server logs for any of the following types of error messages.

Cause 1

The resource URL is not protected.

Solution 1

Verify that the correct `host:port` combination is configured in the Access Manager host identifier configuration.

To resolve this problem:

1. Log in to the Oracle Access Management Administration Console:
`http://oam_adminserver_host:oam_adminserver_port/oamconsole`
2. In the Oracle Access Management Administration Console, click **Application Security** at the top of the window.
3. In the Application Security console, click **Agents** in the Agents section.
 The Search SSO Agents page opens with the WebGates tab active.
4. In the Search SSO Agents page that appears, enter `IAMSuiteAgent` as the name of the Agent you want to find.
5. Click **Search** to initiate the search.
6. Click **IAMSuiteAgent** in the Search Results table.
7. Check the host identifiers for `host:port` combination in the identifier. For example: `IAMSuiteAgent:/oim`
8. For the correct `host:port` combination, check the OIM logs for "Setting web resource url ". This statement will be above "Resource not protected URL" statement.
 In general, Host Identifier should have a combination of OHS (webserver) `host:port` which is front-ending Oracle Identity Manager.

Cause 2

`aaaClient` is not initialized.

Solution 2

Verify that the passwords seeded into OIM domain credential store are correct. For OPEN mode, check for the WebGate password. For SIMPLE mode, check that SSO keystore password and SSO global passphrase are seeded in correctly. For more information, see [Section 2.8.3, "Validate Oracle Identity Manager Domain Credential Store."](#)

Cause 3

Failed to communicate with any of configured OAM Server. Verify that it is up and running.

Solution 3

Verify that the passwords seeded into OIM domain credential store are correct. For OPEN mode, check for the WebGate password. For SIMPLE mode, check that SSO keystore password and SSO global passphrase also are seeded in correctly. For more information, see [Section 2.8.3, "Validate Oracle Identity Manager Domain Credential Store."](#)

Cause 4

`SSOKeystore` tampered or password is incorrect.

Solution 4

Check that the keystore file `ssoKeystore.jks` is present in `OIM_DOMAIN_HOME/config/fmwconfig`. If present, then check if the keystore password is seeded properly into OIM domain credential store. For more information, see [Section 2.8.3, "Validate Oracle Identity Manager Domain Credential Store."](#)

Cause 5

Oracle Identity Manager logs do not have any information about the failure.

Solution 5

To resolve this problem:

1. Enable HTTP headers and capture the headers while running through the First Login, Forgot Password flows. See [Section 2.10.1.1, "Checking HTTP Headers."](#)
2. In the HTTP headers, look for Set-Cookie: ObSSOCookie after the POST method on the First Login, Forgot Password page. Check the domain of the cookie. It should match with the domain for the protected resource URL.
 - If cookie domain is different, update the CookieDomain in the Oracle Identity Manager SSO configuration using Fusion Middleware Control. See [Section 2.8.1, "Validate Oracle Identity Manager SSOConfig."](#)
 - If cookie domain is correct, then check for any time differences on the machines which host the OIM and OAM Servers.

2.10.3 Session Termination Issues

The session termination feature enables the termination of all active user sessions after the user status is modified by an Oracle Identity Manager administrator. The following Oracle Identity Manager operations lead to session termination: user lock or unlock, enable or disable, modify or delete.

Session termination is triggered by Oracle Identity Manager invoking the Access Manager OAP APIs to terminate the session. Communication is over the OAP channel.

To troubleshoot session termination issues:

1. Verify the OAP-related configuration is stored in Oracle Identity Manager SSOConfig. See [Section 2.8.1, "Validate Oracle Identity Manager SSOConfig."](#)
2. Verify `/db/sssointg/EvenHandlers.xml` is in Oracle Identity Manager MDS. See [Section 2.8.4, "Validate Event Handlers for SSO."](#)
3. Verify that `AccessGateID` attribute in Oracle Identity Manager SSOConfig points to a 10g SSO Agent hosted by OAM Server.
4. If SSOConfig points to an 11g Agent ID:
 - a. Create a new 10g SSO Agent.
 - b. Set its ID in `AccessGateID` attribute.
 - c. Update the agent password (`SSOAccessKey`) in the OIM domain credential store.
 - d. If the communication mode is `SIMPLE`, a new keystore file (`ssoKeystore.jks`) must be created using the agent's `aaa_cert.pem` and `aaa_key.pem`, and copied to `OIM_DOMAIN_HOME/config/fmwconfig` directory.
 - e. In `SIMPLE` mode, update the SSO keystore key (`SSOKeystoreKey`) and the SSO global passphrase (`SSOGlobalPP`) in the OIM domain credential store.

For information about creating a new 10g SSO Agent or `ssoKeystore.jks`, see *Administrator's Guide for Oracle Access Management*.

2.10.4 Account Self-Locking Issues

Use Case 1

Both LDAP store and Access Manager lock out the user due to multiple failed login attempts. The user attempts to reset his or her password using the Oracle Identity Manager (OIM) "Forgot Password" page, but the reset operation fails.

Possible Explanation

The user's locked status has not yet propagated to Oracle Identity Manager.

1. Check if the user is locked in Oracle Identity Manager:
 - a. Log in to the Identity Self Service application as an Oracle Identity Manager administrator.
 - b. Navigate to the **Users** section, then search for the user.
 - c. Check if the Identity status is `locked`.
2. If the status is not `locked`, run an **LDAP User Create and Update Reconciliation** scheduled job, and then confirm that the user status is `locked`.

Use Case 2

The user account self-locks due to multiple invalid credentials login attempts. Later, when the user attempts to log in with the correct credentials, he or she is not able to log in. The user expects to log in first and then change the password, but login fails consistently.

Possible Explanation

Both LDAP directory and Access Manager may have locked the user account. In this case the user cannot log in to Oracle Identity Manager or to any protected page. The user has to use the Forgot Password flow to reset the password.

Note that if only Access Manager locks out the user, the user can log in to Oracle Identity Manager and change the password immediately.

Use Case 3

The LDAP directory `pwdMaxFailure` count of three is less than the `oblogintrycount` value of five. The LDAP directory locks out the user due to multiple invalid credentials login attempts (in this case, three attempts). Later, when the user tries to log in with the correct credentials, on the fourth attempt the user still cannot log in. The user expects to log in first and then change the password, but login fails consistently.

Possible Explanation

LDAP directory locked out the user, but Access Manager did not. The user cannot log in with the correct password even though the `oblogintrycount` is less than five, but following the Forgot Password flow works and resets the password.

Note that when LDAP directory locks out the user there is nothing to reconcile into Oracle Identity Manager because Oracle Identity Manager does not reconcile user accounts that are locked in LDAP store. When LDAP store locks the user, Oracle Identity Manager shows the user as active. Following the Forgot Password flow is the only way to reset the password.

Use Case 4

The LDAP directory `pwdMaxFailure` count value of seven is less than the `oblogintrycount` value of five. Access Manager locked out the user due to multiple invalid credentials login attempts. Later, when the user tries to login with the correct credentials, the user is able to log in and is redirected to change the password, but the reset password operation fails.

Possible Explanation

The user locked status has not yet propagated to Oracle Identity Manager.

1. Check if the user is locked in Oracle Identity Manager:
 - a. Login to Identity Self Service application as an Oracle Identity Manager administrator.
 - b. Navigate to **Users** section, then search for the user.
 - c. Check if the Identity status is `locked`.
2. If the status is not `locked`, run an **LDAP User Create and Update Reconciliation** scheduled job, and then confirm that the user status is `locked`.

Note that use case one and this use case look similar. In use case one, both LDAP directory and Access Manager locked the user account, whereas in this use case only Access Manager locks the user. The remedy for both use cases is the same, however.

Use Case 5

The user cannot remember his or her password and tries to reset the password using the Forgot Password flow. The user provides his or her user login, provides a new password, and provides incorrect challenge answers. After three failure attempts, both LDAP directory and Access Manager lock the user. The user expects to get locked out after five attempts instead of three attempts because the `oblogintrycount` value is 5.

Possible Explanation

The password reset attempts in the Oracle Identity Manager Reset/Forgot Password flow are governed by the Oracle Identity Manager system property `XL.MaxPasswordResetAttempts` and the default value is 3. Consequently, the user is locked out immediately after three attempts. Oracle Identity Manager locks the user natively in LDAP directory and in Access Manager.

Note that password reset attempts are different from login attempts. Login attempts are governed by Access Manager (`oblogintrycount=5`) and password reset attempts by Oracle Identity Manager (`XL.MaxPasswordResetAttempts=3`).

Use Case 6

LDAP directory locks the user because some constant LDAP binding used incorrect credentials. Access Manager does not lock out the user. When the user tries to log in with the correct credentials, he is not able to log in.

Possible Explanation

LDAP directory locks the user out in this use case, not Access Manager. The user cannot log in with the correct password even if the `oblogintrycount` is still less than 5, but the user can reset his or her password by following the Forgot Password flow.

Note that when a user is only locked out by LDAP directory, the user's lock-out status is not reconciled into Oracle Identity Manager. Consequently, the user shows up as

still active in Oracle Identity Manager even though the user is locked in LDAP directory.

Use Case 7

For Access Manager and Oracle Identity Manager integrated environments prior to 11.1.2.1, the automatic unlocking of users does not work.

Possible Explanation

For the automatic unlocking feature to work, additional patches to Oracle Access Manager, Oracle Identity Manager and Oracle Virtual Directory are required.

For a list of patches and instructions to configure automatic unlocking, see My Oracle Support document ID 1496808.1.

Use Case 8

When the user resets his password, the password reset is not immediate.

1. The user account self-locks due to multiple invalid credentials login attempts.
2. The user uses the Forgot Password flow to reset the password.
3. The user account is still locked, and he is not able to login to Oracle Identity Manager.

Possible Explanation

The user's locked status has not yet propagated to Oracle Identity Manager.

1. Check if the user is locked in Oracle Identity Manager:
 - a. Login to Identity Self service application as an Oracle Identity Manager administrator.
 - b. Navigate to the **Users** section, and then search for the user.
 - c. Check if the Identity status is locked.
2. If the status is not locked, run an **LDAP User Create and Update Reconciliation** scheduled job, and then confirm that the user status is locked.

2.10.5 Miscellaneous Issues

This provides solutions for the following miscellaneous issues:

- [Client Based Login to Oracle Identity Manager Fails](#)
- [Logout Throws 404 Error](#)
- [Old Password Still Works After a Password Reset](#)

2.10.5.1 Client Based Login to Oracle Identity Manager Fails

For successful client-based login to Oracle Identity Manager:

- The client-based login user must be present in the LDAP provider.
- An LDAP Authenticator must be configured in the OIM domain security realm corresponding to the LDAP provider where the user is present. See [Section 2.8.2, "Validate Security Provider Configuration."](#)

2.10.5.2 Logout Throws 404 Error

If logging out of an Oracle Identity Manager protected application throws a 404 error, verify that the logout configuration is present in `jps-config.xml`. See [Section 2.8.5, "Validate SSO Logout Configuration."](#)

If needed, the JPS configuration can be fixed by editing the `jps-configuration` file located in `$DOMAIN_HOME/config/fmwconfig` and then restarting all the servers.

To resolve a misconfiguration in `jps-config.xml`:

1. In a terminal window issue the following commands: `cd $DW_ORACLE_HOME/common/bin`
2. `./wlst.sh`
3. `connect()`
4. `addOAMSSOProvider(loginuri="/${app.context}/adfAuthentication", logouturi="/oamssso/logout.html", autologinuri="/obrar.cgi")`
5. `exit`
6. Restart all servers in the domain.

For information, see "Starting or Stopping the Oracle Stack" in *Installation Guide for Oracle Identity and Access Management*.

2.10.5.3 Old Password Still Works After a Password Reset

In Active Directory environments, old passwords can remain active for up to one hour after a password reset. During this interval, both the old and new password can successfully bind to the Active Directory server. This is the expected behavior.

2.10.5.4 ConfigOIM Failed While Seeding Oracle Identity Manager Policies into Access Manager

As part of running `configOIM`, Oracle Identity Manager policies are seeded into Access Manager using the Access Management exposed REST endpoint.

An exception while seeding Oracle Identity Manager policies occurs when the user credentials used for accessing Access Manager exposed endpoint does not have enough privileges to perform the operation.

The solution is as follows:

1. Make sure `IDSTORE_WLSADMINUSER` is the same user which was used while running the `prepareIdStore mode=wls` command.
2. Try to access the Access Manager REST endpoint using `curl` command:

```
curl -u weblogic_idm:Welcome1 "http://OAM_ADMIN_HOST:OAM_ADMIN_PORT/oam/services/rest/11.1.2.0.0/ssa/policyadmin/appdomain"
```

Where:

- `weblogic_idm` is the user as mentioned for `IDSTORE_WLSADMINUSER` and `Welcome1` is the password for the user.

If this command fails to return the list of application domains present in Access Manager, then make sure `configOAM` is run properly and the Access Manager admin server is restarted before running `configOIM`.

Integrating Access Manager, OAAM, and OIM

The Oracle Access Management Access Manager (Access Manager), Oracle Adaptive Access Manager (OAAM), and Oracle Identity Manager (OIM) integration provides control access to resources with Access Manager, strong multi-factor authentication and advanced real-time fraud prevention with OAAM, and self-service password management with OIM.

This chapter describes how to integrate Oracle Access Management Access Manager (Access Manager), Oracle Identity Manager (OIM), and Oracle Adaptive Access Manager.

You can also integrate with Oracle Privileged Account Manager (OPAM). Links to all available procedures appear in [Table 1–2](#) and [Table 1–3](#).

This chapter contains these sections:

- [About Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager Integration](#)
- [Definitions, Acronyms, and Abbreviations](#)
- [Integration Roadmap](#)
- [Integration Prerequisites](#)
- [Integrating Access Manager and Oracle Identity Manager](#)
- [Enabling LDAP Synchronization for Oracle Identity Manager](#)
- [Integrating Access Manager and Oracle Adaptive Access Manager](#)
- [Integrating Oracle Identity Manager and Oracle Adaptive Access Manager](#)
- [Performing Additional Configuration Depending on Deployment](#)
- [Troubleshooting Common Problems](#)

3.1 About Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager Integration

In the Oracle Access Management Access Manager (Access Manager), Oracle Adaptive Access Manager (OAAM), and Oracle Identity Manager (OIM) integration, the secure password collection features of the last two products are added to Access Manager-protected applications.

The range of secure password collection and challenge-related functionality include:

- Fine control over the authentication process and full capabilities of pre-authentication and post-authentication checking against OAAM policies.

Access Manager acts as the authenticating and authorizing service, while Oracle Adaptive Access Manager provides the rich, strong authenticators and performs risk and fraud analysis

- Robust challenge question feature set in Oracle Adaptive Access Manager that replaces the more limited set in Oracle Identity Manager
- Control of password validation, storage, and propagation duties and workflow capabilities
- Ability to create and reset the password without assistance for expired and forgotten passwords
- Secure access to multiple applications with one authentication step

Access Manager does not provide its own identity service; instead, Access Manager:

- Consumes identity services provided by Oracle Identity Manager, LDAP directories, and other sources; and
- Integrates with Oracle Identity Manager and Oracle Adaptive Access Manager to deliver a range of secure password collection functionality to Access Manager-protected applications.

Responsibilities are divided as follows:

Table 3–1 Responsibilities for Each Component in Integration

Component	Responsibilities
Oracle Adaptive Access Manager	Responsible for: <ul style="list-style-type: none"> ■ Running real-time risk analysis rules before and after authentication ■ Navigating the user through login, challenge, registration, and self-service flows
Oracle Identity Manager	Responsible for: <ul style="list-style-type: none"> ■ Provisioning users to add, modify, or delete users ■ Managing passwords through Reset Password or Change Password flows
Access Manager	Responsible for: <ul style="list-style-type: none"> ■ Authenticating and authorizing users ■ Providing advanced status flags such as Reset Password, Password Expired, User Locked, and others

3.1.1 Deployment Options for Strong Authentication

In the integration scenario, Access Manager acts as the authenticating and authorizing module, while Oracle Adaptive Access Manager provides strong authenticators and performs risk and fraud analysis.

There are two ways that Access Manager can leverage the strong authentication capabilities of Oracle Adaptive Access Manager:

- OAAM Basic Integration with Access Manager

Access Manager users who want to add login security, including Knowledge Based Authentication (KBA), may use OAAM Basic Integration with Access Manager (OAAM Basic). This option still requires an OAAM Admin Server, but it does not require the deployment of a separate OAAM Server. OAAM functionality is accessed through native OAAM calls. OAAM Basic has a smaller footprint than

OAAM Advanced Integration with Access Manager using TAP (OAAM Advanced using TAP).

The OAAM Basic differs from the OAAM Advanced using TAP in that it does not provide access to more advanced features such as One-Time Password (OTP) and Step Up Authentication. In addition, this native integration is not customizable beyond basic screen branding.

OAAM Basic cannot be used in the Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager integration.

- OAAM Advanced Integration with Access Manager
Access Manager users who want advanced features and customizations beyond that available with native integration may use OAAM Advanced Integration with Access Manager (OAAM Advanced using TAP). Leveraging the Java Oracle Access Protocol (OAP) library, the integration of Access Manager and Oracle Adaptive Access Manager requires a full OAAM deployment.

For implementation details, see [Appendix C, "Integrating Oracle Adaptive Access Manager with Access Manager."](#)

3.1.2 Deployment Options for Password Management

You can implement password management features for Access Manager-protected applications by integrating Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager.

This section explains the deployment options for password management. For more information about the scenarios that are supported by each deployment, and the flow that achieves each scenario see, [Section 1.5, "Common Integration Scenarios"](#).

In the context of password management, Access Manager works in different deployment modes:

1. Access Manager and Oracle Identity Manager integrated for authentication and password management.

For details, see [Section 1.5.3.1, "Access Manager Integrated with Oracle Identity Manager."](#)

2. Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager integrated for authentication, password management, fraud detection, and additional capabilities.

For details of the processing flow, see, [Section 1.5, "Common Integration Scenarios"](#).

For implementation details, see [Section 3.3, "Integration Roadmap."](#)

3. Access Manager also provides a password policy management feature through the Oracle Access Management Console. The password policy is applied to all resources protected by Access Manager. This feature is not used in the Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager integration documented in this chapter. For more information about this Oracle Access Management feature, see "Managing Common Services, Certificate Validation, and Password Policy" in *Administrator's Guide for Oracle Access Management*.

3.2 Definitions, Acronyms, and Abbreviations

This section provides key definitions, acronyms, and abbreviations that are related to the Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager integration.

Table 3–2 Advanced Integration Terms

Term	Definition
Action	<p>Oracle Adaptive Access Manager provides functionality to calculate the risk of an access request, an event or a transaction, and determine proper outcomes to prevent fraud and misuse. The outcome can be an action, which is an event activated when a rule is triggered. For example: block access, challenge question, ask for PIN or password, and so on.</p> <p>For information, see "Managing Policies, Rules, and Conditions" in <i>Administering Oracle Adaptive Access Manager</i>.</p>
Advanced integration with Access Manager	<p>OAAM Advanced Integration is an integration of Access Manager and full deployment of Oracle Adaptive Access Manager with or without integrating Oracle Identity Manager.</p> <ul style="list-style-type: none"> ■ An Access Manager and Oracle Adaptive Access Manager integration with a full OAAM deployment without Oracle Identity Manager. This option provides authentication schemes, device fingerprinting, risk analysis, KBA challenge mechanisms, and additional advanced security access features, such as step up authentication. It includes advanced features and extensibility such as OTP Anywhere, challenge processor framework, shared library framework, and secure self-service password management flows. ■ An Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager integration. This option provides advanced features and customizations beyond that available with native integration. Leveraging the Java OAP library, the integration of Access Manager and Oracle Adaptive Access Manager requires a full OAAM deployment.
Alert	<p>Alerts are messages that indicate the occurrence of an event. An event can be that a rule was triggered, a trigger combination was met or an override was used.</p> <p>Alert groups are used as results within rules so that when a rule is triggered all of the alerts within the groups are created.</p> <p>For information, see "Managing Policies, Rules, and Conditions" in <i>Administering Oracle Adaptive Access Manager</i>.</p>
Authentication	<p>Authentication is the process of verifying a person's, device's, or application's identity. Authentication deals with the question "Who is trying to access my services?"</p>

Table 3–2 (Cont.) Advanced Integration Terms

Term	Definition
Authentication Level	<p>Access Manager supports various authentication levels to which resources can be configured so as to provide discrete levels of security required to access various resources. Discrete authentication levels distinguish highly protected resources from other resources. The TAP token sent by Access Manager provides parameters related to the authentication level.</p> <p>The trust level of the authentication scheme reflects the challenge method and degree of trust used to protect transport of credentials from the user.</p> <p>The trust level is expressed as an integer value between 0 (no trust) and 99 (highest level of trust).</p> <p>Note: After a user is authenticated for a resource at a specified level, the user is automatically authenticated for other resources in the same application domain or in different application domains, if the resources have the same or a lower trust level as the original resource.</p> <p>Current Authentication level is the current authentication level of the user.</p> <p>Target Authentication level is the authentication level required to access the protected resource.</p>
Authorization	<p>Authorization regards the question "Who can access what resources offered by which components?"</p>
Authentication Scheme	<p>Access to a resource or group of resources can be governed by a single authentication process known as an authentication scheme. An authentication scheme is a named component that defines the challenge mechanism required to authenticate a user. Each authentication scheme must also included a defined authentication module.</p> <p>When you register a partner (either using the Oracle Access Management Console or the remote registration tool), the application domain that is created is seeded with a policy that uses the authentication scheme that is set as the default scheme. You can choose any of the existing authentication schemes as the default for use during policy creation.</p>
Authentipad Checkpoint	<p>The Authentipad checkpoint determines the type of device to use based on the purpose of the device.</p>
Basic Integration of Access Manager and OAAM	<p>Access Manager users wishing to add login security, including Knowledge Based Authentication (KBA), may use OAAM Basic Integration (native). This integration option will still require an OAAM Admin Server, but it does not require a separate deployment of the OAAM Server (the functionality is accessed through native OAAM calls); therefore, the footprint is reduced.</p> <p>The native integration does not provide access to more advanced features such as One-Time Password (OTP) through SMS, email, or IM. The native integration is not customizable beyond basic screen branding.</p>
Blocked	<p>A user is blocked when a policy has found certain conditions to be "true" and is set up to respond to these conditions with a "Block" action. If those conditions change, the user may no longer be "blocked." The "Blocked" status is not necessarily permanent and therefore may or may not require an administrator action to resolve.</p>
Challenge Parameters	<p>Challenge parameters are short text strings consumed and interpreted by WebGates and Credential Collector modules to operate in the manner indicated by those values. The syntax for specifying any challenge parameter is:</p> <p><parameter>=<value></p> <p>This syntax is not specific to any WebGate release (10g versus 11g). Authentication schemes are independent of WebGate release.</p>

Table 3–2 (Cont.) Advanced Integration Terms

Term	Definition
Challenge Questions	<p>Challenge Questions are a finite list of questions used for secondary authentication.</p> <p>During registration, users are presented with several question menus. For example, he may be presented with three question menus. A user must select one question from each menu and enter answers for them during registration. Only one question from each question menu can be registered. These questions become the user's "registered questions."</p> <p>When rules in OAAM Admin trigger challenge questions, OAAM Server displays the challenge questions and accepts the answers in a secure way for users. The questions can be presented in the QuestionPad, TextPad, and other virtual authentication devices, where the challenge question is embedded into the image of the authenticator, or simple HTML.</p>
Checkpoint	<p>A checkpoint is a specified point in a session when Oracle Adaptive Access Manager collects and evaluates security data using the rules engine.</p> <p>Examples of checkpoints are:</p> <ul style="list-style-type: none"> ■ Pre-authentication: Rules are run before a user completes the authentication process. ■ Post-authentication: Rules are run after a user is successfully authenticated. <p>For information, see "Managing Policies, Rules, and Conditions" in <i>Administering Oracle Adaptive Access Manager</i>.</p>
Delegated Authentication Protocol	<p>The Delegated Authentication Protocol (DAP) challenge mechanism indicates that Access Manager does an assertion of the token that it receives, which differs from the standard challenge "FORM" mechanism with the external option.</p>
Device	<p>Device is a computer, PDA, cell phone, kiosk, and other web-enabled device used by a user</p>
Device fingerprinting	<p>Device fingerprinting collects information about the device such as browser type, browser headers, operating system type, locale, and so on. Fingerprint data represents the data collected for a device during the login process that is required to identify the device whenever it is used to log in. The fingerprinting process produces a fingerprint that is unique to the user and designed to protect against the "replay attacks" and the "cookie-based registration bypass" process. The fingerprint details help in identifying a device, check whether it is secure, and determine the risk level for the authentication or transaction.</p> <p>A customer typically uses these devices to log in: PC, notebook, mobile phone, smart phone, or other web-enabled machines.</p>

Table 3–2 (Cont.) Advanced Integration Terms

Term	Definition
IAMSuiteAgent	<p>The IAMSuiteAgent (Security Provider in WebLogic Server and corresponding 10g Webgate Profile in Access Manager) is installed out of the box when you install Access Manager. It is implemented directly on the WebLogic Server and evaluates all requests coming in to the WebLogic Server. The IAMSuiteAgent is preconfigured to provide Single-Sign On (using the IAMSuiteAgent WebGate Profile in Access Manager) for the Identity Management domain consoles, Oracle Identity Manager, Oracle Adaptive Access Manager, and other Identity Management servers created during domain creation. It is like a WebGate, but it only protects internal URLs (configured out of the box with the IAM Suite application domain in Access Manager) provided by various products in the Identity and Access Management Suite. In enterprise deployments, there is usually a reverse proxy layer of web servers between the Identity and Access Management products and the end user. Because of this, you could remove the IAMSuiteAgent (Security Provider in WebLogic Server) and configure appropriate WebGate and Host Identifiers through the Oracle Access Management Administration Console and use the IAM Suite application domain with the newly created WebGate front ending Identity and Access Management components/products. If required, resources similar to IAM Suite application domain can be added to the authentication/authorization policies of the WebGate's application domain (if a new application domain is created with the creation of the WebGate Profile front ending Identity and Access Management components/products).</p> <p>Even after disabling/deleting IAMSuiteAgent Provider on WebLogic, the IAMSuite WebGate profile on Access Manager could be used. This IAMSuite WebGate profile is used in the Access Manager and OAAM integration using TAP.</p>
Knowledge Based Authentication (KBA)	<p>Knowledge-based authentication (KBA) is a secondary authentication method that provides an infrastructure based on registered challenge questions.</p> <p>It enables end-users to select questions and provide answers which are used to challenge them later on.</p> <p>Security administration include:</p> <ul style="list-style-type: none"> ■ Registration logic to manage the registration of challenge questions and answers ■ Answer Logic to intelligently detect the correct answers in the challenge response process ■ Validations for answers given by a user at the time of registration <p>For information, see "Managing Knowledge-Based Authentication" in the <i>Administering Oracle Adaptive Access Manager</i>.</p>
KeyPad	<p>Virtual keyboard for entry of passwords, credit card number, and so on. The KeyPad protects against Trojan or keylogging.</p>
LDAPScheme	<p>The Authentication scheme used to protect Access Manager-related resources (URLs) for most directory types based on a form challenge method.</p>

Table 3–2 (Cont.) Advanced Integration Terms

Term	Definition
Multi-Level Authentication	<p>Every authentication scheme requires an authentication level. The lower this number, the less stringent the scheme. A higher level number indicates a more secure authentication mechanism.</p> <p>Single sign-on (SSO) capability enables users to access more than one protected resource or application with a single sign in. After a successful user authentication at a specific level, the user can access one or more resources protected by one or more application domains. However, the authentication schemes used by the application domains must be at the same level (or lower). When a user accesses a resource protected with an authentication level that is greater than the level of his current SSO token, he is re-authenticated. In the Step Up Authentication case, the user maintains his current level of access even if failing the challenge presented for the higher level. This is "additional authentication".</p> <p>For information, see "Managing Authentication and Shared Policy Components" in <i>Administrator's Guide for Oracle Access Management</i>.</p>
Oracle Access Protocol (OAP)	<p>Oracle Access Protocol (OAP) enables communication between Access System components (for example, OAM Server, WebGate) during user authentication and authorization. This protocol was formerly known as NetPoint Access Protocol (NAP) or COREid Access Protocol.</p>
One-time Password (OTP)	<p>One-time Password is a risk-based challenge solution consisting of a server generated one time password delivered to an end user via a configured out of band channel. Supported OTP delivery channels include short message service (SMS), email, and instant messaging. OTP can be used to compliment KBA challenge or instead of KBA. As well both OTP and KBA can be used alongside practically any other authentication type required in a deployment. Oracle Adaptive Access Manager also provides a challenge processor framework. This framework can be used to implement custom risk-based challenge solutions combining third party authentication products or services with OAAM real-time risk evaluations.</p> <p>For information, see "Setting Up OTP Anywhere" in <i>Administering Oracle Adaptive Access Manager</i>.</p>
Access Manager and Oracle Adaptive Access Manager TAP Integration	<p>In Access Manager and OAAM TAP Integration, OAAM Server acts as a trusted partner application. The OAAM Server uses the Trusted authentication protocol (TAP) to communicate the authenticated user name to the OAM Server after it performs strong authentication, risk and fraud analysis and OAM Server will own the responsibility of redirecting to the protected resource.</p>
OAAM Admin	<p>OAAM Administration Console. Web application to administer all environment and Adaptive Risk Manager and Adaptive Strong Authenticator features.</p>
OAMAdminConsoleScheme	<p>Authentication scheme for Oracle Access Management Console.</p>
OAAMAdvanced	<p>Authentication scheme that protects resources with an external context type. This authentication scheme is used when complete integration with OAAM is required. A WebGate must front end the partner.</p>
OAAMBasic	<p>Authentication scheme that protects resources with a default context type. This scheme should be used when OAAM Basic integration with Access Manager is required. Here, advanced features like OTP are not supported.</p>
OAAM Server	<p>Runtime component that includes the rules engine and end user interface flows. It provides adaptive risk manager and adaptive strong authentication features, Web services, LDAP integration, and user Web application which is used in all deployment types except native integration</p>
Policies	<p>Policies contain security rules and configurations used to evaluate the level of risk at each checkpoint.</p> <p>For information, see "Managing Policies, Rules, and Conditions" in <i>Administering Oracle Adaptive Access Manager</i>.</p>

Table 3–2 (Cont.) Advanced Integration Terms

Term	Definition
Post-authentication rules	<p>Rules are run after a user is successfully authenticated.</p> <p>For information, see "Managing Policies, Rules, and Conditions" in <i>Administering Oracle Adaptive Access Manager</i>.</p>
Pre-authentication rules	<p>Rules are run before a user completes the authentication process.</p> <p>For information, see "Managing Policies, Rules, and Conditions" in <i>Administering Oracle Adaptive Access Manager</i>.</p>
Profile	The customer's registration information including security phrase, image, challenge questions, challenge (question and OTP) counters, and OTP.
Protection level	<p>There are three protection levels in which to choose from:</p> <ul style="list-style-type: none"> ■ Protected (the default). Protected resources are associated with a protected-level Authentication policy that uses a variety of authentication schemes (LDAP, for example). Authorization policies are allowed for protected resources. Responses, constraints, auditing, and session management are enabled for protected resources using a policy that protects the resource. ■ Unprotected. Unprotected resources are associated with an unprotected-level Authentication policy (level 0) that can use a variety of authentication schemes (LDAP, for example). Authorization policies are allowed for unprotected resources, and a basic one is needed to allow such access. However, an elaborate policy with constraints and responses is irrelevant. Responses, constraints, and auditing are enabled for Unprotected resources using a policy that protects the resource. Only Session Management is not enabled. Access to Unprotected resources incur an OAM Server check from WebGate, which can be audited. ■ Excluded (these are public). Only HTTP resource types can be excluded. Typically security insensitive files like Images (*.jpg, *.png), protection level Excluded resources do not require an OAM Server check for Authentication, Authorization, Response processing, Session management, and Auditing. Excluded resources cannot be added to any user-defined policy in the Oracle Access Management Console. The WebGate does not contact the OAM Server while allowing access to excluded resources; therefore, such access is not audited. Most regular resource validations apply to Excluded resources. However, excluded resources are not listed when you add resources to a policy. There is no Authentication or Authorization associated with the resource. Note: If a resource protection level is modified from "Protected" to "Excluded" and a policy exists for that resource, modification will fail until the resource is first disassociated with the policy.
Registration	<p>Registration is the enrollment process, the opening of a new account, or other event where information is obtained from the user.</p> <p>During the Registration process, the user is asked to register for questions, image, phrase and OTP (email, phone, and so on) if the deployment supports OTP. Once successfully registered, OTP can be used as a secondary authentication to challenge the user.</p>
Risk score	<p>OAAM risk scoring is a product of numerous fraud detection inputs such as a valid user, device, location, and so on. These inputs are weighted and analyzed within the OAAM fraud analytics engine. The policy generates a risk score based on dozens of attributes and factors. Depending on how the rules in a policy are configured, the system can yield an elevated risk score for more risky situations and lower scores for lower-risk situations. The degree of elevation can be adjusted with the weight assigned to the particular risk. The risk score is then used as an input in the rules engine. The rules engine evaluates the fraud risk and makes a decision on the action to take.</p>
Rules	<p>Fraud rules are used to evaluate the level of risk at each checkpoint. For information on policies and rules, see the "OAAM Policy Concepts and Reference" chapter in the <i>Administering Oracle Adaptive Access Manager</i>.</p>

Table 3–2 (Cont.) Advanced Integration Terms

Term	Definition
Single sign-on (SSO)	Single sign-on (SSO) is a process that gives users the ability to access multiple protected resources (Web pages and applications) with a single authentication.
Step Up Authentication	<p>Step Up Authentication occurs when a user is attempting to access a resource more sensitive than ones he had already accessed in this session. To gain access to the more sensitive resource, a higher level of assurance is required. Oracle Access Management resources are graded by authentication level, which defines the relative sensitivity of a resource.</p> <p>For example, if a user accesses a corporate portal home page that is defined as authentication level 3, a basic password authentication is required. The time card application that links off the portal home is more sensitive than the portal home page, so the application is defined as authentication level 4, which requires basic password and risk-based authentication provided by Oracle Adaptive Access Manager. So, if a user logs in to the portal with a valid user name and password, and then clicks the time card link, his device is fingerprinted and risk analysis determines if additional authentication, such as a challenge question, is required to allow him access.</p>
Strong Authentication	<p>An authentication factor is a piece of information and process used to authenticate or verify the identity of a person or other entity requesting access under security constraints. Two-factor authentication (T-FA) is a system wherein two different factors are used in conjunction to authenticate. Using two factors as opposed to one factor generally delivers a higher level of authentication assurance.</p> <p>Using more than one factor is sometimes called strong authentication or multi-factor authentication.</p>
TAP	TAP stands for Trusted authentication protocol. This is to be used, when authentication is performed by a third party and Access Manager asserts the token sent back. After asserting the token, Access Manager creates its cookie and continues the normal single-sign on flow. A trust mechanism exists between the OAM Server and the external third party which performs the authentication. In this scenario, Access Manager acts as an asserter and not authenticator.
TAPScheme	<p>This is the authentication scheme that is used to protect resources in an Access Manager and OAAM integration that uses TAP. If you want two TAP partners with different tapRedirectUrls, create a new authentication scheme using the Oracle Access Management Console and use that scheme.</p> <p>When configured, this authentication scheme can collect context-specific information before submitting the request to the Access Server. Context-specific information can be in the form of an external call for information.</p>
TextPad	Personalized device for entering a password or PIN using a regular keyboard. This method of data entry helps to defend against phishing. TextPad is often deployed as the default for all users in a large deployment then each user individually can upgrade to another device if they wish. The personal image and phrase a user registers and sees every time they login to the valid site serves as a shared secret between user and server.

Table 3–2 (Cont.) Advanced Integration Terms

Term	Definition
Virtual authentication device	A personalized device for entering a password or PIN or an authentication credential entry device. The virtual authentication devices harden the process of entering and transmitting authentication credentials and provide end users with verification they are authenticating on the valid application.
Web Agent	<p>A single sign-on agent (also known as a policy-enforcement agent, or simply an agent) is any front-ending entity that acts as an access client to enable single sign-on across enterprise applications.</p> <p>To secure access to protected resources, a Web server, Application Server, or third-party application must be associated with a registered policy enforcement agent. The agent acts as a filter for HTTP requests, and must be installed on the computer hosting the Web server where the application resides.</p> <p>Individual agents must be registered with Access Manager 11g to set up the required trust mechanism between the agent and OAM Server. Registered agents delegate authentication tasks to the OAM Server.</p>
WebGate	Web server plug-in that acts as an access client. WebGate intercepts HTTP requests for Web resources and forwards them to the OAM Server for authentication and authorization

3.3 Integration Roadmap

[Table 3–3](#) lists the high-level tasks for integrating Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager.

Table 3–3 Integration Flow for Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager

Number	Task	Information
1	Verify that all required components have been installed and configured prior to integration.	For information, see " Integration Prerequisites ".
2	Integrate Access Manager and Oracle Identity Manager.	For information, see " Integrating Access Manager and Oracle Identity Manager ".
3	Configure LDAP synchronization for Oracle Identity Manager. This is required for integration between Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager.	For information, see " Enabling LDAP Synchronization for Oracle Identity Manager ".
4	Integrate Access Manager and Oracle Adaptive Access Manager.	For information, see " Integrating Access Manager and Oracle Adaptive Access Manager ".
5	Set up the integration between OAAM and OIM.	For information, see " Integrating Oracle Identity Manager and Oracle Adaptive Access Manager ".
6	Perform additional configuration that you may need depending on your requirements.	For information, see " Performing Additional Configuration Depending on Deployment ".

3.4 Integration Prerequisites

Prior to integrating Oracle Access Management Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager, you must have installed all the required components, including any dependencies, and configured the environment in preparation for the integration tasks that follow.

Note: Key installation and configuration information is provided in this section. However, not all component prerequisite, dependency, and installation instruction is duplicated here. Adapt information as required for your environment.

For complete installation information, follow the instructions in *Installation Guide for Oracle Identity and Access Management*.

Table 3–4 lists the required components that must be installed and configured before the Oracle Access Management Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager integration tasks are performed.

Table 3–4 Access Manager, OAAM, and OIM Integration Required Components

Component	Information
Oracle Database	<p>Ensure that you have an Oracle Database installed on your system before installing Oracle Identity and Access Management. The database must be up and running to install the relevant Oracle Identity and Access Management components.</p> <p>For more information, see "Database Requirements" in <i>Installation Guide for Oracle Identity and Access Management</i>.</p> <p>For information about certified databases, see the "Database Requirements" topic in the <i>Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)</i> document.</p>
Repository Creation Utility (RCU)	<p>Install and run the Repository Creation Utility to create the schemas for Access Manager, OAAM, and OIM in a database. You must use the Repository Creation Utility that is version compatible with the products you are installing.</p> <p>Note: To create database schemas for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) components, you must use the 11g Release 2 (11.1.2.3.0) version of the Oracle Fusion Middleware Repository Creation Utility.</p> <p>Oracle Fusion Middleware Repository Creation Utility (RCU) is available on the Oracle Technology Network (OTN) Web site. For more information about using RCU, see "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)" in <i>Installation Guide for Oracle Identity and Access Management</i> and <i>Oracle Fusion Middleware Repository Creation Utility User's Guide</i>.</p> <p>For information about RCU requirements for Oracle Databases, see "RCU Requirements for Oracle Databases" in the <i>Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)</i> document.</p>
Oracle Unified Directory	<p>Oracle Unified Directory (OUD) is configured as your LDAP identity store. For information, see Section 2.3, "Configuring the Identity Store."</p> <p>Other component LDAP Servers are possible. Refer to Section 2.3, "Configuring the Identity Store" for more information about supported configurations.</p>
Oracle WebLogic Servers for Access Manager, Oracle Adaptive Access Manager, Oracle Identity Manager, and Oracle HTTP Server	<p>Prior to installing the Oracle WebLogic Server, ensure that your machines meet the system, patch, kernel, and other requirements.</p> <p>Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager can be configured on the same WebLogic Domain or separate WebLogic Domains. By default, the Access Manager and OAAM applications are configured on separate WebLogic Domains.</p> <p>For complete information about installing Oracle WebLogic Server, see <i>Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server</i>.</p>

Table 3–4 (Cont.) Access Manager, OAAM, and OIM Integration Required Components

Component	Information
Access Manager	<p>For information on installing and configuring Access Manager, see "Installing and Configuring Oracle Identity and Access Management (11.1.2)" and "Configuring Oracle Access Management" in <i>Installation Guide for Oracle Identity and Access Management</i>.</p> <p>Install Oracle Access Management Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager on different WebLogic Servers.</p> <p>Oracle Adaptive Access Manager and Access Manager can be in a new WebLogic Domain or in an existing one. They can be on the same domain or separate WebLogic Domains.</p> <p>At installation, Access Manager is configured with the database policy store. The Access Manager and Oracle Adaptive Access Manager wiring requires the database policy store.</p>
OAAM	<p>For information on installing and configuring Oracle Adaptive Access Manager, see "Installing and Configuring Oracle Identity and Access Management (11.1.2)" and "Configuring Oracle Adaptive Access Manager" in <i>Installation Guide for Oracle Identity and Access Management</i>.</p>
OIM	<p>For more information, see "Installing and Configuring Oracle Identity and Access Management" and "Configuring Oracle Identity Manager" in <i>Installation Guide for Oracle Identity and Access Management</i>.</p> <p>Note: When configuring Oracle Identity Manager, the LDAP directory must be configured to be used as an identity store. Ensure that all installation instructions are followed, including any prerequisites for enabling LDAP synchronization. For more information, see Enabling LDAP Synchronization in Oracle Identity Manager.</p> <p>Note: You must create the <code>wfullclient.jar</code> when installing Oracle Identity Manager and this file must be present before performing the integration steps. Follow the installation instructions carefully. For information on creating the <code>wfullclient.jar</code>, see "Post-Configuration Steps" in <i>Installation Guide for Oracle Identity and Access Management</i>.</p>
Oracle SOA Suite and patches	<p>For more information on installing and configuring the SOA Suite, see <i>Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite</i></p>
Oracle HTTP Server	<p>For more information on installing the HTTP Server, see <i>Oracle Fusion Middleware Installation Guide for Oracle Web Tier</i>.</p>
Oracle Access Manager 10g or Access Manager 11g agent (WebGate) for Oracle HTTP Server 11g on the Oracle HTTP Server 11g instance.	<p>Prior to installing the WebGate with Access Manager, review <i>Oracle Fusion Middleware Supported System Configurations</i> from the Oracle Technology Network to locate the certification information for the 10g or 11g WebGate you want to use for your deployment.</p> <p>For information on installing and registering 10g WebGates to use with Access Manager 11g, see "Registering and Managing 10g WebGates with Access Manager 11g" in <i>Administrator's Guide for Oracle Access Management</i>.</p> <p>For information on installing and registering 11g WebGate for use with Access Manager 11g, see "Installing and Configuring Oracle HTTP Server 11g WebGate for OAM" in <i>Oracle Fusion Middleware Installing Webgates for Oracle Access Manager</i>.</p>

The steps below are based on the assumption that Access Manager and Oracle Identity Manager are integrated using the out-of-the box integration.

Note: If so preferred, Oracle Access Management Access Manager and Oracle Adaptive Access Manager can be installed in separate domains or on the same WebLogic Domain.

For multiple domain installation, the `oaam.csf.useMBeans` property must be set to `true`. Refer to "Set Up the Credential Store Framework (CSF) Configuration" in the *Administering Oracle Adaptive Access Manager* for information on setting this parameter.

During the integration steps below, for reference we will refer to the WebLogic Server Domain which contains Oracle Access Management Access Manager as `OAM_DOMAIN_HOME`, and the WebLogic Server Domain which contains OAAM as `OAAM_DOMAIN_HOME`.

3.5 Integrating Access Manager and Oracle Identity Manager

Integration between Oracle Identity Manager and Access Manager is required for integration between Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager.

For more information, see [Chapter 2, "Integrating Access Manager and Oracle Identity Manager."](#)

3.6 Enabling LDAP Synchronization for Oracle Identity Manager

Enabling LDAP synchronization for Oracle Identity Manager is required for integration between Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager.

Oracle Adaptive Access Manager works off the same directory with which Oracle Identity Manager is synchronizing.

Note: The UID must match the CN of the newly created user in the LDAP store; otherwise, a login failure occurs.

For information about enabling LDAP synchronization for Oracle Identity Manager, see [Appendix E, "Enabling LDAP Synchronization in Oracle Identity Manager"](#)

3.7 Integrating Access Manager and Oracle Adaptive Access Manager

This task involves integrating the Access Manager and Oracle Adaptive Access Manager components as part of integrating Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager to deliver password management and challenge-related functionality to Access Manager-protected applications.

You configure the Access Manager and Oracle Adaptive Access Manager integration so that the OAAM server acts as a trusted partner application. The OAAM server uses the Trusted Authentication Protocol (TAP) to communicate the authenticated user name to the OAM Server after it performs strong authentication, and risk and fraud analysis. In this integration, the OAM Server is responsible for redirecting to the protected resource.

For information on integrating Oracle Adaptive Access Manager and Access Manager, refer to [Appendix C, "Integrating Oracle Adaptive Access Manager with Access Manager."](#)

Table 3–5 lists the high-level tasks for integrating Access Manager and Oracle Adaptive Access Manager and provides references to where the instructions are located.

The configuration instructions assume Access Manager and Oracle Adaptive Access Manager are integrated using the out-of-the box integration.

Table 3–5 Integration Flow for Access Manager and Oracle Adaptive Access Manager

Number	Task	Information
1	Verify that all required components have been installed and configured prior to integration.	For information, see " Integration Prerequisites. "
2	Ensure the Access Manager and OAAM Administration Consoles and managed servers are running.	For information, see " Restarting the Servers. "
3	Create the OAAM Admin users and OAAM groups. Before you can access the OAAM Administration Console, you must create administration users.	For information, see " Creating the OAAM Users and OAAM Groups. "
4	Import the OAAM base snapshot. A full snapshot of policies, dependent components and configurations is shipped with Oracle Adaptive Access Manager. For Oracle Adaptive Access Manager to be functional, you must import the snapshot into the system.	For information, see " Importing the Oracle Adaptive Access Manager Snapshot. "
5	Validate that Access Manager was set up correctly. You should be able to log in to the Oracle Access Management Console successfully.	For information, see " Validating Initial Configuration of Access Manager. "
6	Verify that Oracle Adaptive Access Manager is set up correctly by accessing the OAAM Server.	For information, see " Validating Initial Configuration of Oracle Adaptive Access Manager. "
7	Register the WebGate agent with Access Manager 11g to set up the required trust mechanism between the Agent and OAM Server. After registration, the Agent collaborates communication between the OAM Server and its services and acts as a filter for HTTP/HTTPS requests. The Agent intercepts requests for resources protected by Access Manager and works with Access Manager to fulfill access requirements.	For information on installing and registering 10g WebGates to use with Access Manager 11g, see "Registering and Managing 10g WebGates with Access Manager 11g" in <i>Administrator's Guide for Oracle Access Management</i> . For information on installing and registering 11g WebGate for use with Access Manager 11g, see "Installing and Configuring Oracle HTTP Server 11g WebGate for OAM" in <i>Oracle Fusion Middleware Installing Webgates for Oracle Access Manager</i> .
8	Register the OAAM server to act as a trusted partner application to Access Manager. A partner application is any application that delegates the authentication function to Access Manager 11g.	For information, see " Registering the OAAM Server as a Partner Application to Access Manager. "
9	Set the agent password. When Access Manager is installed, a default agent profile called IAMSuiteAgent is created. This profile is used by Oracle Adaptive Access Manager when integrating with Access Manager. When the IAMSuiteAgent profile is first created, it has no password. You must set a password before the profile can be used by Oracle Adaptive Access Manager for integration.	For information, see " Adding an Agent Password to the IAMSuiteAgent Profile. "
10	Update the IAMSuiteAgent.	For information, see " Updating the Domain Agent Definition If Using Domain Agent for IDM Domain Consoles. "

Table 3–5 (Cont.) Integration Flow for Access Manager and Oracle Adaptive Access Manager

Number	Task	Information
11	Verify TAP partner registration using the Oracle Access Management tester.	For information, see "Verifying TAP Partner Registration."
12	Set up TAP integration properties in OAAM.	For information, see "Setting Up Access Manager TAP Integration Properties in OAAM."
13	Configure the integration to use OAAM TAPScheme to protect Identity Management product resources in the IAMSuiteAgent application domain.	For information, see "Configuring the Integration to Use TAPScheme to Protect Identity Management Resources in the IAMSuiteAgent Application Domain."
14	Configure the authentication scheme in the policy-protected resource policy to protect a resource with the OAAM TAPScheme.	For information, see "Configuring a Resource to be Protected with TAPScheme."
15	Validate the Access Manager and Oracle Adaptive Access Manager Integration.	For information, see "Validating the Access Manager and Oracle Adaptive Access Manager Integration."

3.8 Integrating Oracle Identity Manager and Oracle Adaptive Access Manager

This section describes how to integrate Oracle Identity Manager and Oracle Adaptive Access Manager for the three-way integration of Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager:

- [Setting Oracle Identity Manager Properties for Oracle Adaptive Access Manager](#)
- [Updating OAAM Properties to Enable Integration Between Oracle Identity Manager and OAAM](#)
- [Configuring Oracle Identity Manager Credentials in the Credential Store Framework](#)
- [Configuring Cross Domain Trust Between Oracle Identity Manager and Oracle Adaptive Access Manager](#)

3.8.1 Setting Oracle Identity Manager Properties for Oracle Adaptive Access Manager

In Oracle Identity Manager, the `OIM.ChangePasswordURL` and `OIM.ChallengeQuestionModificationURL` properties must be set to valid OAAM URLs, and `OIM.DisableChallengeQuestions` must be set to true for Oracle Adaptive Access Manager to provide the challenge questions functionality instead of Oracle Identity Manager. Follow these steps to set each property.

To modify Oracle Identity Manager properties, take these steps:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Configuration, click **Configuration Properties**.
3. In the left pane of the System Configuration section, click **Advanced Search**.
4. Enter the property name in the Search field.
5. Click the icon next to the Search field.
6. In the search results table, click the property to open the details for the property.
7. Set the property as documented in [Table 3–6](#). Then, click **Save**.

Note: For the URLs, use the host names as they were configured in Access Manager. For example, if a complete host name (with domain name) was provided during Access Manager configuration, use the complete host name for the URLs.

Table 3–6 Oracle Identity Manager Redirection

Properties	Property Name and Value
OIM.DisableChallengeQuestions	TRUE
OIM.ChangePasswordURL	<p>URL for change password page in Oracle Adaptive Access Manager</p> <pre>http://oaam_server_managed_server_host: oaam_server_managed_server_port/ oaam_server/oimChangePassword.jsp</pre> <p>In a high availability (HA) environment, set this property to point to the virtual IP URL for the OAAM server.</p>
OIM.ChallengeQuestionModificationURL	<p>URL for challenge questions modification page in Oracle Adaptive Access Manager</p> <pre>http://oaam_server_managed_server_host: oaam_server_managed_server_port/ oaam_server/oimResetChallengeQuestions.jsp</pre>

8. Restart the Oracle Identity Manager managed server.

3.8.2 Updating OAAM Properties to Enable Integration Between Oracle Identity Manager and OAAM

To set OAAM properties for Oracle Identity Manager:

1. Log in to the OAAM Admin Console:

```
http://oaam_managed_server_host:oaam_admin_managed_server_port/oaam_admin
```

You must log in as a user with access to the Properties Editor.

2. In the navigation tree, click **Environment** and double-click **Properties**. The Properties search page is displayed.
3. To set a property value, enter its name in the **Name** field and click **Search**. The current value is shown in the search results window.
4. Click **Value**. Enter the new value and click **Save**.

Set the following properties according to your deployment:

Table 3–7 Configuring Oracle Identity Manager Property Values

Property Name	Property Values
bharosa.uio.default.user.management.provider.classname	com.bharosa.vcrypt.services.OAAMUserMgmtOIM
oaam.oim.auth.login.config	<code>\${oracle.oaam.home}/../designconsole/config/authwl.conf</code>
oaam.oim.url	<p><code>t3://OIM-Managed-Server:OIM-Managed-Port</code></p> <p>For example: <code>t3://host.mycorp.example.com:14000</code></p>
oaam.oim.xl.homedir	<code>\${oracle.oaam.home}/../designconsole</code>
bharosa.uio.default.signon.links.enum.selfregistration.url	<p>The URL for Self Registrations is as follows:</p> <p><code>http://OIM-Managed-Server-Host:OIM-Managed-Server-Port/identity/faces/register?&backUrl=http://OIM-Managed-Server-Host:OIM-Managed-Server-Port/identity</code></p> <p>Note: If Oracle HTTP Server is configured in front of OIM, then the Oracle HTTP Server host and port should be used in the value instead of the OIM managed server host and port. For example:</p> <p><code>http://OHS-HOST:OHS-PORT/identity/faces/register?&backUrl=http://OHS-HOST:OHS-PORT/identity</code></p>
bharosa.uio.default.signon.links.enum.trackregistration.url	<p>The URL for Track Registrations is as follows:</p> <p><code>http://OIM-Managed-Server-Host:OIM-Managed-Server-Port/identity/faces/trackregistration?&backUrl=http://OIM-Managed-Server-Host:OIM-Managed-Server-Port/identity</code></p> <p>Note: If Oracle HTTP Server is configured in front of OIM, then the Oracle HTTP Server host and port should be used in the value instead of the OIM managed server host and port. For example:</p> <p><code>http://OHS-HOST:OHS-PORT/identity/faces/trackregistration?&backUrl=http://OHS-HOST:OHS-PORT/identity</code></p>
bharosa.uio.default.signon.links.enum.trackregistration.enabled	true
bharosa.uio.default.signon.links.enum.selfregistration.enabled	true

Table 3–7 (Cont.) Configuring Oracle Identity Manager Property Values

Property Name	Property Values
oaam.oim.csf.credentials.enabled	true This property enables the configuring of credentials in the Credential Store Framework as opposed to maintaining them using the Properties Editor. This step is performed so that credentials can be securely stored in CSF.
bharosa.uio.default.singlelogin.links.enum.selfregistration.enabled	Set this property to true to enable the Self Registration link only if Single Login Page mode is enabled. Single Login Page mode, where user name and password inputs are on the same page, is enabled through OAAM customization. For more information about the Single Login Page mode, see "Configuring a Single Login Page" in <i>Developer's Guide for Oracle Adaptive Access Manager</i> .

Table 3–7 (Cont.) Configuring Oracle Identity Manager Property Values

Property Name	Property Values
bharosa.uio.default.singlelogin.links.enum.selfregistration.url	<p>The URL for the Self Registration link if Single Login Page mode is enabled.</p> <p>The URL is as follows:</p> <pre>http://OIM-Managed-Server-Host: OIM-Managed-Server-Port/identity/faces/ register?&backUrl=http://OIM-Managed-Server-Host:OIM-Managed-Server-Port/identity</pre> <p>Note: If Oracle HTTP Server is configured in front of OIM, then the Oracle HTTP Server host and port should be used in the value instead of the OIM managed server host and port. For example:</p> <pre>http://OHS-HOST:OHS-PORT/identity/faces/register?&backUrl=http://OHS-HOST:OHS-PORT/identity</pre>
bharosa.uio.default.singlelogin.links.enum.trackregistration.enabled	<p>Set this property to <code>true</code> to enable the Track Registration link only if Single Login Page mode is enabled.</p> <p>Single Login Page mode, where user name and password inputs are on the same page, is enabled through OAAM customization. For more information about the Single Login Page mode, see "Configuring a Single Login Page" in <i>Developer's Guide for Oracle Adaptive Access Manager</i>.</p>
bharosa.uio.default.singlelogin.links.enum.trackregistration.url	<p>The URL for the Track Registration link if Single Login Page mode is enabled.</p> <p>The URL is as follows:</p> <pre>http://OIM-Managed-Server-Host: OIM-Managed-Server-Port/identity/faces/ trackregistration?&backUrl=http://OIM-Managed-Server-Host:OIM-Managed-Server-Port/identity</pre> <p>Note: If Oracle HTTP Server is configured in front of OIM, then the Oracle HTTP Server host and port should be used in the value instead of the OIM managed server host and port. For example:</p> <pre>http://OHS-HOST:OHS-PORT/identity/faces/trackregistration?&backUrl=http://OHS-HOST:OHS-PORT/identity</pre>

3.8.3 Configuring Oracle Identity Manager Credentials in the Credential Store Framework

Oracle Adaptive Access Manager must have the credentials of an OIM Administrator in order to perform various activities. A key for Oracle Identity Manager WebGate credentials is created in MAP `oaam`. So that the OIM credentials can be securely stored

in the Credential Store Framework, follow the steps below to add a password credential to the OAAM domain.

1. Log in to the Oracle Fusion Middleware Enterprise Manager Console:
`http://weblogic_host:administration_port/em`
You must log in as a WebLogic Administrator. For example, `WebLogic`.
2. Expand the Base Domain in the navigation tree in the left pane.
3. Select your domain name, right-click, and select the menu option **Security** and then the option **Credentials** in the submenu.
4. Click **Create Map**.
5. Click **oaam** to select the map, and then click **Create Key**.
6. In the pop-up dialog, ensure that **Select Map** is **oaam**.
7. Provide the following properties and click **OK**.

Table 3–8 Oracle Identity Manager Credentials

Name	Value
Map Name	oaam
Key Name	oim.credentials
Key Type	Password
UserName	User name of Oracle Identity Manager Administrator For example, <code>xelsysadm</code>
Password	Password of Oracle Identity Manager Administrator

3.8.4 Configuring Cross Domain Trust Between Oracle Identity Manager and Oracle Adaptive Access Manager

You must configure cross domain trust because Oracle Identity Manager and Oracle Adaptive Access Manager are in separate domains.

Configure Cross-Domain Trust in the Oracle Adaptive Access Manager Domain

1. Log in to WebLogic Administration Console of Oracle Adaptive Access Manager.
2. Click the domain and select the **Security** tab.
3. Expand the **Advanced** section.
4. Select **Cross domain security enabled**.
5. Select a shared secret and type it in the **Credential** and **Confirm Credential** fields.
6. Save the configuration changes.

Configure Cross-Domain Trust in the Oracle Identity Manager Domain

1. Log in to WebLogic Administration Console of Oracle Identity Manager.
2. Click the domain and select the **Security** tab.
3. Expand the **Advanced** section.
4. Select **Cross domain security enabled**.
5. Select a shared secret and type it in the **Credential** and **Confirm Credential** fields.

Use the same shared secret you used when you were configuring cross-domain trust in the OAAM domain.

6. Save the configuration changes.

3.9 Performing Additional Configuration Depending on Deployment

Depending on your requirements, you may need to perform tasks in addition to those documented above.

For information related to Access Manager and OAAM integration, refer to [Section C.6, "Other Access Manager and OAAM Integration Configuration Tasks."](#)

3.9.1 Adding the `-Djava.security.auth.login.config` JAVA System Property if Using JDK 7

If the Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager integrated environment uses JDK 7, add the following JAVA system property to the `OAAM_DOMAIN/bin/setDomainEnv.sh` script and restart the OAAM server:

```
-Djava.security.auth.login.config=${ORACLE_HOME}/designconsole/config/authwl.conf
```

3.9.2 Changing the Authentication Scheme to TAPScheme for Upgrade of Oracle Identity Manager

If you have upgraded Oracle Identity Manager or Access Manager in an Access Manager, OAAM, and Oracle Identity Manager integrated environment, change the Authentication Scheme from LDAPScheme to TAPScheme for both Protected HigherLevel and Protected LowerLevel Policies under the IAM Suite domain. To do so:

1. Log in to the Oracle Access Management Console:
`http://oam_adminserver_host:oam_adminserver_port/oamconsole`
2. In the Oracle Access Management Console, click **Application Security** at the top of the window.
3. In the Application Security console, click **Application Domains** in the Access Manager section.
4. In the Search Application Domains page that appears, enter `IAM Suite` in the Name field.
5. Click the **Search** button to initiate the search.
6. Click **IAM Suite** in the Search Results table and click **Edit**.
7. In the IAM Suite Application Domain, click the **Authentication Policies** tab.
8. Click **Protected HigherLevel Policy** to display its configuration.
9. In the Authentication Scheme field, change **LDAP Scheme** to **TAPScheme** and click **Apply**.
10. Navigate to the IAM Suite tab, click the **Authentication Policies** tab.
11. Click **Protected LowerLevel Policy** to display its configuration.
12. In the Authentication Scheme field, change **LDAP Scheme** to **TAPScheme** and click **Apply**.

3.9.3 Changing the Authentication Scheme to TAPScheme After Moving from a Test to a Production Environment

After moving the OIM domain from test to production for an 11g Release 2 (11.1.2.3) Access Manager, Oracle Identity Manager, and OAAM integrated environment where Access Manager and OAAM are in the same domain and Oracle Identity Manager is in another domain, you must:

- Select the TAPScheme as the Authentication Scheme for the Protected HigherLevel Policy under the IAM Suite Application domain.
- Ensure that the Authentication Scheme for the resource `/oamTapAuthenticate` in the IAM Suite Application domain is LDAPScheme.

To use TAPscheme for Identity Management product resources in the IAM Suite domain Protected HigherLevel Policy, the following configuration must be performed:

1. Log in to the Oracle Access Management Console:

```
http://oam_adminserver_host:oam_adminserver_port/oamconsole
```

2. In the Oracle Access Management Console, click **Application Security** at the top of the window.
3. In the Application Security console, click **Application Domains** in the Access Manager section.
4. In the Search Application Domains page that appears, enter `IAM Suite` in the Name field.
5. Click the **Search** button to initiate the search.
6. Click **IAM Suite** in the Search Results table and click **Edit**.
7. In the IAM Suite Application Domain page, click the **Authentication Policies** tab.
8. Click **Protected HigherLevel Policy** to display its configuration.
9. In the Authentication Scheme field, change **LDAP Scheme** to **TAPScheme** and click **Apply**.
10. In the Resources tab, click `/oamTAPAuthenticate` in the Resources table.
11. Click the **Delete** button in the table.
12. Click **Apply** to submit changes and close the confirmation window.

Make sure the Authentication Scheme is LDAPScheme for the resource `/oamTapAuthenticate` (in the IAM Suite Application domain). If the Authentication Scheme is LDAPScheme, no further modification is required.

If the Authentication Scheme is not LDAPScheme, proceed as follows:

1. In the IAM Suite Application Domain page, click the **Authentication Policies** tab, then click the **Create** button to open the Create Authentication Policy page.
2. Enter a unique name in the Name field.
3. For authentication scheme, choose **LDAPScheme**.
4. Click the **Resources** tab.
5. Click the **Add** button in the Resources tab.
6. Click the **Search** button.
7. Click `/oamTAPAuthenticate` in the Results table.

8. Click **Add Selected**.
9. Click **Apply** to save changes and close the confirmation window.

3.10 Troubleshooting Common Problems

This section describes common problems you might encounter in an Access Manager, OAAM, and OIM integrated environment, and explains how to solve them. It contains the following topics:

- [User Encounters a Non-Working URL](#)
- [User is Redirected in a Loop After User Enters Wrong Password](#)
- [User is Redirected to an Oracle Identity Manager Page](#)
- [Successful Authentication Creates Two User Sessions](#)
- [OAAM Test Login URL Fails After Access Manager and OAAM Integration](#)
- [Initialization Error Occurs When the User Resets the User Password](#)

In addition to this section, review the *Oracle Fusion Middleware Error Messages Reference* for information about the error messages you may encounter.

For information about additional troubleshooting resources, see [Section 1.7, "Using My Oracle Support for Additional Troubleshooting Information."](#)

3.10.1 User Encounters a Non-Working URL

You encounter a non-working URL. For example, you click the **Forgot Password** link, but are redirected to the login page.

Cause

Policies and challenge questions are not available as expected in your Oracle Adaptive Access Manager environment.

Solution

Ensure that the default base policies and challenge questions shipped with Oracle Adaptive Access Manager have been imported into your system. For details, see "Setting Up the Oracle Adaptive Access Manager Environment" in the *Administering Oracle Adaptive Access Manager*.

3.10.2 User is Redirected in a Loop After User Enters Wrong Password

A user is redirected in a loop when he enters an incorrect password.

Cause

Value for the login page is incorrect.

Solution

If redirect loops occur when users enter incorrect passwords, then verify that the `oaam.uio.login.page` property is set properly in the OAAM Properties page. The value for the `oaam.uio.login.page` property should be set to `/oaamLoginPage.jsp`. For information on setting properties in Oracle Adaptive Access Manager, see "Using the Properties Editor" in *Administering Oracle Adaptive Access Manager*.

3.10.3 User is Redirected to an Oracle Identity Manager Page

A user is redirected to the OIM forgot password, OIM reset password, or OIM challenge question setup page.

Cause

The authentication scheme for the resource in Access Manager was not configured correctly.

Solution

If two applications point to the same identity store (the same set of users have access to the different applications), the resources protected in Access Manager must have the same authentication and authorization policies for both the applications.

3.10.4 Successful Authentication Creates Two User Sessions

Access Manager creates two concurrent sessions when the user logs in through OAAM and is successfully authenticated through Access Manager.

Cause

In an Access Manager, OAAM, and OIM integrated environment, any authentication results in two user sessions being created in Oracle Access Management Access Manager (visible in Oracle Access Management Console under Session Management, and in the `OAM_SESSIONS` table in MDS).

One session is created by the IAMSuiteAgent and the other session is created by WebGate.

Solution

Check the value of the property `oaam.uio.oam.authenticate.withoutsession`.

3.10.5 OAAM Test Login URL Fails After Access Manager and OAAM Integration

The test login URL `/oaam_server` is used to verify that the OAAM configuration is working before proceeding with the integration of Access Manager. This URL is not intended for use after the integration of Access Manager and OAAM.

3.10.6 Initialization Error Occurs When the User Resets the User Password

An Oracle Identity Manager client initialization error results sometimes when the user clicks the **Reset password** link in an Oracle Identity Manager and OAAM integrated environment. An error similar to the following is logged in the OAAM Server managed server log file `OAAM_DOMAIN/servers/oaam_server/logs`:

```
<Oct 17, 2014 9:04:29 AM PDT> <Error> <oracle.oaam> <BEA-000000> <Error
loading plugin instance for
className=com.bharosa.vcrypt.services.OAAMUserMgmtOIM
java.lang.IllegalArgumentException: No Configuration was registered that can
handle the configuration named xellerate
at com.bea.common.security.jdkutils.JAASConfiguration.getAppConfigurationEntry(JA
ASConfiguration.java:130)
at javax.security.auth.login.LoginContext.init(LoginContext.java:259)
at javax.security.auth.login.LoginContext.<init>(LoginContext.java:425)
at Thor.API.Security.LoginHandler.weblogicLoginHandler.login(weblogicLoginHandler
.java:58)
at oracle.iam.platform.OIMClient.login(OIMClient.java:212)
at oracle.iam.platform.OIMClient.login(OIMClient.java:196)
```

```
at com.bharosa.vcrypt.services.OAAMUserMgmtOIM.init(OAAMUserMgmtOIM.java:415)
at com.bharosa.vcrypt.services.OAAMUserMgmtOIM.<init>(OAAMUserMgmtOIM.java:89)
```

If the error occurs, add the following JAVA system property to the *OAAM_DOMAIN/bin/setDomainEnv.sh* script and restart the OAAM server:

```
-Djava.security.auth.login.config=${ORACLE_HOME}/designconsole/config/authwl.conf
```

Configuring SSL for Integrated IdM Components

After integrating identity management components like Oracle Access Management Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager, you can configure SSL to secure the communication between these components.

This chapter contains these topics:

- [About SSL for Integrated IdM](#)
- [Configuring SSL on Servers in the OAM Domain](#)
- [Configuring SSL for Oracle Identity Manager](#)
- [Configuring SSL on Servers in the OAAM Domain](#)
- [Configuring SSL for Oracle Unified Directory](#)
- [Configuring SSL for Oracle HTTP Server](#)
- [Securing IdM Components against the Poodle Vulnerability](#)
- [Completing SSL Configuration for Integrated IdM](#)

4.1 About SSL for Integrated IdM

You must be aware of certain background information before using the procedures to enable SSL in an IdM environment.

This section contains these topics:

- [Assumptions about Integrated IdM Environment](#)
- [Roadmap for End-to-End IdM SSL](#)

4.1.1 Assumptions about Integrated IdM Environment

This discussion makes certain assumptions which you should take into account before using the procedures here.

The assumptions are as follows:

- You have used the procedures in the following guides to install and scale out your Oracle Identity Manager (OIM), Oracle Oracle Access Manager (OAM), and Oracle Adaptive Access Manager (OAAM) components:
 - *Installation Guide for Oracle Identity and Access Management*
 - *High Availability Guide*

- You are performing these SSL procedures in the context of an integrated IdM environment. This means that you have already used the roadmap in [Table 1–2](#) to integrate OAM, OIM, and OAAM.
- You are using Oracle Unified Directory (OUD) as your identity store. Configuring OUD for the integrated IdM environment is described in applicable chapters of this guide.

4.1.2 Roadmap for End-to-End IdM SSL

[Table 4–1](#) shows the stages in which you implement SSL wiring for integrated IdM components:

Table 4–1 Roadmap for End-to-end IdM SSL

Procedure	Notes
Configure Clustering for Managed Servers	Out of scope of this document. For details about clustering IdM components, see <i>High Availability Guide</i> .
Configure SSL in the Domain Hosting OAM	Section 4.2
Configure SSL in the Domain Hosting OIM	Section 4.3
Configure SSL in the Domain Hosting OAAM	Section 4.4
Configure SSL for OUD	Section 4.5
Configure SSL for Oracle HTTP Server	Section 4.6
Complete SSL Configuration for Integrated IdM	Section 4.8

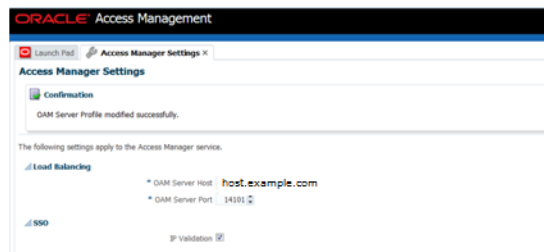
4.2 Configuring SSL on Servers in the OAM Domain

To configure SSL on all the servers residing in the OAM domain:

1. Log in to the WebLogic console, expand Environment, and click Servers.
2. Select the OAM server to configure.
3. In the Settings for *server* page, under the server properties, check the **SSL Listen Port Enabled** box.

Name:	oam_server1
Machine:	host.example.com
Cluster:	(Standalone)
Listen Address:	<input type="text"/>
<input checked="" type="checkbox"/> Listen Port Enabled	
Listen Port:	<input type="text" value="20297"/>
<input checked="" type="checkbox"/> SSL Listen Port Enabled	
SSL Listen Port:	<input type="text" value="14101"/>

4. Click **Save**.
5. Log in to the OAM console.
6. Click the Access Manager Settings tab.
7. Update OAM Server Port to point to the server SSL port which you specified in Step 3. Select the https protocol for OAM Server Protocol.



8. Click **Apply**.
9. Update the secure port in the `oam-config.xml` configuration file as follows:
 - a. Navigate to the folder `OAM_HOME/iam/common/bin` and launch the `wlst` script.
 - b. Connect as administrator.
 - c. Execute the command:

```
updateOIMHostPort(hostName = "oimhost" , port = "4443", secureProtocol = "true")
```

For additional information about configuring SSL in the Oracle Access Manager environment, see *Administrator's Guide for Oracle Access Management*.

4.3 Configuring SSL for Oracle Identity Manager

This section describes the procedure for generating keys, signing and exporting certificates, setting up SSL Configuration for Oracle Identity Manager and for the components with which Oracle Identity Manager interacts, and establishing secure communication between them.

This section includes the following topics:

- [Generating Keys](#)

- [Signing the Certificates](#)
- [Exporting the Certificate](#)
- [Importing the Certificate](#)
- [Enabling SSL for Oracle Identity Manager and SOA Servers](#)

Note:

- Use these procedures to generate certificates for OIM as well as its SOA server. The same custom identity and trust stores are usable for both.
 - [Section 4.3.1](#) through [Section 4.3.4](#) provide example commands that will be used later in the procedure. These are for reference and the sample values are not mandatory; use your own data during configuration.
 - See "Enabling SSL Communication" in the *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about enabling Secure Sockets Layer (SSL) communication for various Segregation of Duties (SoD) purposes.
 - See *Administering Oracle Identity Manager* for additional SSL configuration in the OIM environment.
-

4.3.1 Generating Keys

You can generate private and public certificate pairs by using the keytool command.

The syntax is:

```
$JAVA_HOME/jre/bin/keytool -genkey -alias alias -keyalg algorithm -keysize key-size -dname DN -keypass key-password -keystore keystore-name -storepass keystore-password
```

The following example creates an identity keystore named support.jks:

```
$JAVA_HOME/jre/bin/keytool -genkey  
-alias support  
-keyalg RSA  
-keysize 1024  
-dname "CN=localhost, OU=Identity, O=MyCorp Corporation,C=US"  
-keypass weblogic1  
-keystore support.jks  
-storepass weblogic1
```

When generating the certificate for OIM, in CN attribute specify the machine name where OIM is deployed. Likewise when generating the certificate for SOA, in CN attribute specify the machine name where SOA is deployed. For example:

```
-dname "CN=myhost.us.example.com, OU=Identity, O=Example Corporation,C=US"
```

Note:

- Change the parameter values passed to the `keytool` command according to your requirements. Ensure that there is no line break in the `keytool` arguments.
- If JDK 7u40 or later is used, then the value of the `keysize` option must be greater than or equal to 1024. For more information about this limitation, see "Default x.509 Certificates Have Longer Key Length" at the following URL:

<http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html>

4.3.2 Signing the Certificates

Use the `keytool` command to sign the certificates that you created. In this example, both the certificate and keystore have the same password (`weblogic1`):

```
$JAVA_HOME/jre/bin/keytool -selfcert -alias support
-sialg MD5withRSA -validity 2000 -keypass weblogic1
-keystore support.jks
-storepass weblogic1
```

Note: Change the parameter values passed to the `keytool` command according to your requirements. Ensure that there is no line break in the `keytool` arguments.

4.3.3 Exporting the Certificate

Use the `keytool` command to export the certificate from the identity keystore to a file.

The syntax is:

```
$JAVA_HOME/jre/bin/keytool -export -alias alias -file file-to-export -keypass
key-password -keystore keystore-name -storepass keystore-password
```

For example, the following command exports the certificate to a file named `supportcert.pem`:

```
$JAVA_HOME/jre/bin/keytool -export -alias support
-file supportcert.pem
-keypass weblogic1
-keystore support.jks
-storepass weblogic1
```

Note: Change the parameter values passed to the `keytool` command according to your requirements. Ensure that there is no line break in the `keytool` argument.

4.3.4 Importing the Certificate

Use the `keytool` command to import the certificate from a file.

```
keytool -import -alias alias -trustcacerts -file file-to-import -keystore
keystore-name -storepass keystore-password
```

In this example, the certificate file `supportcert.pem` is imported to the identity keystore `client_store.jks` with password `weblogic1`:

```
keytool -import -alias serverwl -trustcacerts -file supportcert.pem -keystore
client_store.jks -storepass weblogic1
```

Note: Change the parameter values passed to the `keytool` command according to your requirements. Ensure that there is no line break in the `keytool` arguments.

4.3.5 Enabling SSL for Oracle Identity Manager and SOA Servers

The following tasks need to be performed to configure Oracle Identity Manager and SOA servers to operate in SSL mode:

- [Enabling SSL for Oracle Identity Manager](#)
- [Changing Front End URLs using MBeans](#)
- [Changing SOA Server URL to Use SSL Port](#)
- [Configuring SSL for Oracle Identity Manager Utilities](#)

For additional information about configuring SSL in the Oracle Identity Manager environment, see *Administering Oracle Identity Manager*.


4.3.5.1 Enabling SSL for Oracle Identity Manager

You can enable SSL for Oracle Identity Manager by using default keystore settings, or by specifying your own keystore.

Note: See "Generating Keys" in *Administering Oracle Identity Manager* for information about generating custom keys.

To enable SSL for Oracle Identity Manager with a specific keystore:

1. In the WebLogic Server Administration Console, click **Environment, Servers**, and select the OIM server. On the Settings for Server page click the **Configuration** tab, and then **General**.
2. Click **Lock & Edit**.
3. Check the SSL Listen Port Enabled box. The default port is 14001.

Name:	oim_server1
Machine:	(None)
Cluster:	(Standalone)
 Listen Address:	<input type="text"/>
<input checked="" type="checkbox"/> Listen Port Enabled	
Listen Port:	<input type="text" value="15979"/>
<input checked="" type="checkbox"/> SSL Listen Port Enabled	
SSL Listen Port:	<input type="text" value="18866"/>

Click **Save**.

4. Select the Keystores tab.
5. From the Keystores drop-down, select **Custom Identity and Custom Trust**.

Settings for oim_server1


Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services **Keystores** SSL Federation Services Deployment Migration Tuning Overload

Health Monitoring Server Start Web Services

Save Cancel

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

Keystores: 

- Custom Identity and Command Line Trust
- Custom Identity and Custom Trust**
- Custom Identity and Java Standard Trust
- Demo Identity and Demo Trust

Save Cancel

Which configuration rules should be used for finding the server's identity and trust keystores? [More Info...](#)

Click **Save**.

6. Back on the Keystores tab, in the Custom Identity Keystore field, enter the absolute path of custom identity keystore filename. For example:

DOMAIN_HOME/config/fmwconfig/support.jks

Note:

- The keystore created at `DOMAIN_HOME/config/fmwconfig/` by Oracle Identity Manager during installation is `default-keystore.jks`.
 - If you are using a different name for truststore than the default name `default-keystore.jks`, take the following steps:
 1. Add Oracle Identity Manager credential store map key. If you are using any other name, such as `support.jks`, then create a key in the credential store by using Oracle Enterprise Manager.
 2. Change `DirectDB` config in the `oim-Config.xml` file either by exporting/importing this file from MDS or by using Enterprise Manager. If the latter, navigate to `XMLConfig` in Application Defined MBeans section of System Mbean Browser, and then change the SSL parameters, for example:


```
SSLConfig dBTrustStore="support.jks"
```
-
-

7. Specify `JKS` as the custom identity keystore type.
8. Type the password into the Custom Identity Keystore Passphrase and the Confirm Custom Identity Keystore Passphrase fields. This is the same password that you specified for the `-storepass` property when generating keys in [Section 4.3.1](#) (for example, `weblogic1`).
9. In the Custom Trust Keystore field, enter the absolute path of custom trust keystore filename. For example:


```
DOMAIN_HOME/config/fmwconfig/client_store.jks
```
10. Specify `JKS` as the custom trust keystore type.
11. Type the password into the Custom trust Keystore Passphrase and the Confirm Custom Trust Keystore Passphrase fields. In both fields, enter the same password that you specified for the `-storepass` property when importing the certificate in [Section 4.3.4](#) (for example, `weblogic1`).
12. Click **Save**.
13. Click the **SSL** tab.
14. Enter the private key alias. This is the same alias that you specified for the `-alias` property when generating keys in [Section 4.3.1](#).
15. Type the password into the Private Key Passphrase and the Confirm Private Key Passphrase fields. This is the same password that you specified for the `-keypass` property when generating keys in [Section 4.3.1](#) (for example, `weblogic1`).
16. Click **Advanced**.
17. Set Hostname Verification to "None".
18. Click **Save**.

19. Click **Activate changes**.
20. Restart all servers for these changes to take effect.
21. Repeat steps 1 through 20 for the SOA server (soa_server1). OIM server's custom identity and custom trust stores (support.jks and client_store.jks respectively) can play the same role for SOA server as well, so you do not need to regenerate custom identity and custom trust stores for soa_server1. Instead, reuse OIM's custom identity store and custom trust store for SOA.

Note:

- On JDK 7u40 or later, the value of the keysize option must be greater than or equal to 1024. For more information about this limitation, see "Default x.509 Certificates Have Longer Key Length" at the following URL:

<http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html>

After enabling SSL on Oracle Identity Manager and SOA Servers, perform the following changes for establishing secured communication between them:

- [Changing Front End URLs using MBeans](#)
- [Changing SOA Server URL to Use SSL Port](#)

4.3.5.2 Changing Front End URLs using MBeans

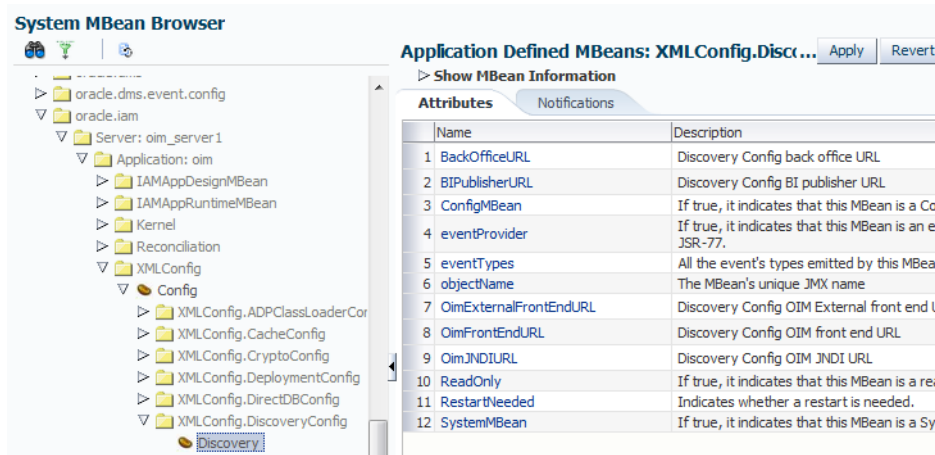
Modify the front end URLs as follows:

1. When the WebLogic admin and Oracle Identity Manager managed servers (at least one server if clustered) are running, log in to Enterprise Manager (EM).

For example:

`http://AdminServer/em`

2. Expand Identity and Access, and under OIM locate the Oracle Identity Manager instance.
3. Right click the instance and select System MBean Browser.
4. Under Application Defined MBeans, navigate to `oracle.iam, Server:oim_servername, Application:oim, XMLConfig, Config, XMLConfig.DiscoveryConfig`, and then `Discovery`.



5. Enter a new value for the "OimFrontEndURL" attribute, providing a non-SSL value, in the format:

`http://OIM-Host:OIM-Non-SSL-Port`

For example:

`http://myoimserver.mydomain.com:14000`

Note: In a clustered deployment, the change to the `OimFrontEndURL` must be made on each server in the cluster.

6. Enter a new value for the "OimExternalFrontEndURL" attribute, providing the protocol as `https` and the OHS `https` port, in the format:

`https://OHS-host-front-ending-OIM:OHS-SSL-Port`

For example:

`https://myoimserver.mydomain.com:4443`

Note: In a clustered deployment, the change to the `OimExternalFrontEndURL` must be made on each server in the cluster.

7. Click **Save** to apply the changes.

4.3.5.3 Changing SOA Server URL to Use SSL Port

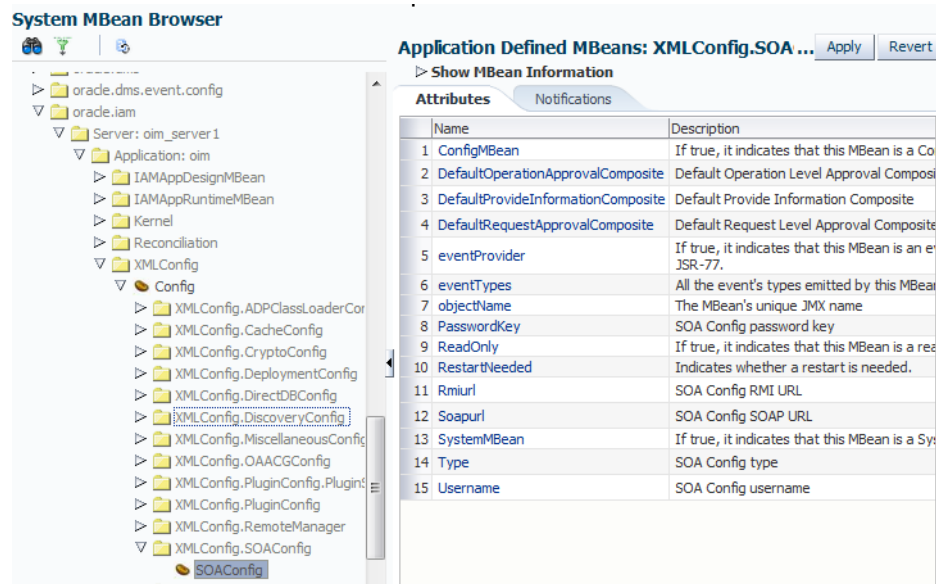
To change SOA server URL to use SSL port:

1. When the admin server and Oracle Identity Manager managed servers are running, log in to Enterprise Manager (EM).

For example:

`http://ADMINISTRATIVE_SERVER/em`

2. Navigate to Identity and Access, Oracle Identity Manager.
3. Right click and select System MBean Browser.
4. Under Application Defined MBeans, navigate to `oracle.iam`, `Application:oim`, `XMLConfig`, `Config`, `XMLConfig.SOAConfig`, `SOAConfig`.



5. Change the values of the `Rmiurl` attribute, providing the `t3s` protocol.

This is the application server URL. For a clustered installation, it is a comma-separated list of all the SOA managed server URLs in the format:

```
t3s://SOA-Host:SOA-SSL-Port
```

For example:

```
t3s://mysoaserver1.mydomain.com:8002
```

```
t3s://mysoa1.mydomain.com:8001,mysoa2.mydomain.com:8002,mysoa3.com:8003
```

Note: `Rmiurl` is used for accessing SOA EJBs deployed on SOA managed servers.

6. Change the value of the `Soapurl` attribute, providing the URL in the format:

```
t3s://SOA-Host:SOA-SSL-Port
```

For example:

```
https://mysoa.mydomain.com: 8001
```

Note: `Soapurl` is used to access SOA web services deployed on SOA managed servers. This is the web server/load balancer URL, in case of a SOA cluster front ended with web server/load balancer. In case of single SOA server, it can be the application server URL.

7. Click **Apply** to save the changes.

4.3.5.4 Configuring SSL for Oracle Identity Manager Utilities

Oracle Identity Manager client utilities include `setDomainEnv.sh` and `startWeblogic.sh`. Under JDK7, SSL configuration requires adding certain Java options to these utilities.

The steps are:

1. Open `DOMAIN_HOME/bin/setDomainEnv.sh` of the OIM domain for editing.
2. After the line `export JAVA_DEBUG`, add the following `JAVA_OPTIONS`:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.security.SSL.protocolVersion=SSL3 "
JAVA_OPTIONS="${JAVA_OPTIONS} -Djavax.net.ssl.trustStore=
Location of OIM trust store
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.SSL.enforceConstraints=off "
```

For example, specify the trust store as:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Djavax.net.ssl.trustStore=/scratch/mydir/client_
store1.jks -Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.SSL.enforceConstraints=off "
```

3. Locate the section:

```
if [ "${debugFlag}" = "true" ] ; then
JAVA_DEBUG="-Xdebug -Xnoagent -Xrunjdw:transport=dt_socket,address=${DEBUG_
PORT},server=y,suspend=n -Djava.compiler=NONE"
export JAVA_DEBUG
```

Below it, add these `JAVA_OPTIONS`:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.security.SSL.protocolVersion=SSL3
-Dssl.debug=true
-Dweblogic.security.TrustKeyStore=DemoTrust "
```

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Djavax.net.ssl.trustStore=
Location of OIM trust store
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.SSL.enforceConstraints=off "
```

For example, specify the trust store as:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Djavax.net.ssl.trustStore=
/scratch/mydir/client_store1.jks
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.SSL.enforceConstraints=off "
```

4. Locate the `EXTRA_JAVA_PROPERTIES`:

```
EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES} -Dsoa.archives.dir=${SOA_
ORACLE_HOME}/soa -Dsoa.oracle.home=${SOA_ORACLE_HOME}
-Dsoa.instance.home=${DOMAIN_HOME}
-Dtangosol.coherence.clusteraddress=227.7.7.12
-Dtangosol.coherence.clusterport=9778 -Dtangosol.coherence.log=jdk
-Djavax.xml.soap.MessageFactory=oracle.j2ee.ws.saaj.soap.MessageFactoryImpl
-Dweblogic.transaction.blocking.commit=true
-Dweblogic.transaction.blocking.rollback=true -Djavax.net.ssl.trustStore=${WL_
HOME}/server/lib/DemoTrust.jks "
```

Remove the reference to `DemoTrust.jks` so modified `EXTRA_JAVA_PROPERTIES` will look like this:

```
EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES} -Dsoa.archives.dir=${SOA_
ORACLE_HOME}/soa -Dsoa.oracle.home=${SOA_ORACLE_HOME}
-Dsoa.instance.home=${DOMAIN_HOME}
-Dtangosol.coherence.clusteraddress=227.7.7.12
-Dtangosol.coherence.clusterport=9778 -Dtangosol.coherence.log=jdk
```

```
-Djavax.xml.soap.MessageFactory=oracle.j2ee.ws.saa.j.soap.MessageFactoryImpl
-Dweblogic.transaction.blocking.commit=true
-Dweblogic.transaction.blocking.rollback=true"
```

5. Save and close `setDomainEnv.sh`.
6. Open the file `DOMAIN_HOME/bin/startWebLogic.sh` for editing. Change `JAVA_OPTIONS` from:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dlaunch.main.class=${SERVER_CLASS}
-Dlaunch.class.path="${CLASSPATH} "
-Dlaunch.complete=weblogic.store.internal.LockManagerImpl -cp ${WL_
HOME}/server/lib/pcl2.jar
```

to:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dlaunch.main.class=${SERVER_CLASS}
-Dlaunch.class.path="${CLASSPATH} "
-Dlaunch.complete=weblogic.store.internal.LockManagerImpl -cp ${WL_
HOME}/server/lib/pcl2.jar -Djavax.net.ssl.trustStore=location of trust store
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.SSL.enforceConstraints=off"
```

For example:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dlaunch.main.class=${SERVER_CLASS}
-Dlaunch.class.path="${CLASSPATH} "
-Dlaunch.complete=weblogic.store.internal.LockManagerImpl -cp ${WL_
HOME}/server/lib/pcl2.jar -Djavax.net.ssl.trustStore=/scratch/myhost/client_
store.jks -Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.SSL.enforceConstraints=off"
```

7. Save and close `startWebLogic.sh`.

Caution: These utility files are overwritten every time the domain is updated (for example after WebLogic upgrade, after running `config oim`, offline upgrade, and so on), so you must repeat this procedure after every update.

For additional details about configuring SSL in the Oracle Identity Manager environment, see *Administering Oracle Identity Manager*.

4.4 Configuring SSL on Servers in the OAAM Domain

OAAM shares a domain with Access Manager, so we can also refer to this domain as the OAM-OAAM domain. SSL must be configured in this domain for both the OAAM server and the admin server for OAAM.

The steps are as follows:

1. Log in to WebLogic Server console.
2. Click Servers, and select the OAAM admin server.
3. Check the option "SSL Listen Port Enabled" and provide the SSL Listen port.
4. Repeat these steps for the OAAM server.

4.5 Configuring SSL for Oracle Unified Directory

You can configure Oracle Unified Directory to accept SSL-based connections using a self-signed certificate.

When using this procedure, note that:

- Using a self-signed certificate is not recommended for production purposes. To install a certificate for production purposes, see "Configuring Key Manager Providers" in *Administering Oracle Unified Directory*.
- This procedure is required *only* if the SSL and StartTLS settings were not specified during installation, or if you want to change those settings.

This procedure assumes the following:

- Oracle Unified Directory is installed on the system on which you are working.
 - The Java `keytool` utility is in your path. If not, either add it to your path or provide the complete path to it when invoking the commands. The `keytool` utility is provided with the Java Runtime Environment (JRE).
 - The administration connector is listening on the default port (4444) and the `dsconfig` command is accessing the server running on the local host. If this is not the case, the `--port` and `--hostname` options must be specified in that command.
1. Generate a private key for the certificate, using the `keytool` command with the `-genkeypair` option.

For example:

```
$ keytool -genkeypair -alias server-cert -keyalg rsa \
  -dname "CN=myhost.example.com,O=Example Company,C=US" \
  -keystore config/keystore -storetype JKS
```

- `-alias alias`. Specifies the name used to refer to the certificate in the keystore. The default name used by the server is `server-cert`.
- `-keyalg algorithm`. Specifies the algorithm used to generate the private key. This is usually `rsa`.
- `-dname subject`. Specifies the subject to use for the certificate.

Change the value of the `-dname` argument so that it is suitable for your environment:

The value of the `CN` attribute should be the fully-qualified name of the system on which the certificate is being installed.

The value of the `O` attribute should be the name of your company or organization.

The value of the `C` attribute should be the two-character abbreviation for your country.

- `-keystore path`. Specifies the path to the keystore file. The file will be created if it does not already exist.

The default keystore path used by the server is `config/keystore`. This `config` folder exists where your OUD middleware is installed, and the path to the `config` folder is structured as:

```
/Middleware/oud_instance_name/OUd/config
```

For example:

```
/scratch/mytest/OU DR2PS2/Oracle/Middleware/asinst_1/OU D/config
```

- `-keypass password`. Specifies the password used to protect the private key in the keystore. If the password is not provided, you will be prompted for it.
- `-storepass password`. Specifies the password used to protect the contents of the keystore. If the password is not provided, you will be prompted for it.
- `-storetype type`. Specifies the keystore type. For the JKS keystore, for example, the value should always be JKS.

You are prompted for a password to protect the contents of the keystore and for a password to protect the private key.

2. Generate a self-signed certificate for the key.

For example:

```
$ keytool -selfcert -alias server-cert -validity 1825 \
-keystore config/keystore -storetype JKS
```

- `-alias alias`. Specifies the name used to refer to the certificate in the keystore. This name should be the same as the value used when creating the private key with the `-genkeypair` option.
- `-validity days`. Specifies the length of time in days that the certificate should be valid. The default validity is 90 days.
- `-keystore path`. Specifies the path to the keystore file. The file will be created if it does not already exist.
- `-keypass password`. Specifies the password used to protect the private key in the keystore. If this is not provided, then you will be interactively prompted for it.
- `-storepass password`. Specifies the password used to protect the contents of the keystore. If this is not provided, then you will be interactively prompted for it.
- `-storetype type`. Specifies the keystore type. For the JKS keystore, the value should always be JKS.

When you are prompted for the keystore password and private key password, enter the same passwords that you provided in the previous step.

3. Create a text file named `config/keystore.pin`.

The file must contain the password that you chose to protect the contents of the keystore. If you change this file, remember that it must match the keystore manager configuration. If you decide to create a file with a different name, for example, the corresponding keystore manager's `key-store-file` property for JKS must match the path and file name.

4. Export the public key for the certificate that you created.

For example:

```
$ keytool -exportcert -alias server-cert -file config/server-cert.txt -rfc \
-keystore config/keystore -storetype JKS
```

5. Create a new trust store and import the server certificate into that trust store.

For example:

```
$ keytool -importcert -alias server-cert -file config/server-cert.txt \
```

```
-keystore config/truststore -storetype JKS
```

6. Use the `dsconfig` utility to enable the key manager provider, trust manager provider, and connection handler. `dsconfig` is present in the `bin` directory of OUD's installed path (a typical path looks like `/asinst_1/OUd/bin`). You must supply the OUD admin port and the OUD server hostname as well.

For example:

```
./dsconfig -D "cn=directory manager" -j pwd.txt -X -n
\set-key-manager-provider-prop --provider-name JKS --set enabled:true --port
1111 --hostname myhost.us.example.com
```

```
./dsconfig -D "cn=directory manager" -j pwd.txt -X -n
\set-trust-manager-provider-prop --provider-name "Blind Trust" \--set
enabled:true --port 1111 --hostname myhost.us.example.com
```

```
./dsconfig -D "cn=directory manager" -j pwd.txt -X -n
\set-connection-handler-prop --handler-name "LDAPS Connection Handler" \--set
"trust-manager-provider:Blind Trust" --set key-manager-provider:JKS \--set
listen-port:1636 --set enabled:true --port 1111 --hostname
myhost.us.example.com
```

For `-set listen-port` provide any port number which is not in use; Port 1636 is the standard LDAPS port, but you cannot use this port if it is already taken.

- a. If you have specified a different value for `-keypass` and `-storepass` when generating the private key in step 1, you must provide the key password using `dsconfig`:

```
$ dsconfig -D "cn=directory manager" -j pwd-file -X -n \
create-key-manager-provider-key-pin --provider-name JKS --set
key-pin-file:<file with key password> --type generic --pin-name server-cert
```

For the name of the key pin, provide the same name as the alias of the certificate. This identifies which key pin/password is associated with each certificate in the key manager provider.

- b. In step 3, if you created a text file with a location and name other than `config/keystore.pin`, for example a text file called `config/mykeystore.pin`, specify that information as follows:

```
$ dsconfig -D "cn=directory manager" -j pwd-file -X -n \
set-key-manager-provider-prop --provider-name JKS --set enabled:true \
--set keystore-pin-file:/config/mykeystore.pin
```

7. The server now has a second listener that accepts SSL-based client connections. Test the configuration with the `ldapsearch` command, for example:

```
$ ldapsearch --port 1636 --useSSL --baseDN "" --searchScope base
"(objectClass=*)"
```

You are prompted to trust the server's certificate. On typing `yes`, the root DSE entry should be returned.

For detailed information about keystores and truststores for OUD, see "Configuring Key Manager Providers" and "Configuring Trust Manager Providers", respectively in *Administering Oracle Unified Directory*.

4.6 Configuring SSL for Oracle HTTP Server

You configure SSL for Oracle HTTP Server (OHS) manually by updating the `opmn.xml` file.

Perform the following steps to enable SSL manually:

1. Open `opmn.xml` in a text editor.
2. In the `<ias-component id="HTTP_Server">` entry, change the start mode from "ssl-disabled" to "ssl-enabled". After modification, the entry should look as follows:

```
<data id="start-mode" value="ssl-enabled"/>
```

3. Save and close `opmn.xml`.
4. Reload OPMN using the following command:

```
opmnctl reload
```

5. Stop Oracle HTTP Server using the following command:

```
Linux: ORACLE_HOME/opmn/bin> opmnctl [verbose] stopproc
ias-component=HTTP_Server
```

```
Windows: ORACLE_HOME\opmn\bin> opmnctl [verbose] stopproc
ias-component=HTTP_Server
```

6. Start Oracle HTTP Server using the following command:

```
Linux: ORACLE_HOME/opmn/bin> opmnctl [verbose] startproc
ias-component=HTTP_Server
```

```
Windows: ORACLE_HOME\opmn\bin> opmnctl [verbose] startproc
ias-component=HTTP_Server
```

7. You can verify if SSL was enabled successfully by navigating to the SSL port, for example:

```
HTTPS://hostname:4443
```

4.7 Securing IdM Components against the Poodle Vulnerability

It is recommended that you use the TLSv1 protocol due to the security vulnerability affecting SSL v3.0 (Padding Oracle On Downgraded Legacy Encryption, or "Poodle"). In Release 11.1.2.3.0, which relies on WebLogic Server 10.3.6 or higher, configuring the entire domain to use JSSE SSL is recommended.

The following topics provide details:

- [Configuring OAM and OIM Domains with the TLSv1 Protocol](#)
- [Configuring OUD with the TLSv1 Protocol](#)
- [Configuring OHS with the TLSv1 Protocol](#)

4.7.1 Configuring OAM and OIM Domains with the TLSv1 Protocol

Configure your OAM and OIM domains as follows:

1. Open the (OAM or OIM) domain's `setDomainEnv.sh` for editing.
2. Enable JSSE SSL by adding the following Java option:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.ssl.JSSEEnabled=true "
```

3. Enable TLSv1 by adding the following two Java options:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.security.SSL.protocolVersion=TLS1 "
```

and:

```
JAVA_OPTIONS="${JAVA_OPTIONS}
-Dweblogic.security.SSL.minimumProtocolVersion=TLSv1.0 "
```

4. Disable the SSLv3 protocol by removing or commenting out the Java option:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.security.SSL.protocolVersion=SSL3 "
```

5. In the OIM domain, locate the section:

```
if [ "${debugFlag}" = "true" ] ; then
JAVA_DEBUG="-Xdebug -Xnoagent -Xrunjdp:transport=dt_socket,address=${DEBUG_
PORT},server=y,suspend=n -Djava.compiler=NONE"
export JAVA_DEBUG
```

Following `export JAVA_DEBUG`, add the Java option:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.security.SSL.protocolVersion=TLS1
-Dssl.debug=true -Dweblogic.security.TrustKeyStore=DemoTrust "
```

6. Restart all servers in each OAM and OIM domain.

For additional information about protecting components in Oracle Identity Manager from this vulnerability, follow the instructions in support alert Doc ID 1944350.1 *CVE-2014-3566 - Instructions to Mitigate the SSL v3.0 Vulnerability (aka "Poodle Attack") in Oracle Identity Manager* at:

<https://support.oracle.com>

4.7.2 Configuring OUD with the TLSv1 Protocol

To enable TLSv1 on OUD, follow the instructions in support alert Doc ID 1950331.1 *CVE-2014-3566 Instructions to Mitigate the SSL v3.0 Vulnerability (aka "Poodle Attack") in Oracle Unified Directory* at:

<https://support.oracle.com>

If you are using Java 7, refer to the section "OUD with Java 7". If using Java 6, refer to the section "OUD with Java 6".

4.7.3 Configuring OHS with the TLSv1 Protocol

To enable TLSv1 on OHS 11g, follow the instructions in support alert Doc ID 1936300.1 *How to Change SSL Protocols (to Disable SSL 2.0/3.0) in Oracle Fusion Middleware Products* at:

<https://support.oracle.com>

Refer to the section "Oracle HTTP Server (OHS) 11g".

4.8 Completing SSL Configuration for Integrated IdM

Certain additional tasks are required to complete SSL wiring for the integrated components.

The steps are as follows:

1. Export the OUD server certificate to a file using `keytool export`. For example, his command saves the OUD certificate in a file named `ldapcert.pem`:

```
keytool -export -alias server-cert -file ldapcert.pem -keystore weblogic1
-keystore keystore -storepass weblogic1
```

2. To ensure the OUD server is trusted, import the OUD certificate from Step 2 into OAM's Java keystore using the `keytool import` command:

```
keytool -import -alias alias -file certificate_file -keystore cacerts_file
```

For example:

```
keytool -import -alias trust -file /scratch/jre/bin/ldapcert.pem
-keystore /scratch/jre/lib/security/cacerts
```

3. When prompted, enter the password as `changeit`.
4. Ensure that the OAM user identity store points to OUD's SSL port, as follows:
 - a. Log in to the OAM console.
 - b. Edit `userIdentityStore`.
 - c. Check the "Enable SSL" option.
 - d. In the Location text box, specify OUD's SSL port.
 - e. Save your changes.
5. To ensure that clients access the OAM, OIM, and OAAM servers using the OHS host and SSL port, take these steps:
 - a. Login to the OAM WebLogic Server console.
 - b. Navigate to **Servers**, then **AdminServer**, then **Configuration**, then **General**, then **Advanced**.
 - c. Enable "WebLogic Plug-In Enabled".
 - d. Repeat these steps for all servers in OAM and OIM domains.
6. To configure logout from the OAM, OIM, and OAAM servers:
 - a. Log in to the OAM console.
 - b. Open the profile for the version 11g agent which was registered through `idmConfigTool configOAM` (see [Section D.4.4](#) for command details).
This profile is named `webgateName_11g`, for example `testwebgate_11g`.
 - c. As originally configured, the Logout Redirect URL has the format:

```
http://host_name:14100/oam/server/logout
```

Modify the URL to specify the `https` protocol and the managed server SSL port. It should look like this:

```
https://host_name:14101/oam/server/logout
```
7. Update these OAAM properties to specify the `https` protocol and the SSL port of OHS:

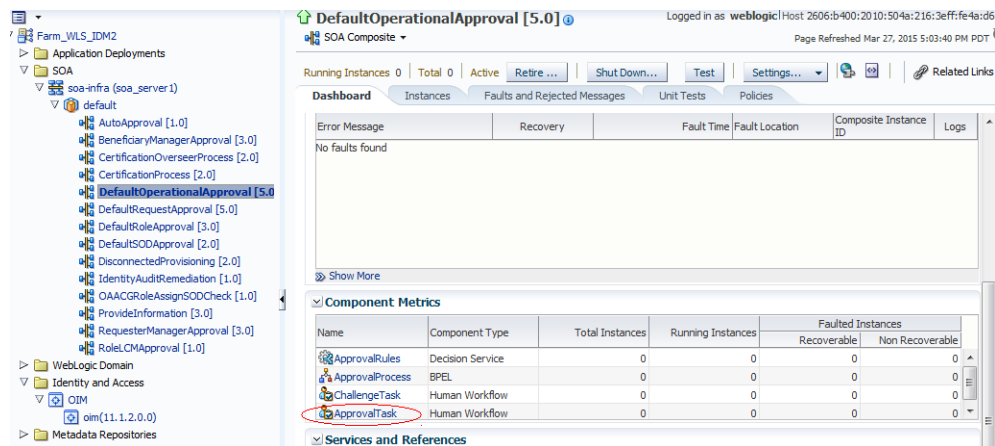
```
bharosa.uio.default.signon.links.enum.selfregistration.url
bharosa.uio.default.signon.links.enum.trackregistration.url
```

- To ensure that resources protected by Tapscheme are redirected to the OAM managed server's SSL port, update the following section of the OAM configuration file `oam-config.xml`:

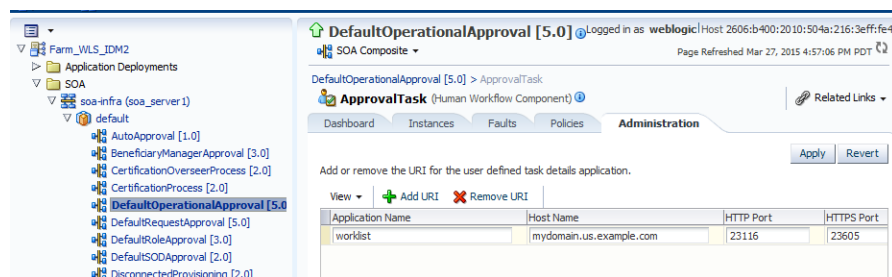
```
<Setting Name="HOST_ALIAS_1" Type="htf:map">
  <Setting Name="serverhost" Type="xsd:string">example.us.com</Setting>
  <Setting Name="serverprotocol" Type="xsd:string">https</Setting>
  <Setting Name="serverport" Type="xsd:string">14301</Setting>
</Setting>
```

Note that `serverprotocol` is `https` and `serverport` is the SSL port of OAM's managed server.

- Restart all servers in the OAM and OAMM domains.
- Log in to the OIM domain's EM console.
- Expand Application Deployments, then SOA.
- Click `DefaultOperationalApproval`.
- In the detail pane, click the `Dashboard` tab, and locate `ApprovalTask`.



- Click the `Administration` tab and provide the value for the `https` port of OHS.



- Click **Apply** to save the change.
- Repeat Steps 12 through 15 for the SOAComposite's `DefaultRequestApproval`, again supplying the `https` OHS port.
- Restart OIM servers.

Integrating Oracle Mobile Security Suite and Oracle Identity Manager

This chapter explains how to integrate Oracle Mobile Security Suite (OMSS) with Oracle Identity Manager. Oracle Mobile Security Suite gives an organization the necessary controls to streamline management of mobile devices and access to business applications from mobile devices. By integrating Oracle Mobile Security Suite with Oracle Access Management Access Manager and Oracle Identity Manager organizations will inherit a rationalized platform through which they can securely manage access to business applications and mobile devices.

For instructions about how to install the components described in this example integration, see *Installation Guide for Oracle Identity and Access Management* and *Installing Oracle Mobile Security Access Server*.

For instructions on integrating Oracle Identity Manager and Access Manager, see [Chapter 2, "Integrating Access Manager and Oracle Identity Manager."](#)

This chapter contains the following topics:

- [About the Oracle Mobile Security Suite and Oracle Identity Manager Integration](#)
- [Oracle Mobile Security Suite and Oracle Identity Manager Integrated Architecture](#)
- [Integrating Oracle Mobile Security Suite and Oracle Identity Manager](#)
- [Configuring Administrators for Oracle Identity Manager and Mobile Security Suite Administration](#)
- [Integrating Oracle Mobile Security Suite in Upgrade Scenarios](#)
- [Viewing Oracle Mobile Security Manager Console Pages in the Oracle Identity Manager Console](#)

5.1 About the Oracle Mobile Security Suite and Oracle Identity Manager Integration

Setting up Oracle Identity Manager and Oracle Mobile Security Suite enables you to manage identities with Oracle Identity Manager and access corporate applications and data with Access Manager. Oracle Identity Manager is a user provisioning and administration solution that automates user account management and Access Manager provides a centralized and automated single sign-on (SSO) solution to corporate applications. Oracle Mobile Security Suite enables the system to securely provide access to enterprise data on mobile devices. It enables business users by giving them secure access to enterprise applications and data from mobile devices.

5.2 Oracle Mobile Security Suite and Oracle Identity Manager Integrated Architecture

This section briefly covers the architecture for Oracle Mobile Security Suite integrated with Oracle Identity Manager.

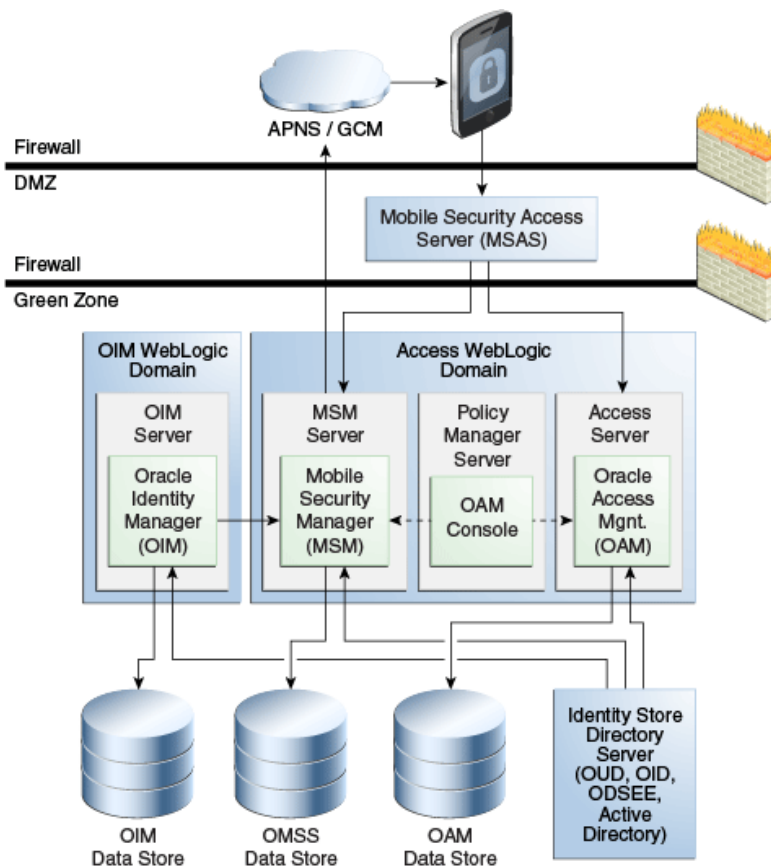
Oracle Mobile Security Manager and Oracle Access Management are deployed together in a WebLogic domain. When Oracle Identity Manager is integrated with Oracle Mobile Security Suite, Oracle Identity Manager is deployed in a separate Oracle Identity Manager WebLogic domain.

Oracle Mobile Security Suite and Oracle Identity Manager are configured to use a common Identity Store. Access Manager uses a user identity store pointing to the same directory as Oracle Mobile Security Suite and Oracle Identity Manager. All applications are based on the same user population.

The Mobile Security Manager user interface (console) pages are rendered within the Oracle Identity Manager interface by using the Oracle Mobile Security Suite shared library, which is deployed on the Oracle Identity Manager server and acts as a Representation State Transfer (REST) client to the Mobile Security Manager server. Users can manage their Oracle Mobile Security Suite accounts from Oracle Identity Manager. Oracle Identity Manager persists its data in the Oracle Identity Manager data store.

Figure 5–1 shows Oracle Identity Manager integrated with Oracle Mobile Security Suite.

Figure 5–1 Logical Diagram Showing Oracle Identity Manager integrated with Oracle Mobile Security Suite



5.3 Integrating Oracle Mobile Security Suite and Oracle Identity Manager

Oracle Mobile Security Suite (including the OAM server) can also be integrated with Oracle Identity Manager 11.1.2.3. Customers can use the OIM Admin Console to manage mobile devices, policies and apps. Self-service users can use the OIM self-service console to manage mobile devices and Workspaces, in addition to managing their user profiles and accounts.

This section provides step-by-step instructions for integrating Mobile Security Suite and Oracle Identity Manager. It contains the following topics:

- [Oracle Mobile Security Suite and Oracle Identity Manager Integration Roadmap](#)
- [Oracle Mobile Security Suite and Oracle Identity Manager Integration Prerequisites](#)
- [Setting Up Trust Between Oracle Mobile Security Suite and Oracle Identity Manager Domains](#)
- [Wiring Oracle Mobile Security Manager and Oracle Identity Manager](#)

5.3.1 Oracle Mobile Security Suite and Oracle Identity Manager Integration Roadmap

[Table 5–1](#) lists the high-level tasks for setting up Oracle Mobile Security Suite with Oracle Identity Manager.

Table 5–1 Setting Up Oracle Mobile Security Suite with Identity Manager

No.	Task	Information
1.	Verify that all required components have been installed and configured prior to integration.	For more information, see Section 5.3.2, "Oracle Mobile Security Suite and Oracle Identity Manager Integration Prerequisites."
2.	Set up trust between Oracle Mobile Security Suite and Oracle Identity Manager domains.	For information, see Section 5.3.3, "Setting Up Trust Between Oracle Mobile Security Suite and Oracle Identity Manager Domains."
3.	Perform Oracle Mobile Security Manager wiring with Oracle Identity Manager.	For information, see Section 5.3.4, "Wiring Oracle Mobile Security Manager and Oracle Identity Manager."
4.	Configure Administrators for Oracle Identity Manager and Oracle Mobile Security Suite administration.	For information, see Section 5.4, "Configuring Administrators for Oracle Identity Manager and Mobile Security Suite Administration."

If you are upgrading an Oracle Identity Manager and Access Manager integrated environment to 11.1.2.3 and want to integrate Oracle Mobile Security Suite, you must perform additional steps prior to the main integration tasks as documented in ["Integrating Oracle Mobile Security Suite During an Upgrade of an Oracle Identity Manager and Access Manager Integrated Environment."](#)

5.3.2 Oracle Mobile Security Suite and Oracle Identity Manager Integration Prerequisites

Before you start integrating Oracle Mobile Security Suite with Oracle Identity Manager, ensure you have installed the required components and necessary dependencies and set up the prerequisite environment.

[Table 5–2](#) lists the required components and prerequisite environment.

Table 5–2 Required Components and Environment Configurations

Component/Requirement	Information
Oracle Mobile Security Manager, Access Manager, and Oracle Identity Manager schemas	<p>The appropriate schemas were created for Oracle Mobile Security Manager, Access Manager, and Oracle Identity Manager. The schemas reside in the same database or different databases.</p> <p>Oracle Mobile Security Manager and Oracle Identity Manager must have different schemas.</p> <p>For more information, see "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)" in <i>Installation Guide for Oracle Identity and Access Management</i>.</p>
Oracle Access Management and Oracle Mobile Security Manager	<p>Oracle Access Management and Oracle Mobile Security Manager were configured in the same WebLogic domain when you ran the Oracle Fusion Middleware Configuration Wizard.</p> <p>The IDM Configuration Tool (<code>idmConfigtool</code>) was run to configure Access Manager to support Oracle Mobile Security Suite.</p> <p>For more information on Oracle Mobile Security Manager configuration with Oracle Access Manager, see "Configuring Oracle Mobile Security Suite" in <i>Installation Guide for Oracle Identity and Access Management</i>.</p> <p>When you configured the domain, Access Manager was configured with the database policy store.</p>
Oracle Mobile Security Access Server	<p>The Oracle Mobile Security Access Server software was installed and wired with Oracle Mobile Security Manager. For information the installation of Oracle Mobile Security Access Server, refer to <i>Installing Oracle Mobile Security Access Server</i>.</p>
Oracle Identity Manager	<p>Oracle Identity Manager was installed and integrated with Access Manager. For information on the configuration of Oracle Identity Manager, see "Configuring Oracle Identity Manager" in <i>Installation Guide for Oracle Identity and Access Management</i>. For information about the integration of Access Manager and Oracle Identity Manager, see Chapter 2, "Integrating Access Manager and Oracle Identity Manager."</p> <p>Note: LDAP synchronization must already be configured.</p>
Oracle Unified Directory, Active Directory, or Oracle Internet Directory	<p>Oracle Identity Manager, Access Manager and Oracle Mobile Security Suite point to the same LDAP directory.</p> <p>Access Manager, Oracle Mobile Security Suite, and Oracle Identity Manager must have been configured against the same identity store so that all applications are based on the same user population.</p>
Data Sources	<p>Oracle Identity Manager, Access Manager, and Oracle Mobile Security Suite must use different data sources.</p>

5.3.3 Setting Up Trust Between Oracle Mobile Security Suite and Oracle Identity Manager Domains

Oracle Identity Manager will make remote ReST calls to the Oracle Mobile Security Manager server for accessing data. In order to have secure exchange, trust has to be established between Oracle Mobile Security Manager and Oracle Identity Manager servers.

To set up trust between the Oracle Mobile Security Suite and Oracle Identity Manager domains, perform the following steps:

Establish Signer Trust

1. Export the default signing certificate `xell.crt` in `default-keystore.jks` from the Oracle Identity Manager domain. In Oracle Identity Manager, `default-keystore.jks` is located in the `$DOMAIN_HOME/config/fmwconfig/` directory.

```
keytool -keystore default-keystore.jks -storepass oim-keystore-password
-exportcert -alias xell -file xell.crt
```

`oim-keystore-password` is entered when you configure Oracle Identity Manager using the Oracle Identity Manager Configuration Wizard.

2. Obtain the Oracle Web Services Manager (OWSM) password from the JPS Credential Store. Perform the following steps in the Oracle Mobile Security Manager domain:

- a. Log in to Oracle Enterprise Manager Fusion Middleware Control at

```
http://weblogic_host:port/em
```

- b. From the target navigation pane, expand **WebLogic Domain** and select the `base_domain`.
- c. On right side of the Fusion Middleware Control navigation panel, click the **Weblogic Domain** menu and select **System MBean Browser**.
- d. Using the System MBean Browser, search for **JpsCredentialStore**.
- e. Click the Operation tab shown in the details pane, and then, click **getPortableCredential**.

For **P1**, enter: `oracle.wsm.security`

For **P2**, enter: `keystore-csf-key`

- f. Click the **Invoke** button.

The Return Value table is displayed below the Parameters table. The `owsm-password` (the password for the JPS keystore of the domain-`default-keystore.jks`) is displayed in the password field.

Once `owsm-password` is retrieved, use it to load `xell.crt` in the keystore.

3. Import signing certificate `xell.crt` in `default-keystore.jks` of the Oracle Mobile Security Suite domain.

```
keytool -keystore default-keystore.jks -storepass owsm-password -importcert
-alias xell -file xell.crt
```

Establish SSL Trust

Note: These steps are optional. This configuration should be done only when communication is over SSL (HTTPS port of Mobile Security Manager server).

1. Export the Oracle Mobile Security Manager CA certificate from the Oracle Mobile Security Manager trust store. The trust store is located in `$DOMAIN_HOME/config/fmwconfig/wlstrust.jks`.

```
keytool -keystore wlstrust.jks -storepass msm-keystore-pass -exportCert -file
```

```
selfsigned.crt -alias cacert
```

msm-keystore-pass is an input in `idmConfigTool -configOMSS -> "OMSS_KEystore_PASSWORD"`.

2. Import the Oracle Mobile Security Manager CA certificate into the Oracle Identity Manager Server trust store.

```
keytool -keystore DemoTrust.jks -storepass DemoTrustKeyStorePassPhrase
-importcert -file selfsigned.crt -alias msmca
```

If the Oracle Identity Manager server is configured against a custom trust store, Oracle Mobile Security Manager's CA certificate should be imported there. If the server uses a default trust store, then this certificate should be imported into `DemoTrust.jks`. The `DemoTrust.jks` file is located in `$WL_HOME/server/lib/DemoTrust.jks`.

Oracle Mobile Security Manager's CA certificate is stored in `$DOMAIN_HOME/config/fmwconfig/server-identity.jks` against alias "ca". The password to access this keystore is provided when you run the `idmConfigTool -configOMSS` command.

5.3.4 Wiring Oracle Mobile Security Manager and Oracle Identity Manager

If you have upgraded Oracle Identity Manager to 11.1.2.3 and want to use the WebLogic Scripting Tool instead of the `idmConfigTool` command to perform wiring, see ["Wiring Oracle Mobile Security Manager and Oracle Identity Manager if Oracle Identity Manager is Upgraded."](#)

To perform wiring of Oracle Mobile Security Suite and Oracle Identity Manager using the `idmConfigTool`, proceed as follows:

Note: Skip this step if you ran the `idmConfigTool -configOIM` command with the `OIM_MSM_REST_SERVER_URL` parameter during Access Manager and Oracle Identity Manager integration. Oracle Mobile Security Suite and Oracle Identity Manager are already wired if you performed this step. For details, see [Section 2.5, "Integrating Access Manager with Oracle Identity Manager."](#)

1. Create a properties file called `config_omss.prop`. This file will be used to seed the Oracle Mobile Security Manager server URL in Oracle Identity Manager and set the system property `OMSS_Enabled` when you run the `idmConfigTool -configOIM` command with the properties file.
2. Add the following properties to the `config_omss.prop` file.

```
OIM_MSM_REST_SERVER_URL:https://msm_server_host:msm_server_port/
WLSPASSWD:WebLogic-Server-administrator-password
```

or

```
OIM_MSM_REST_SERVER_URL:http://msm_server_host:msm_server_port/
WLSPASSWD:WebLogic-Server-administrator-password
```

The `OIM_MSM_REST_SERVER_URL` parameter is used to enable the Oracle Mobile Security Manager task flows in the Oracle Identity Manager Console.

3. Ensure that the Oracle Identity Manager Managed Server is up and running.

For information on starting the managed server, see "Starting or Stopping the Oracle Stack" in *Installation Guide for Oracle Identity and Access Management*.

4. Set the environment variables required for the `idmconfigtool` command. For information on setting environment variables, see [Section D.2, "Set Up Environment Variables."](#)
5. Change the directory to the `IAM_ORACLE_HOME/idmtools/bin` directory:

```
cd IAM_ORACLE_HOME/idmtools/bin
```

You will be running the `idmConfigTool` command from the `IAM_ORACLE_HOME/idmtools/bin` directory.

6. Enable Oracle Mobile Security Manager task flows by running the `idmConfigTool -configOIM` command:

```
idmConfigTool.sh -configOIM input_file=inputpropfile log_level=FINEST log_
file=logfilename
```

For example:

```
idmConfigTool.sh -configOIM input_file=config_omss.prop log_level=FINEST log_
file=omss_log
```

For information on the `configOIM` command option, see [Section D.4.5, "configOIM Command."](#)

7. Restart the Oracle Identity Manager Managed Server.

The Oracle Identity Manager managed server must be restarted for the OMSS Enabled property to take effect.

For information on starting and stopping the managed server, see "Starting or Stopping the Oracle Stack" in *Installation Guide for Oracle Identity and Access Management*.

5.4 Configuring Administrators for Oracle Identity Manager and Mobile Security Suite Administration

In an Oracle Identity Manager and Oracle Mobile Security Suite integrated environment, you can configure Administrators who can act as both Oracle Identity Manager and Oracle Mobile Security Suite Administrators in the following ways:

- Configure Oracle Mobile Security Suite Administrator and Help Desk User in Oracle Identity Manager
- Grant Oracle Identity Manager Administrator privileges to an Access Manager Administrator

Note: If you have upgraded Oracle Identity Manager to 11.1.2.3, you must perform additional steps in the 11.1.2.3 Oracle Identity Manager Console for the Administration Role tab to be available for configuring Administrators. For more information, see ["Configuring Administrators for Oracle Identity Manager and Mobile Security Suite Administration if Oracle Identity Manager is Upgraded."](#)

5.4.1 Setting Up Administrators

To configure Administrators, you must complete the steps in this section.

Setting Up an Administrator Group in Oracle Identity Manager

To set up an Administrator Group in Oracle Identity Manager, perform the following steps:

1. Log in to the Oracle Identity Manager Console:
`http://oimhost:oimport/identity`
2. Click **Manage** in the upper right corner.
3. Select **Administration Roles**.
The Create Admin Role train component is displayed to create the Administrator Role.
4. In the General Role Information section, fill in the following information:
Name: The name of the role.
Display Name: The name displayed in the console.
Description: The description of the role.
5. In the Capabilities tab, add all capabilities.
6. In the Members stop/tab, assign all members that you want as Administrators:
 - a. Click the **Assign Users** button to search for users.
 - b. Select users from the results table.
 - c. Click the **Add Selected** button.
 - d. Click **Select**.
7. In the Scope of Control stop/tab, assign the organization in which this role will take effect:

Note: It is important to select a scope. You can select **Top** if you want these privileges to apply across the system.

- a. Click the **Add Organization** button to search for the organization.
 - b. Select organizations from the results table.
 - c. Click the **Add Selected** button.
 - d. Click **Select**.
8. In the Summary tab, click **Finish**.

Determining the Oracle Mobile Security Suite System Administrator Groups

Before granting Oracle Mobile Security Suite System Administrators the Oracle Identity Manager Administrator Role, you need to determine the names of the Oracle Mobile Security Suite System Administrator Groups.

Look up the Oracle Mobile Security Suite System Administrator Groups using the Access Policy Manager Console:

1. Log in to the Access Policy Manager Console.
2. Click **Configuration**.
3. Choose **Settings, View, Mobile Security Manager Settings**, and then **Identity Store Settings**.

4. View the set of Group Names configured as System Administrator Groups.

Setting Up an Administrator Group in Oracle Mobile Security Suite

To set up an Administrator Group in Oracle Mobile Security Suite, follow these steps:

1. Prepare the directory: Create an Administrator Role and make all assigned Administrators a member of this role, as documented in ["Setting Up an Administrator Group in Oracle Identity Manager"](#).
2. Determine the Oracle Mobile Security Suite System Administrator Groups, as documented in ["Determining the Oracle Mobile Security Suite System Administrator Groups"](#).
3. Log in to the Access Policy Manager Console as an existing Administrator:
`http://oamhost:oamport/access`
4. Click **Mobile Security Settings > Identity Store Settings**.
5. Within the System Admin Groups section, click **+Add** to add the Administrator Group.

5.4.2 Configuring Help Desk Users

To configure Help Desk Users, you must complete the steps in this section.

Setting Up a Help Desk User Group in Oracle Identity Manager

To set up a Help Desk User Group in Oracle Identity Manager, perform the following steps:

1. Log in to the Oracle Identity Manager Console:
`http://oimhost:oimport/identity`
2. Click **Manage** in the upper right corner.
3. Select **Administration Roles**.
The Create Admin Role train component is displayed to create the Administrator Role.
4. In the General Role Information section, fill in the following information:
Name: The name of the role.
Display Name: The name displayed in the console.
Description: The description of the role.
5. In the Capabilities tab, add the capabilities **Role Modify** and **Role View/Search**, and **All** capabilities on users.
6. In the Members stop/tab, assign all members that you want as Administrators:
 - a. Click the **Assign Users** button to search for users.
 - b. Select users from the results table.
 - c. Click the **Add Selected** button.
 - d. Click **Select**.
7. In the Scope of Control stop/tab, assign the organization in which this role will take effect:

Note: It is important to select a scope. You can select **Top** if you want these privileges to apply across the system.

- a. Click the **Add Organization** button to search for the organization.
 - b. Select organizations from the results table.
 - c. Click the **Add Selected** button.
 - d. Click **Select**.
8. In the Summary tab, click **Finish**.

Determining the Oracle Mobile Security Suite Help Desk User Group

Before granting Oracle Mobile Security Suite Help Desk Administrators the Oracle Identity Manager Help Desk Administrator Role, you need to determine the names of the Oracle Mobile Security Suite Help Desk User Groups.

Look up the Oracle Mobile Security Suite Help Desk User Groups using the Access Policy Manager Console:

1. Log in to the Access Policy Manager Console.
2. Click **Configuration**.
3. Choose **Settings, View, Mobile Security Manager Settings**, and then **Identity Store Settings**.
4. View the set of Group Names configured as Help Desk User Groups.

Setting Up the Help Desk User Group in Mobile Security Suite

To set up a Help Desk User Group in Mobile Security Suite, follow these steps:

1. Prepare the directory: Create a Help Desk role and make all assigned Help Desk Users a member of this role as documented in "[Setting Up a Help Desk User Group in Oracle Identity Manager](#)".
2. Determine the Oracle Mobile Security Suite Help Desk User Groups, as documented in "[Determining the Oracle Mobile Security Suite Help Desk User Group](#)".
3. Log in to the Access Policy Manager Console as an existing Administrator:
`http://oamhost:oamport/access`
4. Click **Mobile Security Settings > Identity Store Settings**.
5. Within the Helpdesk Groups section, click **+Add** to add the Help Desk User Group.

5.5 Integrating Oracle Mobile Security Suite in Upgrade Scenarios

This section contains information about additional steps you need to perform before or during the integration of Mobile Security Suite and Oracle Identity Manager if you have upgraded Oracle Identity Manager or an Oracle Identity Manager and Access Manager integrated environment to 11.1.2.3. The steps do not apply to new installations of Oracle Identity Manager.

Integrating Oracle Mobile Security Suite During an Upgrade of an Oracle Identity Manager and Access Manager Integrated Environment

If you are upgrading an Oracle Identity Manager and Access Manager integrated environment to 11.1.2.3 and want Oracle Mobile Security Suite to be integrated in the upgrade, you must perform these steps:

Note: It is recommended that you follow these steps after upgrade, but before setting up trust between Oracle Mobile Security Suite and Oracle Identity Manager domains and wiring Oracle Identity Manager and Oracle Mobile Security Manager.

1. In the OIM Domain, add the following lines in the `jps-config.xml` file under the `trust.provider.embedded` property set. (Skip this step if the lines are already present.)

```
<property name="trust.issuerName" value="www.oracle.com"/>
<property name="trust.aliasName" value="xell"/>
```

2. If the Oracle Mobile Security Manager SSL URL is or will be provided in `OIM_MSM_REST_SERVER_URL`, as documented in "[Wiring Oracle Mobile Security Manager and Oracle Identity Manager](#)," the following steps are required.

Note: If non-SSL communication is intended, these steps are not required.

- a. Log in to the WebLogic Administration Console.
- b. Navigate to **servers > oim_server1 > Configuration > SSL**.
- c. Select **Use JSSE SSL**.
Ignore this step if **Use JSSE SSL** is already selected.
- d. Click **Save**.
- e. Restart the managed servers (once) after wiring of Oracle Mobile Security Suite with Oracle Identity Manager.

For information on starting and stopping the managed server, see "Starting or Stopping the Oracle Stack" in *Installation Guide for Oracle Identity and Access Management*.

Wiring Oracle Mobile Security Manager and Oracle Identity Manager if Oracle Identity Manager is Upgraded

If you upgraded Oracle Identity Manager to 11.1.2.3 and want to use the WebLogic Scripting Tool instead of `idmConfigTool` to perform wiring, follow these steps:

1. Log in to the Oracle Identity Manager System Administration Console:

```
http://OIM-Host:OIM-port/sysadmin
```

2. Navigate to **Configuration Properties**, search for the property **OMSS Enabled**, and provide the value as `true`.
3. Run the WebLogic Scripting Tool from the following location:

```
/Oracle_IDM1/common/bin/wlst.sh
```

4. Run the following command:

```
createCred(map="msm",
key="msmLoginConfig",user="https://OASM-Host-Machine:OASM-SSL-Port/" ,
password="www.oracle.com",desc="RestConfig")
```

For example:

```
createCred(map="msm",
key="msmLoginConfig",user="https://abcde.example.com:14181/" ,
password="www.oracle.com",desc="RestConfig")
```

5. After running the command, restart the OIM Server.

Configuring Administrators for Oracle Identity Manager and Mobile Security Suite Administration if Oracle Identity Manager is Upgraded

If you upgraded Oracle Identity Manager to 11.1.2.3, perform the following steps in the 11.1.2.3 Oracle Identity Manager Console to make the Administration Role tab available for configuring Administrators:

1. Log in to the Oracle Identity Manager Console.
2. Click **Configuration Properties**.
3. Search for **Workflow Policies Enabled**.
4. Set **Workflow Policies Enabled** to **true**.
5. Restart the OIM Managed Server.

5.6 Viewing Oracle Mobile Security Manager Console Pages in the Oracle Identity Manager Console

The screens that can be displayed in Oracle Identity Manager after enabling Oracle Mobile Security Suite are listed in [Table 5–3](#).

Table 5–3 Oracle Mobile Security Suite Screens

Interface	Screen	Navigation	Who can access?
Identity Self Service	Devices tab in the My Access page	Manage tab, My Access	User who is part of a role to which at least one mobile security policy has been granted.
Identity Self Service	Devices tab in the user details page	Manage tab, Users, open user details	Is available only when: <ul style="list-style-type: none"> Selected user is part of a role to which at least one mobile security policy has been granted. Logged-in user has a role to which the privilege to view the details of all the devices and workspaces in the system has been granted.
Identity Self Service	Mobile Policy tab in the role details page	Manage tab, Roles, open role details	User who is part of a role to which privilege to view all mobile security policies has been granted, and the role is associated with at least one mobile security policy.

Table 5–3 (Cont.) Oracle Mobile Security Suite Screens

Interface	Screen	Navigation	Who can access?
Identity Self Service	Mobile Security Policies page	Manage tab, Policies, Mobile Security Policies	User who is part of a role to which privilege to view all mobile security policies has been granted.
Identity Self Service	Devices page	Manage tab, Mobile Security, Devices	User who is part of a role to which privilege to view the details of all the devices and workspaces in the system has been granted. Note: When integrated with Oracle Identity Manager, Oracle Mobile Security Suite does not consider the Oracle Identity Manager delegated Administrator Role (Organization Administrator, Role Administrator, and so on) privileges. When a Delegated Administrator like an Organization Administrator in Oracle Identity Manager accesses the Devices page, he can see all the devices for all users who are not under his purview. However, when he navigates to the Users page in Oracle Identity Manager he can only see the users who he is supposed to and the devices associated to those users.
Identity Self Service	Device Configurations	Manage tab, Mobile Security, Device Configurations	User who is part of a role to which privilege to view all the device configuration has been granted.
Identity Self Service	Mobile Applications	Manage tab, Mobile Applications	User who is part of a role to which privilege to view all the mobile applications has been granted.
Identity System Administration	Mobile Security Server Settings	Provisioning Configuration, Mobile Security Server Settings	User who is part of a role to which privilege to view all the mobile security server settings has been granted.

See *Oracle Fusion Middleware Help Reference for Oracle Mobile Security Suite Consoles* for information about Oracle Mobile Security Suite menus and screens.

Part III

External SSO Solutions

You can integrate federation partners into the Oracle IdM environment.

This part contains the following chapter:

- [Chapter 6, "Integrating with Identity Federation"](#)

Integrating with Identity Federation

This chapter explains how Oracle Access Management Access Manager leverages identity federation to create an authenticated session with a federation partner.

This chapter contains these sections:

- [Background and Integration Overview](#)
- [Integration with Access Manager 11gR2](#)
- [Scripts for Integration Tasks](#)

6.1 Background and Integration Overview

This section provides background about federation with Access Manager. Topics include:

- [About Oracle Access Management Identity Federation](#)
- [Deployment Options for Identity Federation](#)
- [References](#)

6.1.1 About Oracle Access Management Identity Federation

Identity federation is available in two architectures:

- As a federation engine, known as Oracle Access Management Identity Federation, built into Oracle Access Management (11g Release 2 (11.1.2)).
- As a standalone, self-contained federation server, known as Oracle Identity Federation, that enables single sign-on and authentication in a multiple-domain identity network (11g Release 1 (11.1.1)).

The SP integration Engine included with Oracle Identity Federation consists of a servlet that processes requests from the server to create a user authenticated session at the Identity and Access Management (IAM) server. The engine includes several internal plug-ins that allow it to interact with different IAM servers, including Access Manager (formerly Oracle Access Manager).

6.1.2 Deployment Options for Identity Federation

See Also: For details about naming conventions and name changes in Oracle Access Management, see Introduction to Oracle Access Management in *Administrator's Guide for Oracle Access Management* .

Various deployment options are available for leveraging identity federation with Access Manager to create an authenticated user session.

The Oracle Fusion Middleware framework supports these integrated approaches to cross-domain single sign-on:

- An Oracle Access Management Identity Federation engine built into the Access Manager server. All configuration is performed in Access Manager.
This approach is available in 11g Release 2 (11.1.2.3.0). The engine supports both Service Provider (SP) and Identity Provider (IdP) modes.
- Separate Oracle Identity Federation and Oracle Access Manager servers that can be integrated to provide federation capabilities. Management and configuration of both servers is required for this integration.

This approach is available in 11g Release 1 (11.1.1).

Under this approach, Oracle Identity Federation provides two deployment scenarios for Oracle Access Manager:

- Oracle Identity Federation 11g Release 1 (11.1.1) integrated with Oracle Access Manager 10g
- Oracle Identity Federation 11g Release 1 (11.1.1) integrated with Access Manager 11g

[Table 6–1](#) summarizes the options available to integrate the identity federation products with Oracle Access Management Access Manager and provides links to deployment procedures:

Table 6–1 Deployment Options Involving Oracle Access Manager

Access Manager Version	Description	Additional Information
Oracle Access Management Access Manager 11gR2	Access Manager contains a built-in federation engine that supports both SP and IdP mode functionality configurable through the Access Manager administration console.	Introduction to Federation within Oracle Access Suite Console in the <i>Administrator's Guide for Oracle Access Management</i> Section 6.2
Oracle Access Manager 11gR1	The stand-alone Oracle Identity Federation 11g Release 1 server integrates with the Access Manager 11g server.	Integrating Oracle Identity Federation in the <i>Oracle Fusion Middleware Integration Guide for Oracle Access Manager</i>
Oracle Access Manager 10g	The stand-alone Oracle Identity Federation 11g Release 1 server integrates with the Oracle Access Manager 10g server.	<i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>

6.1.3 References

Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation.

6.2 Integration with Access Manager 11gR2

This section describes how to integrate Access Manager 11g Release 2 (11.1.2.3.0) with Oracle Identity Federation 11g Release 1 (11.1.1). This is also referred to as Access Manager 11gR2 with Oracle Identity Federation 11gR1.

- [Architecture](#)
- [Overview of Integration Tasks](#)

- Prerequisites
- Additional Setup
- Register Oracle HTTP Server with Access Manager
- Configure Oracle Identity Federation
- Configure Access Manager
- Protecting a Resource with OIFScheme
- Test the Configuration

6.2.1 Architecture

Two integration modes are described in this chapter:

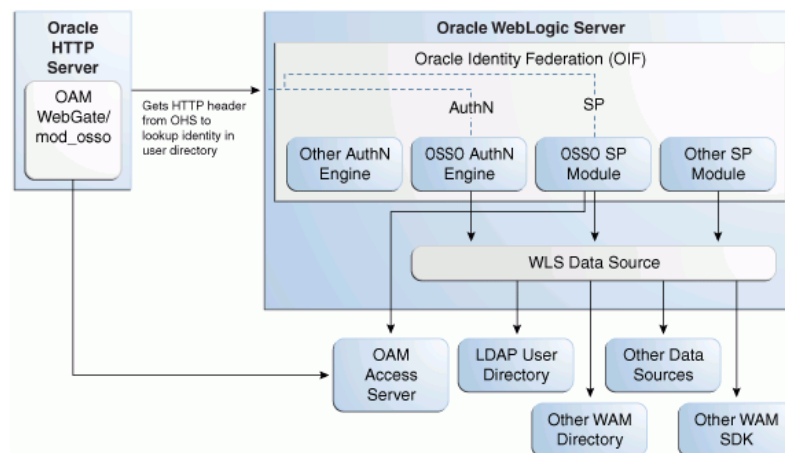
- SP Mode

This mode enables Oracle Identity Federation to authenticate the user via Federation SSO and propagate the authentication state to Access Manager, which maintains the session information.
- Authentication Mode

This mode enables Access Manager to authenticate the user on behalf of Oracle Identity Federation.

Figure 6–1 describes the processing flow in each mode:

Figure 6–1 Access Manager with Identity Federation



In the SP mode, Oracle Identity Federation uses the federation protocols to identify a user, and requests Access Manager to create an authenticated session at Access Manager.

In the authentication mode, Oracle Identity Federation delegates authentication to Access Manager through the use of a WebGate agent protecting an Oracle Identity Federation resource. Once the user is authenticated, the WebGate will assert the user's identity by an HTTP Header that Oracle Identity Federation will read to identify the user.

6.2.2 Overview of Integration Tasks

The integration between Access Manager and Oracle Identity Federation requires the following tasks:

- Ensure that the necessary components, including Oracle WebLogic Server and Identity Management (IdM) components, are installed and operational. For details, see [Section 6.2.4](#).
- Register Oracle HTTP Server as a partner with Access Manager to protect a resource. For details, see [Section 6.2.5](#).
- Configure the Oracle Identity Federation server to function as a service provider (SP) and/or as an identity provider (IdP) with Access Manager. For details, see [Section 6.2.6](#).
- Configure Access Manager to delegate authentication to Oracle Identity Federation and/or to authenticate a user on behalf of Oracle Identity Federation, For details, see [Section 6.2.7](#).

6.2.3 Prerequisites

You must install the following components prior to undertaking the integration tasks:

- Oracle WebLogic Server
- Oracle HTTP Server 11g
- Access Manager 11g
- Oracle Identity Federation 11g
- WebGate (required in authentication mode)

Note: Refer to the Certification Matrix for platform and version details.

See Also:

Oracle Fusion Middleware Installation Guide for Oracle Identity Management

6.2.4 Additional Setup

Oracle WebLogic Server

Ensure that the administration and managed servers are up and running.

Oracle HTTP Server

For testing purposes, identify or create a resource to be protected. For example, create an `index.html` file to serve as a test resource.

Oracle Identity Federation

Access the Fusion Middleware Control console for the Oracle Identity Federation server using a URL of the form:

`http://oif_host:oif_em_port/em`

Verify that all the servers are running.

6.2.5 Register Oracle HTTP Server with Access Manager

This section shows how you can register Oracle HTTP Server and 11g WebGate with Access Manager, depending on the protection mechanism you have chosen.

Follow these steps to register Oracle HTTP Server and Access Manager 11g WebGate with Access Manager for authentication:

Note: In this procedure, `MW_HOME` represents the Oracle Fusion Middleware Home directory.

1. Locate the `OAM11GRequest.xml` file or the `OAM11GRequest_short.xml` file, which resides in the directory:

```
MW_HOME/Oracle_IDM1/oam/server/rreg/input
```

2. Make the necessary changes to the file.
3. Locate the `oamreg.sh` script, which resides in the directory:

```
MW_HOME/Oracle_IDM1/oam/server/rreg/bin
```

4. Execute the script using the command string:

Note: The user is `weblogic`, and you must supply the password.

```
./oamreg.sh inband input/OAM11GRequest.xml
```

or

```
./oamreg.sh inband input/OAM11GRequest_short.xml
```

5. Using the Access Manager console, create a resource representing the Oracle Identity Federation URL to be protected by Access Manager for authentication. This URL contains the hostname and port of the Oracle Identity Federation server, and the path to the resource, which is mode-dependent:

```
http(s)://oif-host:oif-port/fed/user/authnoam11g
```

6. Protect this resource with an authentication policy and an authorization policy.
7. Restart Oracle HTTP Server:

```
Oracle_WT1/instances/instance1/bin/opmnctl restartproc process-type=OHS
```

You can also restart Oracle HTTP Server with:

```
Oracle_WT1/instances/instance1/bin/opmnctl stopall
Oracle_WT1/instances/instance1/bin/opmnctl startall
```

6.2.6 Configure Oracle Identity Federation

This section describes how to configure Oracle Identity Federation to be integrated with Access Manager:

- In SP mode, Access Manager will delegate authentication to Oracle Identity Federation for Federation SSO.
- In Authentication mode, Oracle Identity Federation will delegate authentication to Access Manager.

This section contains these topics:

- [Verify the User Data Store](#)
- [Configure Oracle Identity Federation Authentication Engine](#)
- [Configure Oracle Identity Federation SP Integration Module](#)

6.2.6.1 Verify the User Data Store

Oracle Identity Federation and Access Manager must use the same LDAP directory:

- The LDAP directory to be used must be defined in Access Manager as the default Identity Store.
- The Oracle Identity Federation User Data Store must reference the LDAP directory to be used.

Take these steps to verify the data store configuration:

1. Locate the Oracle Identity Federation instance in Fusion Middleware Control.
2. Navigate to **Administration**, then **Data Stores**.
3. Ensure that the user data store points to the same directory as the default Access Manager identity store.

6.2.6.2 Configure Oracle Identity Federation Authentication Engine

Note: [Section 6.3](#) describes scripts that you can execute to automatically perform the manual operations shown here.

Take these steps to configure the Oracle Identity Federation Authentication Engine to retrieve information provided by the WebGate 11g agent:

1. Locate the Oracle Identity Federation instance in Fusion Middleware Control.
2. Navigate to **Administration**, then **Authentication Engines**.
3. Enable the Access Manager 11g authentication engine.
4. Select WebGate 11g as the Agent Type.
5. Enter OAM_REMOTE_USER as the User Unique ID Header.
6. In the Default Authentication Engine drop-down list, select Oracle Access Manager 11g.
7. Configure logout:
 - If Oracle Identity Federation is also going to be integrated with Access Manager in SP mode, then disable logout as the logout integration with Access Manager 11g will be performed with the OAM11g SP engine.
 - If Oracle Identity Federation is not going to be integrated with Access Manager in SP mode:
 - Enable logout
 - Enter the following as the URL:
`http(s)://oam_host:oam_port/oam/server/logout`
8. Click **Apply**.

6.2.6.3 Configure Oracle Identity Federation SP Integration Module

This section lists the steps that need to be performed to configure Oracle Identity Federation in SP mode for Access Manager, so that Oracle Identity Federation can send assertion tokens and direct session management to Access Manager.

Note: [Section 6.3](#) describes scripts that you can execute to automatically perform the manual operations shown here.

The steps to achieve this are as follows:

1. Locate the Oracle Identity Federation instance in Fusion Middleware Control.
2. Navigate to Administration, then Service Provider Integration Modules.
3. Select the Oracle Access Manager 11g tab.
4. Configure the page as follows:

- Check the **Enable SP Module** box.
- In the Default SP Integration Module drop-down, select Oracle Access Manager 11g.
- Check the **Logout Enabled** box.
- Configure these URLs:

Login URL : `http(s)://oam_host:oam_port/oam/server/dap/cred_submit`
 Logout URL: `http(s)://oam_host:oam_port/oam/server/logout`

where `oam_host` and `oam_port` are the host and port number of the Access Manager server respectively.

- Set Username Attribute value to "cn" to match the Access Manager username attribute.
 - Click **Apply**.
5. Click **Regenerate**.

This action generates a keystore file that contains the keys used to encrypt and decrypt the tokens that are exchanged between the Access Manager and Oracle Identity Federation servers. Be sure to save the keystore file using the **Save As** dialog.

Copy the keystore file to a location within the installation directory of Access Manager.

Note: Make a note of the location, since you will need to refer to it later.

6.2.7 Configure Access Manager

This section describes how to configure Access Manager to integrate with Oracle Identity Federation:

- In SP mode, Access Manager will delegate authentication to Oracle Identity Federation for Federation SSO.
- In Authentication mode, Oracle Identity Federation will delegate authentication to Access Manager.

This section contains these topics:

- [Configure OIFScheme](#)
- [Register Oracle Identity Federation as a Trusted Access Manager Partner](#)

6.2.7.1 Configure OIFScheme

This task configures Access Manager to redirect the user to Oracle Identity Federation for authentication when OIFScheme is used to protect a resource using Federation single sign-on. The steps needed to achieve this are as follows:

1. Log in to the Access Manager Administration Console:

```
http://oam_adminserver_host:oam_adminserver_port/oamconsole
```

2. Select the Policy Configuration tab.
3. Select and open the OIFScheme.
4. In the Challenge URL field, modify the value of OIF-Host and OIF-Port:

```
http(s)://oif-host:oif-port/fed/user/spoam11
```

5. Confirm that the value of the Context Type drop-down is set to "external".
6. Click **Apply** to save the changes.

6.2.7.2 Register Oracle Identity Federation as a Trusted Access Manager Partner

If Oracle Identity Federation is used in SP mode only, or authentication and SP mode, refer to [Section 6.2.7.2.1](#).

If Oracle Identity Federation is used in authentication mode only, refer to [Section 6.2.7.2.2](#).

Note: [Section 6.3](#) describes scripts that you can execute to automatically perform the manual operations shown here to register Oracle Identity Federation as a trusted partner.

6.2.7.2.1 Register Oracle Identity Federation for Use in SP Mode

Note: Prior to performing this procedure, ensure that OAM admin server and all managed servers are running.

Copy the keystore file to a directory under the middleware home in which the Access Manager server is installed.

Use a WLST command to update the OIFDAP partner block in the `oam-config.xml` configuration file. The steps and syntax are as follows:

1. Enter the shell environment by executing:

```
$DOMAIN_HOME/common/bin/wlst.sh
```

2. Connect to the Access Manager administration server with the following command syntax:

```
connect('weblogic', 'password', 'host:port')
```

3. Execute the command to update the partner block in the configuration file:

```
registerOIFDAPPartner (keystoreLocation=location of keystore file,
logoutURL=logoutURL)
```

where `logoutURL` is the Oracle Identity Federation logout URL that is invoked when the Access Manager server logs out the user.

For example:

```
registerOIFDAPPartner (keystoreLocation="/home/pjones/keystore",
logoutURL="http://abcdef0123.in.mycorp.com:1200/fed/user/spsloam1g?doneURL=http://abc1234567.in.mycorp.com:6001/oam/pages/logout.jsp")
```

6.2.7.2.2 Register Oracle Identity Federation for Use in Authentication Mode

Use a WLST command to update the OIFDAP partner block in the `oam-config.xml` configuration file. The steps and syntax are as follows:

1. Enter the shell environment by executing:

```
$DOMAIN_HOME/common/bin/wlst.sh
```

2. Connect to the Access Manager administration server with the following command syntax:

```
connect('weblogic', 'password', 'host:port')
```

3. Execute the command to update the partner block in the configuration file:

```
registerOIFDAPPartnerIDPMode (logoutURL=logoutURL)
```

where `logoutURL` is the Oracle Identity Federation logout URL that is invoked when the Access Manager server logs out the user.

For example:

```
registerOIFDAPPartnerIDPMode (logoutURL="http://abcdef0123.in.mycorp.com:1200/fed/user/authnsloam1g?doneURL=http://abc1234567.in.mycorp.com:6001/oam/pages/logout.jsp")
```

6.2.8 Protecting a Resource with OIFScheme

After the integration of Access Manager and Oracle Identity Federation in SP mode, a resource can now be protected with `OIFScheme`, which will trigger a Federation single sign-on operation when an unauthenticated user requests access to a resource protected by that scheme.

In an Application Domain of the Policy Configuration tab, define an Authentication Policy using the `OIFScheme`, and protect a resource with that authentication policy.

6.2.9 Test the Configuration

The final configuration task is to test whether the integration is correctly configured. The steps differ between authentication mode and SP mode.

- [Test SP Mode Configuration](#)
- [Test Authentication Mode Configuration](#)

6.2.9.1 Test SP Mode Configuration

Take these steps to test for correct configuration in SP mode:

1. Establish federated trust between Oracle Identity Federation and a remote Identity Provider (IdP).
2. Set that identity provider as the default SSO identity provider.
3. Try accessing the protected resource.
4. When set up correctly, you should be redirected to the IdP for authentication. Verify that user credentials are required on this page.
5. Enter valid credentials on the login page.

Note: The user should exist in both the IdP security domain and the Oracle Identity Federation/Access Manager security domain.

6. Check that you are redirected to the protected page.
7. Verify that the following cookies are created:
 - OAM_ID
 - ORA_OSFS_SESSION
 - OHS Cookie

6.2.9.2 Test Authentication Mode Configuration

Take these steps to test for correct configuration in authentication mode:

1. Establish federated trust between Oracle Identity Federation and a remote service provider.
2. Initiate federation single sign-on from the service provider.
3. Verify that you are redirected to the Access Manager login page at the IdP. On this page user credentials are requested.
4. Enter the relevant credentials and process the page.
5. Verify that you are redirected to the service provider domain.

6.3 Scripts for Integration Tasks

This section describes scripts that automate some of the Oracle Identity Federation configuration tasks described in [Section 6.2](#) for Oracle Access Manager integration .

The automated steps make the integration smoother and faster than a purely manual procedure.

This section contains these topics:

- [Perform the Preliminary Procedure](#)
- [Additional Setup](#)
- [Execute the Automated Procedure](#)

6.3.1 Perform the Preliminary Procedure

The prerequisite procedure is performed before you do anything else for integration. Ensure that the following have been done:

1. The following components are installed:

- Oracle WebLogic Server
- Oracle HTTP Server
- Oracle Access Manager 11g
- Oracle Identity Federation 11g

Note: Refer to the Certification Matrix for platform and version details.

For guidance on integration prerequisites, see *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

2. Oracle Identity Federation 11g and Oracle HTTP Server are integrated; that is, Oracle HTTP Server is configured as the front end to the Oracle Identity Federation server.

For details, see "Deploying Oracle Identity Federation with Oracle HTTP Server" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

3. The SSO agent is already created and integrated with Access Manager 11g .

6.3.2 Additional Setup

Oracle WebLogic Server

Ensure that the administration and managed servers are up and running.

Oracle Identity Federation

Access the Fusion Middleware Control console for the Oracle Identity Federation server using a URL of the form:

```
http://oif_host:oif_em_port/em
```

Verify that all the servers are running.

6.3.3 Execute the Automated Procedure

This section describes the procedure that automates some tasks in the integration of Oracle Access Manager with Oracle Identity Federation. The procedure is performed by executing python scripts provided in the distribution.

[Section 6.2.6, "Configure Oracle Identity Federation"](#) describes the tasks that you can automate with scripts.

6.3.3.1 Scope of the Automated Process

The scripts perform the following tasks/procedures:

- Automation of all Oracle Identity Federation configuration
- Registration of Oracle Identity Federation as DAP partner in Access Manager
- Addition of Oracle Identity Federation URLs as protected resources in the policy domain.

6.3.3.2 Copy the Scripts to the Access Manager Machine

You need to copy certain files to the Access Manager host. The files are as follows:

- `setupOIFOAMConfig.sh`,
- `setupOIFOAMIntegration.py`
- locale specific resource bundle `oifWLSTResourceBundle_locale.properties`

Create a directory to save these files or copy into an existing directory, in the Access Manager host machine. For example, `/scratch/scripts` (linux) or `c:\temp\scripts` (Windows).

6.3.3.3 Understand the inputs to the Scripts

The script takes in named parameters as inputs (order of inputs does not matter). The inputs mostly have default values if not passed in.

Table 6–2 shows the inputs needed by the scripts:

Table 6–2 Inputs for the OAM-OIF 11gR1 Integration Scripts

Parameter	Description	Default	Required?
<code>oifHost</code>	Hostname of Oracle Identity Federation managed server	None	Yes
<code>oifPort</code>	Port number of Oracle Identity Federation Managed server	7499	No
<code>oifAdminHost</code>	Hostname of Oracle Identity Federation Admin server	<code>oifHost</code>	No
<code>oifAdminPort</code>	Port number of Oracle Identity Federation Admin server	7001	No
<code>oamAdminHost</code>	Hostname of Access Manager Admin server	<code>localhost</code>	No
<code>oamAdminPort</code>	Port number of Access Manager Admin server	7001	No
<code>agentType</code>	Agent type used, such as <code>webgate10g</code> , <code>webgate11g</code> , <code>mod_osso</code>	<code>webgate11g</code>	No

Note: The agent type is the agent created in Access Manager using the `rreg` tool or through the Access Manager console.

6.3.3.4 Run the Scripts

The automation is run by executing the script file `setupOIFOAMConfig.sh` (Unix) or `setupOIFOAMConfig.cmd` (Windows).

The steps are as follows:

On Unix

The following steps show how to run the script. Substitute the sample parameter values with appropriate values.

1. In a command line prompt set the `DOMAIN_HOME`:


```
export DOMAIN_HOME=path to domain home
```
2. If Oracle Identity Federation administration and managed server are on the same host and the agent type is non-default (for example, `webgate10g`), execute the command:


```
./setupOIFOAMConfig.sh oifHost=myhost oifPort=portnum oamAdminHost=myhost2
oamAdminPort=portnum2 agentType=webgate10g
```

3. If Oracle Identity Federation administration and managed server are on different hosts, with a default agent type (webgate11g), execute the command:

```
./setupOIFOAMConfig.sh oifHost=myhost oifPort=portnum oifAdminHost=myhost2
oifAdminPort=portnum2 oamAdminHost=myhost3 oamAdminPort=portnum3
```

4. If Oracle Identity Federation administration and managed server are on the same host, and all defaults apply from [Table 6-2](#), execute the command:

```
./setupOIFOAMConfig.sh oifHost=myhost oamAdminHost=myhost2
```

On Windows

The following steps show how to run the script. Substitute the sample parameter values with appropriate values.

1. In a command line prompt set the DOMAIN_HOME:

```
set DOMAIN_HOME=path to oam domain home
```

2. If Oracle Identity Federation administration and managed server are on the same host and the agent type is non-default (for example, webgate10g), execute the command:

```
setupOIFOAMConfig.cmd "oifHost=myhost" "oifPort=portnum"
"oamAdminHost=myhost2" "oamAdminPort=portnum2" "agentType=webgate10g"
```

3. If Oracle Identity Federation administration and managed server are on different hosts, with a default agent type (webgate11g), execute the command:

```
setupOIFOAMConfig.cmd "oifHost=myhost" "oifPort=portnum" "oifAdminHost=myhost2"
"oifAdminPort=portnum2" "oamAdminHost=myhost3" "oamAdminPort=portnum3"
```

4. If Oracle Identity Federation administration and managed server are on the same host, and all defaults apply from [Table 6-2](#), execute the command:

```
setupOIFOAMConfig.cmd "oifHost=myhost" " " "oamAdminHost=myhost3"
```


Part IV

Additional Identity Store Configuration

This part contains topics related to additional configuration of the identity store.

This part contains the following chapter:

- [Chapter 7, "Configuring an Identity Store with Multiple Directories"](#)

Configuring an Identity Store with Multiple Directories

This chapter explains how to prepare directories other than Oracle Internet Directory for use as an Identity Store.

This chapter contains the following topics:

- [Section 7.1, "Overview of Configuring Multiple Directories as an Identity Store"](#)
- [Section 7.2, "Configuring Multiple Directories as an Identity Store: Split Profile"](#)
- [Section 7.3, "Configuring Multiple Directories as an Identity Store: Distinct User and Group Populations in Multiple Directories"](#)
- [Section 7.4, "Additional Configuration Tasks"](#)

7.1 Overview of Configuring Multiple Directories as an Identity Store

This chapter describes how to configure Oracle Virtual Directory for two multiple directory scenarios. In both scenarios, you have some user data in a third-party directory, such as Active Directory, and other user data in Oracle Internet Directory.

In both scenarios, you use Oracle Virtual Directory to present all the identity data in a single consolidated view that Oracle Identity Management components can interpret.

The scenarios are as follows:

- **Split Profile:** A split profile, or split directory configuration, is one where identity data is stored in multiple directories, possibly in different locations. You use a split profile when you must extend directory schema in order to support specific schema elements, but you cannot or do not want to extend the schema in the third-party Identity Store. In that case, deploy an Oracle Internet Directory as a shadow directory to store the extended attributes. For details, see [Section 7.3, "Configuring Multiple Directories as an Identity Store: Distinct User and Group Populations in Multiple Directories."](#) (If, on the other hand, you can extend the schema, use the approach described in [Section 2.3.1, "Extending Directory Schema for Access Manager."](#))
- **Distinct User and Group Populations:** Another multidirectory scenario is one where you have distinct user and group populations, such as internal and external users. In this configuration, Oracle-specific entries and attributes are stored in Oracle Internet Directory. Enterprise-specific entries, for example, entries with Fusion Applications-specific attributes, are stored in Active Directory. For details, see [Section 7.3, "Configuring Multiple Directories as an Identity Store: Distinct User and Group Populations in Multiple Directories."](#)

In this chapter, Active Directory is chosen as the non-Oracle Internet Directory Enterprise Directory. The solution is applicable to all enterprises having one or more Active Directories as their enterprise Identity Store.

7.2 Configuring Multiple Directories as an Identity Store: Split Profile

This section describes how to configure multiple directories as an Identity Store. In cases where the Active Directory schema cannot be extended, you use Oracle Internet Directory as a shadow directory to store these attributes. Oracle Virtual Directory links them together to present a single consolidated DIT view to clients. This is called a split profile or split directory configuration. In this configuration, all the Oracle specific attributes and Oracle specific entities are created in Oracle Internet Directory.

This section contains the following topics:

- [Section 7.2.1, "Prerequisites"](#)
- [Section 7.2.2, "Repository Descriptions"](#)
- [Section 7.2.3, "Setting Up Oracle Internet Directory as a Shadow Directory"](#)
- [Section 7.2.4, "Directory Structure Overview - Shadow Join"](#)
- [Section 7.2.5, "Configuring Oracle Virtual Directory Adapters for Split Profile"](#)
- [Section 7.2.6, "Configuring a Global Consolidated Changelog Plug-in"](#)
- [Section 7.2.7, "Validating the Oracle Virtual Directory Changelog"](#)

7.2.1 Prerequisites

The following assumptions and rules apply to this deployment topology:

- Oracle Internet Directory houses the Fusion Identity Store. This means that Oracle Internet Directory is the store for all Fusion Application-specific artifacts. The artifacts include a set of enterprise roles used by Fusion Application and some user attributes required by Fusion Applications. All other stores are referred to as enterprise Identity Stores.
- The enterprise contains more than one LDAP directory. Each directory contains a distinct set of users and roles.
- The enterprise policy specifies that specific user attributes, such as Fusion Application-specific attributes, cannot be stored in the enterprise directory. All the extended attributes must be stored in a separate directory called the shadow directory. This shadow directory must be Oracle Internet Directory because Active Directory does not allow you to extend the schema.
- User login IDs are unique across the directories. There is no overlap of the user login IDs between these directories.
- Oracle Identity Manager has no fine-grained authorization. If Oracle Identity Manager's mapping rules allow it to use one specific subtree of a directory, then it can perform all CRUD (Create, Read, Update, Delete) operations in that subtree of the LDAP directory. There is no way to enable Oracle Identity Manager to read user data in a subtree but not enable it to create a user or delete a user in subtree.
- Referential integrity must be turned off in Oracle Internet Directory so that an Oracle Internet Directory group can have members that are in one of the Active Directory directories. The users group memberships are not maintained across the directories with referential integrity.

7.2.2 Repository Descriptions

This section describes the artifacts in the Identity store and how they can be distributed between Active Directory and Oracle Internet Directory, based on different enterprise deployment requirements.

The Artifacts that are stored in the Identity Store are:

- Application IDs: These are the identities that are required to authenticate applications to communicate with each other.
- Seeded Enterprise Roles: These are the enterprise roles or LDAP group entries that are required for default functionality.
- Enterprise roles provisioned by Oracle Identity Manager: These are runtime roles.
- Enterprise Users: These are the actual users in the enterprise.
- Enterprise Groups: These are the roles and groups that already exist in the enterprise.

In a split profile deployment, the Identity Store artifacts can be distributed among Active Directory and Oracle Internet Directory, as follows.

- Oracle Internet Directory is a repository for enterprise roles. Specifically, Oracle Internet Directory contains the following:
 - Application IDs
 - Seeded enterprise roles
 - Enterprise roles provisioned by Oracle Identity Manager
- Active Directory is the repository for:
 - Enterprise users
 - Enterprise groups (not visible to Oracle Identity Manager or Fusion Applications)

The following limitations apply:

- The Active Directory users must be members of Oracle Internet Directory groups.
- The groups in Active Directory are not exposed at all. Oracle applications only manage the Oracle-created enterprise roles. The groups in Active Directory are not visible to either Oracle Identity Manager or Fusion Applications.

7.2.3 Setting Up Oracle Internet Directory as a Shadow Directory

In cases where Oracle Internet Directory is used as the shadow directory to store certain attributes, such as all the Fusion Application-specific attributes, use a separate container in Oracle Internet Directory to store the shadow attributes.

- The Shadow Entries container (`cn=shadowentries`) must be in a separate DIT from the parent of the users and groups container `dc=mycompany,dc=com`, as shown in [Figure 7-1](#).
- The same ACL configured for `dc=mycompany,dc=com` within Oracle Internet Directory must be configured for `cn=shadowentries`. To perform this configuration, use the `ldapmodify` command. The syntax is as follows:

```
ldapmodify -D cn=orcladmin -q -p portNum -h hostname -f ldifFile
```

The following is a sample LDIF file to use with `ldapmodify`:

```

dn: cn=shadowentries
changetype: modify
add: orclaci
orclaci: access to entry by
group="cn=RealmAdministrators,cn=groups,cn=OracleContext,dc=mycompany,dc=com"
(browse,add,delete)
orclaci: access to attr=(*) by
group="cn=RealmAdministrators,cn=groups,cn=OracleContext,dc=mycompany,dc=com"
(read, write, search, compare)
orclaci: access to entry by
group="cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com" (browse,add,delete)
orclaci: access to attr = (*) by
group="cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com"
(search,read,compare,write)
-
changetype: modify
add: orclentrylevelaci
orclentrylevelaci: access to entry by * (browse,noadd,nodelete)
orclentrylevelaci: access to attr=(*) by * (read,search,nowrite,nocompare)
    
```

- If you have more than one directory for which Oracle Internet Directory is used as a Shadow directory, then you must create different shadow containers for each of the directories. The container name can be chosen to uniquely identify the specific directory for which this is a shadow entry.

7.2.4 Directory Structure Overview - Shadow Join

Figure 7-1 shows the directory structure in the primary and shadow directories. The containers `cn=reservation`, `cn=appIDUsers`, `cn=FusionGroups`, and `cn=DataRoleGroups` are specific to Fusion Applications.

Figure 7-1 Directory Structure

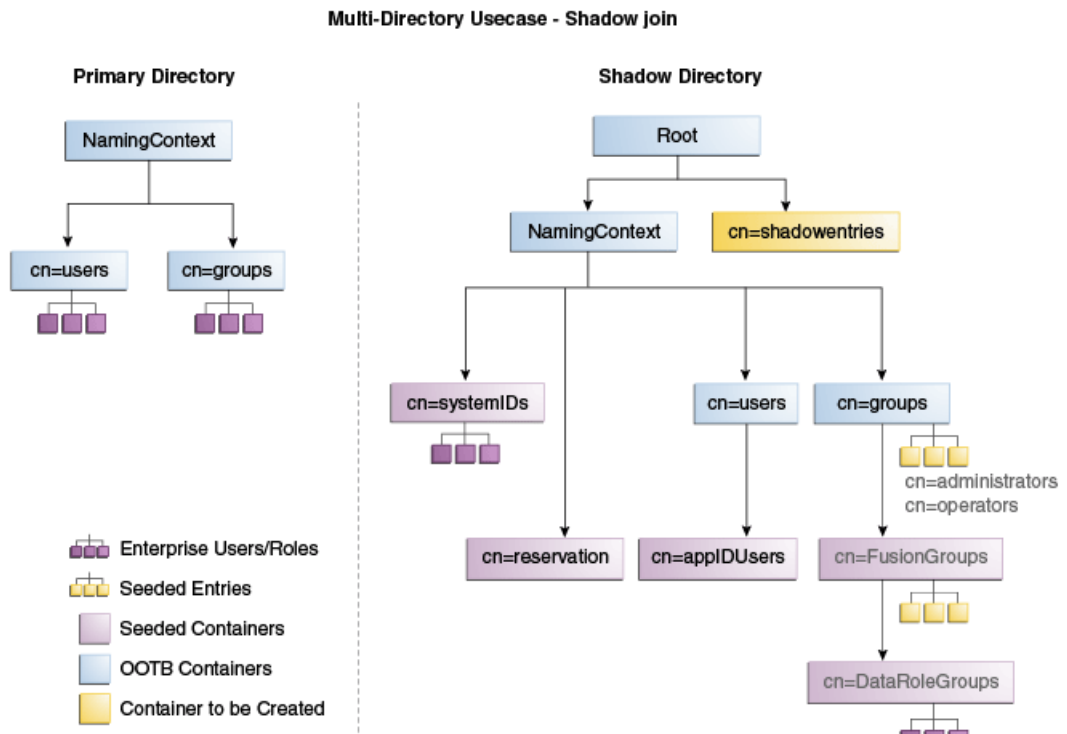


Figure 7-2 shows how the DIT appears to a user or client application. The containers `cn=appIDUsers`, `cn=FusionGroups`, and `cn=DataRoleGroups` are specific to Fusion Applications.

Figure 7-2 Client View of the DIT

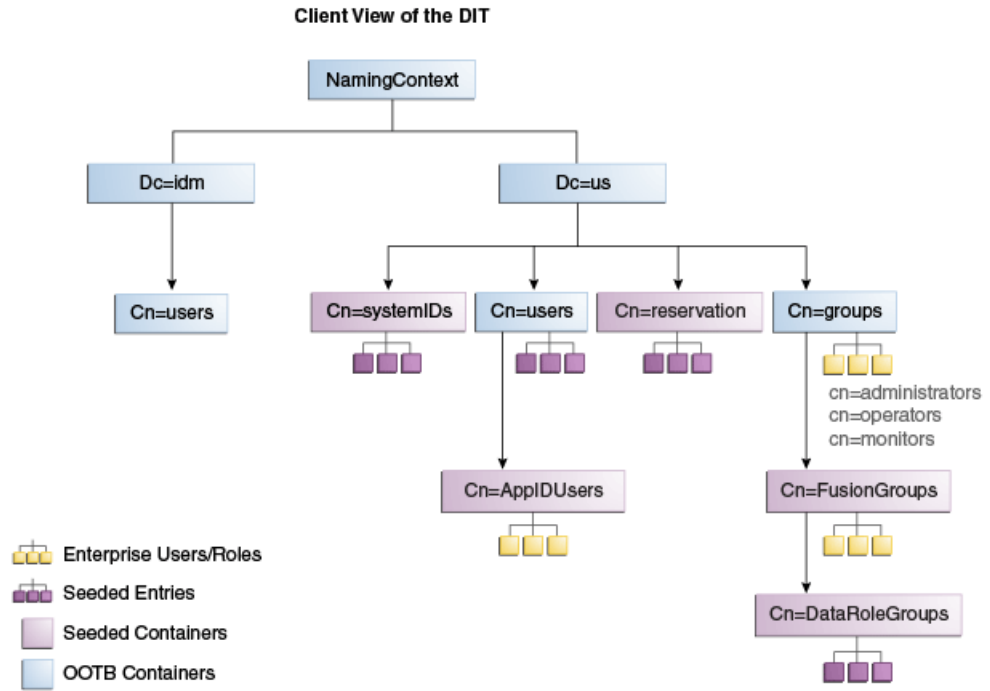
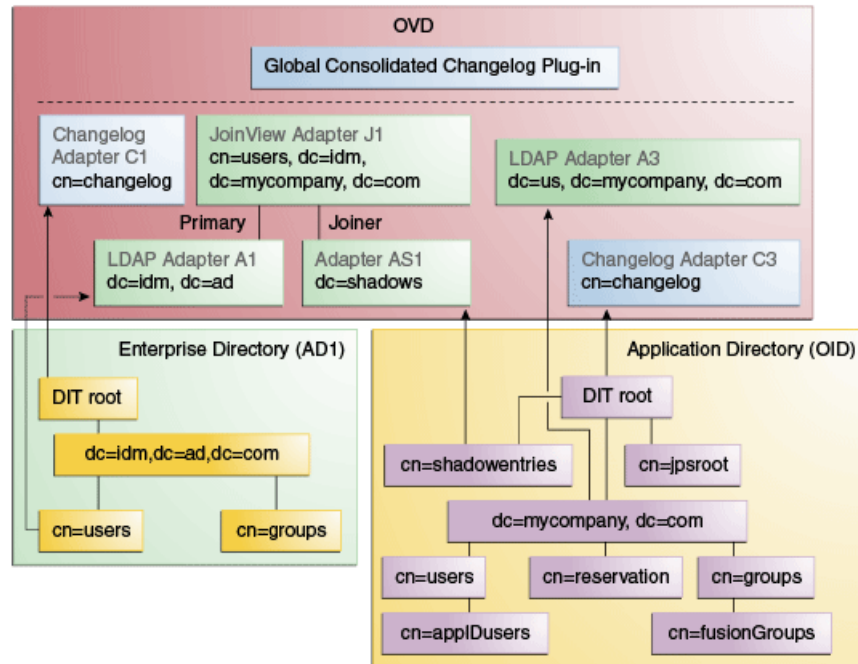


Figure 7-3 summarizes the adapters and plug-ins. The containers `cn=appIDUsers`, and `cn=FusionGroups` are specific to Fusion Applications.

Figure 7-3 Adapter and Plug-in Configuration



7.2.5 Configuring Oracle Virtual Directory Adapters for Split Profile

In order to produce the client side view of the data shown in [Figure 7-2](#), you must configure multiple adapters in Oracle Virtual Directory following the steps in this section.

You can use `idmConfigTool` to create the adapters to facilitate this configuration.

See Also: [Section A.1, "Verifying Oracle Virtual Directory Adapters for Split Profile by Using ODSM"](#) for instructions on viewing the adapters using Oracle Directory Services Manager.

To create the adapters using `idmConfigTool`, perform the following tasks on `IDMHOST1`:

1. Set the environment variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME` and `ORACLE_HOME`.
Set `IDM_HOME` to `IDM_ORACLE_HOME`
Set `ORACLE_HOME` to `IAM_ORACLE_HOME`
2. Create a properties file for the adapter you are configuring called `splitprofile.props`, with the following content:

```
ovd.host:ldaphost1.mycompany.com
ovd.port:8899
ovd.binddn:cn=orcladmin
ovd.ssl:true
ldap1.type:AD
ldap1.host:adhost.mycompany.com
ldap1.port:636
ldap1.binddn:administrator@idmqa.com
ldap1.ssl:true
ldap1.base:dc=idmqa,dc=com
ldap1.ovd.base:dc=idmqa,dc=com
usecase.type:split
ldap2.type:OID
ldap2.host:ldaphost.mycompany.com
ldap2.port:3060
ldap2.binddn:cn=oimLDAP,cn=users,dc=mycompany,dc=com
ldap2.ssl:false
ldap2.base:dc=mycompany,dc=com
ldap2.ovd.base:dc=mycompany,dc=com
```

The following list describes the parameters used in the properties file.

- `ovd.host` is the host name of a server running Oracle Virtual Directory.
- `ovd.port` is the https port used to access Oracle Virtual Directory.
- `ovd.binddn` is the user DN you use to connect to Oracle Virtual Directory.
- `ovd.password` is the password for the DN you use to connect to Oracle Virtual Directory.
- `ovd.oamenabled` is set to `true` if you are using Oracle Access Management Access Manager, otherwise set to `false`.
`ovd.oamenabled` is always `true` in Fusion Applications deployments.
- `ovd.ssl` is set to `true`, as you are using an https port.

- `ldap1.type` is set to `OID` for the Oracle Internet Directory back end directory or set to `AD` for the Active Directory back end directory.
 - `ldap1.host` is the Active Directory host. Use the load balancer name where the host is highly available.
 - `ldap2.host`: The Oracle Internet Directory host. Use the load balancer name where the host is highly available.
 - `ldap1.port` is the port used to communicate with the back end directory.
 - `ldap1.binddn` is the bind DN of the `oimLDAP` user.
 - `ldap1.password` is the password of the `oimLDAP` user
 - `ldap1.ssl` is set to `true` if you are using the back end's SSL connection, and otherwise set to `false`. This should always be set to `true` when an adapter is being created for AD.
 - `ldap1.base` is the base location in the directory tree.
 - `ldap1.ovd.base` is the mapped location in Oracle Virtual Directory.
 - `usecase.type` is set to `Single` when using a single directory type.
3. Configure the adapter by using the `idmConfigTool` command, which is located at:
- `IAM_ORACLE_HOME/idmtools/bin`

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

`IAM_ORACLE_HOME/idmtools/bin`

The syntax of the command on Linux is:

```
idmConfigTool -configOVD input_file=splitprofile.props
```

During the running of the command you will be prompted for the passwords to each of the directories you will be accessing.

The command must be run once for each Oracle Virtual Directory instance.

7.2.6 Configuring a Global Consolidated Changelog Plug-in

Deploy a global level consolidated changelog plug-in to handle changelog entries from all the Changelog Adapters.

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to an Oracle Virtual Directory instance.
3. On the Home page, click the **Advanced** tab. The Advanced navigation tree appears.
4. Expand **Global Plugins**
5. Click the **Create Plug-In** button. The Plug-In dialog box appears.
6. Enter a name for the Plug-in in the Name field.
7. Select the plug-in class **ConsolidatedChglogPlugin** from the list.

8. Click **OK**.
9. Click **Apply**.

7.2.7 Validating the Oracle Virtual Directory Changelog

Run the following command to validate that the changelog adapter is working:

```
$IDM_ORACLE_HOME/bin/ldapsearch -p 6501 -D cn=orcladmin -q -b 'cn=changelog' -s  
base 'objectclass=*' lastchangenumber
```

The command should return a changelog result, such as:

```
Please enter bind password:  
cn=Changelog  
lastChangeNumber=changelog_OID:190048;changelog_AD1:363878
```

If `ldapsearch` does not return a changelog result, double check the changelog adapter configuration.

7.3 Configuring Multiple Directories as an Identity Store: Distinct User and Group Populations in Multiple Directories

In this configuration, you store Oracle-specific entries in Oracle Internet Directory and enterprise-specific entries in Active Directory. If necessary, extend the Active Directory schema as described in "Configuring Active Directory for Use with Oracle Access Management Access Manager and Oracle Identity Manager" in *Enterprise Deployment Guide for Oracle Identity and Access Management*.

Note: The Oracle Internet Directory that is to be used is not necessarily the PolicyStore Oracle Internet Directory. Conceptually, a non-Active Directory directory can be used as the second directory. For convenience, this section refers to the Policy Store Oracle Internet Directory.

The following conditions are assumed:

- Enterprise Directory Identity data is in one or more directories. Application-specific attributes of users and groups are stored in the Enterprise Directory.
- Application-specific entries are in the Application Directory. AppIDs and Enterprise Roles are stored in the Application Directory,

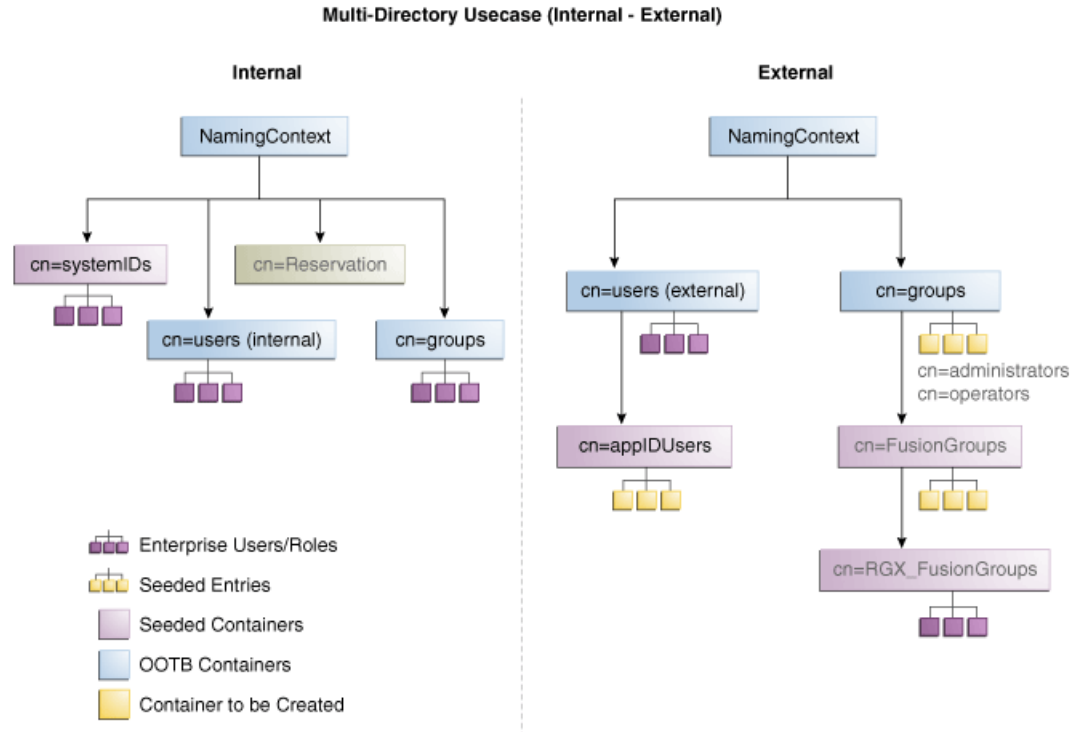
This section contains the following topics:

- [Section 7.3.1, "Directory Structure Overview for Distinct User and Group Populations in Multiple Directories"](#)
- [Section 7.3.2, "Configuring Oracle Virtual Directory Adapters for Distinct User and Group Populations in Multiple Directories"](#)
- [Section 7.3.3, "Creating a Global Plug-in"](#)

7.3.1 Directory Structure Overview for Distinct User and Group Populations in Multiple Directories

Figure 7-4 shows the directory structure in the two directories, listed here as internal and external. The containers `cn=appIDUsers`, `cn=FusionGroups`, and `cn=RGX_FusionGroups` are Fusion Applications-specific.

Figure 7-4 Directory Structure



Oracle Virtual Directory makes multiple directories look like a single DIT to a user or client application, as shown in Figure 7-5. The containers `cn=appIDUsers`, `cn=FusionGroups`, and `cn=RGX_FusionGroups` are Fusion Applications-specific.

Figure 7-5 Client View of the DIT

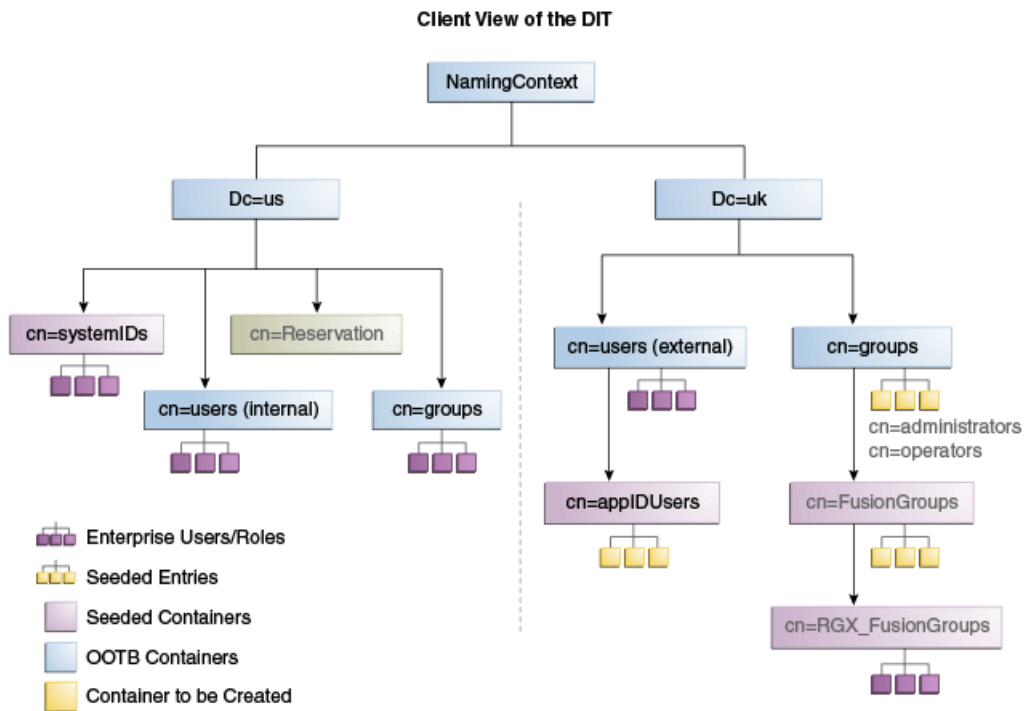
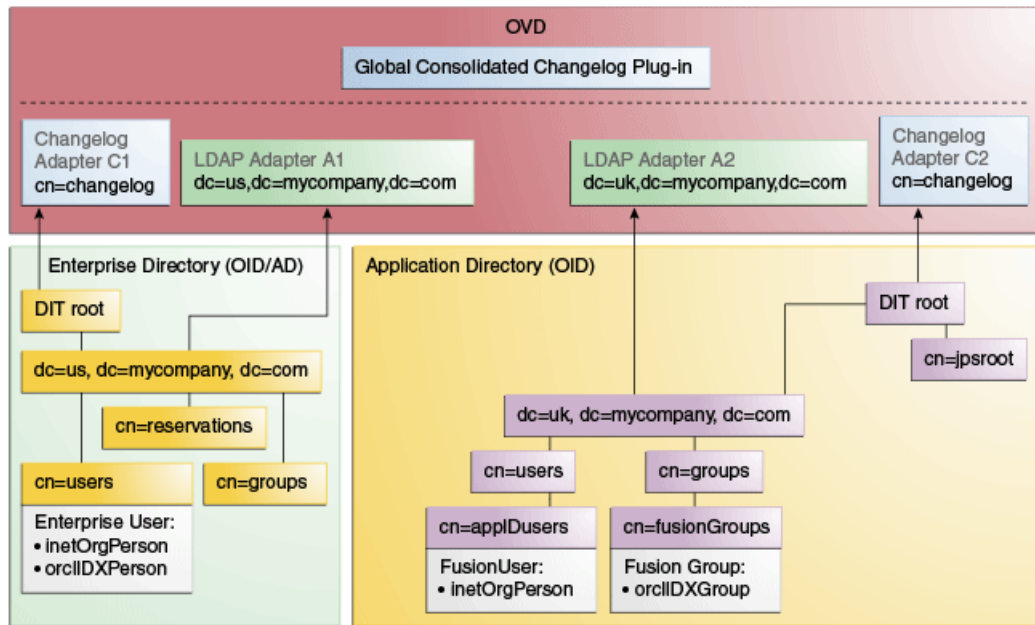


Figure 7-6 provides an overview of the adapter configuration. The classes `inetOrgPerson`, `orclIDXPerson`, and `orclIDXGroup` and the containers `cn=appIDUsers` and `cn=fusionGroups` are required only for Fusion Applications.

Figure 7-6 Configuration Overview



7.3.2 Configuring Oracle Virtual Directory Adapters for Distinct User and Group Populations in Multiple Directories

Create the user adapter on the Oracle Virtual Directory instances running on LDAPHOST1 and LDAPHOST2 individually, as described in the following sections

7.3.2.1 Create Enterprise Directory Adapters

Create Oracle Virtual Directory adapters for the Enterprise Directory. The type of adapter that is created will be dependent on whether or not the back end directory resides in Oracle Internet Directory or Active Directory.

You can use `idmconfigTool` to create the Oracle Virtual Directory User and Changelog adapters for Oracle Internet Directory and Active Directory.

See Also: [Section A.2, "Verifying Adapters for Distinct User and Group Populations in Multiple Directories by Using ODSM"](#) for instructions on viewing the adapters using Oracle Directory Services Manager.

Oracle Identity Manager requires adapters. It is highly recommended, though not mandatory, that you use Oracle Virtual Directory to connect to Oracle Internet Directory.

To create the adapters using `idmconfigTool`, perform the following tasks on IDMHOST1:

1. Set the environment variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME` and `ORACLE_HOME`.
Set `IDM_HOME` to `IDM_ORACLE_HOME`
Set `ORACLE_HOME` to `IAM_ORACLE_HOME`
2. Create a properties file for the OID or AD adapter you are configuring called `ovd1.props`, as follows:

Note: The `usecase.type:single` parameter is not supported for Active Directory through the `configOVD` option.

Oracle Internet Directory adapter properties file:

```
ovd.host:ldaphost1.mycompany.com
ovd.port:8899
ovd.binddn:cn=orcladmin
ovd.password:ovdpassword
ovd.oamenabled:true
ovd.ssl:true
ldap1.type:OID
ldap1.host:oididstore.mycompany.com
ldap1.port:3060
ldap1.binddn:cn=oimLDAP,cn=systemids,dc=mycompany,dc=com
ldap1.ssl:false
ldap1.base:dc=mycompany,dc=com
ldap1.ovd.base:dc=mycompany,dc=com
usecase.type:single
```

Active Directory adapter properties file:

```
ovd.host:ldaphost1.mycompany.com
ovd.port:8899
```

```

ovd.binddn:cn=orcladmin
ovd.password:ovdpassword
ovd.oamenabled:true
ovd.ssl:true
ldap1.type:AD
ldap1.host:adidstore.mycompany.com
ldap1.port:636
ldap1.binddn:cn=adminuser
ldap1.ssl:true
ldap1.base:dc=mycompany,dc=com
ldap1.ovd.base:dc=mycompany,dc=com
usecase.type: single

```

The following list contains the parameters used in the properties file and their descriptions.

- `ovd.host` is the host name of a server running Oracle Virtual Directory.
 - `ovd.port` is the https port used to access Oracle Virtual Directory.
 - `ovd.binddn` is the user DN you use to connect to Oracle Virtual Directory.
 - `ovd.password` is the password for the DN you use to connect to Oracle Virtual Directory.
 - `ovd.oamenabled` is set to `true` if you are using Oracle Access Management Access Manager, otherwise set to `false`.
`ovd.oamenabled` is always `true` in Fusion Applications deployments.
 - `ovd.ssl` is set to `true`, as you are using an https port.
 - `ldap1.type` is set to `OID` for the Oracle Internet Directory back end directory or set to `AD` for the Active Directory back end directory.
 - `ldap1.host` Back end directory host.
 - `ldap1.port` is the port used to communicate with the back end directory.
 - `ldap1.binddn` is the bind DN of the `oimLDAP` user.
 - `ldap1.password` is the password of the `oimLDAP` user
 - `ldap1.ssl` is set to `true` if you are using the back end's SSL connection, and otherwise set to `false`. This should always be set to `true` when an adapter is being created for AD.
 - `ldap1.base` is the base location in the directory tree.
 - `ldap1.ovd.base` is the mapped location in Oracle Virtual Directory.
 - `usecase.type` is set to `Single` when using a single directory type.
3. Configure the adapter by using the `idmConfigTool` command, which is located at:

```
IAM_ORACLE_HOME/idmtools/bin
```

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

```
IAM_ORACLE_HOME/idmtools/bin
```

The syntax of the command on Linux is:

```
idmConfigTool.sh -configOVD input_file=configfile [log_file=logfile]
```

The syntax on Windows is:

```
idmConfigTool.bat -configOVD input_file=configfile [log_file=logfile]
```

For example:

```
idmConfigTool.sh -configOVD input_file=ovd1.props
```

The command requires no input. The output looks like this:

```
The tool has completed its operation. Details have been logged to logfile
```

Run this command on each Oracle Virtual Directory host in your topology, with the appropriate value for `ovd.host` in the property file.

7.3.2.2 Create Application Directory Adapters

Create Oracle Virtual Directory adapters for the Application Directory. The back end directory for the application directory is always Oracle Internet Directory.

You can use `idmconfigTool` to create the Oracle Virtual Directory User and Changelog adapters for Oracle Internet Directory and Active Directory. Oracle Identity Manager requires adapters. It is highly recommended, though not mandatory, that you use Oracle Virtual Directory to connect to Oracle Internet Directory.

To do this, perform the following tasks on `IDMHOST1`:

1. Set the environment variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME` and `ORACLE_HOME`.
Set `IDM_HOME` to `IDM_ORACLE_HOME`
Set `ORACLE_HOME` to `IAM_ORACLE_HOME`
2. Create a properties file for the adapter you are configuring called `ovd1.props`. The contents of this file is as follows.

Oracle Internet Directory adapter properties file:

```
ovd.host:ldaphost1.mycompany.com
ovd.port:8899
ovd.binddn:cn=orcladmin
ovd.password:ovdpassword
ovd.oamenabled:true
ovd.ssl:true
ldap1.type:OID
ldap1.host:oididstore.mycompany.com
ldap1.port:3060
ldap1.binddn:cn=oimLDAP,cn=systemids,dc=mycompany,dc=com
ldap1.password:oidpassword
ldap1.ssl:false
ldap1.base:dc=mycompany,dc=com
ldap1.ovd.base:dc=mycompany,dc=com
usecase.type: single
```

The following list describes the parameters used in the properties file.

- `ovd.host` is the host name of a server running Oracle Virtual Directory.
- `ovd.port` is the https port used to access Oracle Virtual Directory.
- `ovd.binddn` is the user DN you use to connect to Oracle Virtual Directory.

- `ovd.password` is the password for the DN you use to connect to Oracle Virtual Directory.
 - `ovd.oamenabled` is set to `true` if you are using Oracle Access Management Access Manager, otherwise set to `false`.
`ovd.oamenabled` is always `true` in Fusion Applications deployments.
 - `ovd.ssl` is set to `true`, as you are using an `https` port.
 - `ldap1.type` is set to `OID` for the Oracle Internet Directory back end directory or set to `AD` for the Active Directory back end directory.
 - `ldap1.host` is the host on which back end directory is located. Use the load balancer name.
 - `ldap1.port` is the port used to communicate with the back end directory.
 - `ldap1.binddn` is the bind DN of the `oimLDAP` user.
 - `ldap1.password` is the password of the `oimLDAP` user
 - `ldap1.ssl` is set to `true` if you are using the back end's SSL connection, and otherwise set to `false`. This should always be set to `true` when an adapter is being created for AD.
 - `ldap1.base` is the base location in the directory tree.
 - `ldap1.ovd.base` is the mapped location in Oracle Virtual Directory.
 - `usecase.type` is set to `Single` when using a single directory type.
3. Configure the adapter by using the `idmConfigTool` command, which is located at:

`IAM_ORACLE_HOME/idmtools/bin`

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

`IAM_ORACLE_HOME/idmtools/bin`

The syntax of the command on Linux is:

```
idmConfigTool.sh -configOVD input_file=configfile [log_file=logfile]
```

The syntax on Windows is:

```
idmConfigTool.bat -configOVD input_file=configfile [log_file=logfile]
```

For example:

```
idmConfigTool.sh -configOVD input_file=ovd1.props
```

The command requires no input. The output looks like this:

```
The tool has completed its operation. Details have been logged to logfile
```

Run this command on each Oracle Virtual Directory host in your topology, with the appropriate value for `ovd.host` in the property file.

7.3.3 Creating a Global Plug-in

To create a Global Oracle Virtual Directory plug-in, proceed as follows:

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Create connections to each of the Oracle Virtual Directory instances running on LDAPHOST1 and LDAPHOST2, if they do not already exist.
3. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.
4. On the Home page, click the **Advanced** tab. The Advanced navigation tree appears.
5. Click the **+** next to **Global Plugins** in the left pane.
6. Click **Create Plugin**.
7. Create the Global Consolidated Changelog Plug-in as follows:

Enter the following values to create the Global Consolidated Plug-in:

- **Name:** Global Consolidated Changelog
- **Class:** Click **Select** then choose: **ConsolidatedChangelog**

Click **OK** when finished.

The environment is now ready to be configured to work with Oracle Virtual Directory as the Identity Store.

7.4 Additional Configuration Tasks

If you have previously integrated Oracle Identity Manager with a single directory and you are now reintegrating it with multiple directories, you must reset the changelog number for each of the incremental jobs to zero. The changelog numbers are repopulated on the next run.

Part V

Appendices

This part contains supplementary content to support the procedures in the book, and includes the following appendices:

- [Appendix A, "Verifying Adapters for Multiple Directory Identity Stores by Using ODSM"](#)
- [Appendix B, "The idm.conf File"](#)
- [Appendix C, "Integrating Oracle Adaptive Access Manager with Access Manager"](#)
- [Appendix D, "Using the idmConfigTool Command"](#)
- [Appendix E, "Enabling LDAP Synchronization in Oracle Identity Manager"](#)
- [Appendix F, "Configuring Oracle Virtual Directory for Integration with Oracle Access Management Access Manager"](#)

Verifying Adapters for Multiple Directory Identity Stores by Using ODSM

After you have configured your Oracle Virtual Directory adapters as described in Chapter 6, "Configuring an Identity Store with Multiple Directories," you can use ODSM to view the adapters for troubleshooting purposes. This chapter explains how.

This appendix contains the following sections:

- [Section A.1, "Verifying Oracle Virtual Directory Adapters for Split Profile by Using ODSM"](#)
- [Section A.2, "Verifying Adapters for Distinct User and Group Populations in Multiple Directories by Using ODSM"](#)

A.1 Verifying Oracle Virtual Directory Adapters for Split Profile by Using ODSM

This section describes how to validate the adapters created in [Chapter 7.2.5, "Configuring Oracle Virtual Directory Adapters for Split Profile."](#)

This section contains the following topics:

- [Section A.1.1, "Verifying User Adapter for Active Directory Server"](#)
- [Section A.1.2, "Verifying Shadowjoiner User Adapter"](#)
- [Section A.1.3, "Verifying JoinView Adapter"](#)
- [Section A.1.4, "Verifying User/Role Adapter for Oracle Internet Directory"](#)
- [Section A.1.5, "Verifying Changelog adapter for Active Directory Server"](#)
- [Section A.1.6, "Verifying Changelog Adapter for Oracle Internet Directory"](#)
- [Section A.1.7, "Configuring a Global Consolidated Changelog Plug-in"](#)
- [Section A.1.8, "Validate Oracle Virtual Directory Changelog"](#)

A.1.1 Verifying User Adapter for Active Directory Server

Verify the following adapter and plug-ins for Active Directory:

Follow these steps to verify the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM). The URL is of the form: `http://admin.mycompany.com/odsm`.

2. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.
3. On the Home page, click the **Adapter** tab.
4. Click **user_AD1** adapter.
5. Verify that the User Adapter routing is configured correctly:
 - a. **Visibility** must be set to internal.
 - b. **Bind Support** must be set to enable.
6. Verify the User Adapter User Management Plug-in as follows:
 - a. Select the **User Adapter**.
 - b. Click the **Plug-ins** tab.
 - c. Click the **User Management** Plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
 - d. Verify that the plug-in parameters are as follows:

Parameter	Value	Default
directoryType	activedirectory	Yes
exclusionMapping	orclappiduser,uid=samaccountname	
mapAttribute	orclguid=objectGuid	
mapAttribute	uniquemember=member	
addAttribute	user,samaccountname=%uid%,%orcls hortuid%	
mapAttribute	mail=userPrincipalName	
mapAttribute	ntgroupstype=groupstype	
mapObjectclass	groupofUniqueNames=group	
mapObjectclass	orclidperson=user	
pwdMaxFailure	10	Yes
oamEnabled	True ¹	
mapObjectClass	inetorgperson=user	Yes
mapPassword	True	Yes
oimLanguages	Comma separated list of language codes, such as en, fr, ja	

¹ Set oamEnabled to true only if you are using Oracle Access Management Access Manager.

A.1.2 Verifying Shadowjoiner User Adapter

Follow these steps to verify the ShadowJoiner Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to Oracle Virtual Directory.
3. On the Home page, click the **Adapter** tab.

4. Click the **Shadow4AD1** Adapter.
5. Ensure that User Adapter routing as is configured correctly:
 - a. **Visibility** must be set to internal.
 - b. **Bind Support** must be set to enable.
6. Verify the User Adapter as follows:
 - a. Select the User Adapter.
 - b. Click the **Plug-ins** tab.
 - c. Click the **User Management** Plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
 - d. Verify that the parameters are as follows:

Parameter	Value	Default
directoryType	oid	Yes
pwdMaxFailure	10	Yes
oamEnabled	true	
mapObjectclass	container=orclCont ainer	Yes
oimDateFormat	yyyyMMddHHmms s'z'	

A.1.3 Verifying JoinView Adapter

Follow these steps to verify the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to the Oracle Directory Services Manager (ODSM) page.
2. Connect to Oracle Virtual Directory.
3. On the Home page, click the **Adapter** tab.
4. Click the JoinView adapter.
5. Verify the Adapter as follows
 - a. Click **Joined Adapter** in the adapter tree. It should exist
 - b. Click **OK**.

A.1.4 Verifying User/Role Adapter for Oracle Internet Directory

Follow these steps to verify the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to Oracle Virtual Directory.
3. On the Home page, click the **Adapter** tab.
4. Click User Adapter.
5. Verify the plug-in as follows:
 - a. Select the User Adapter.

- b. Click the **Plug-ins** tab.
- c. Click the **User Management** Plug-in in the plug-ins table, then click **Edit**. The plug-in editing window appears.
- d. Verify that the parameters are as follows:

Parameter	Value	Default
directoryType	oid	Yes
pwdMaxFailure	10	Yes
oamEnabled	true	
mapObjectclass	container=orclCont ainer	Yes
oimDateFormat	yyyyMMddHHmms s'z'	

- e. Click **OK**.

A.1.5 Verifying Changelog adapter for Active Directory Server

Follow these steps to verify the Changelog Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to Oracle Virtual Directory.
3. On the Home page, click the **Adapter** tab.
4. Click the changelog_AD1 adapter.
5. Verify the plug-in as follows.
 - a. Select the Changelog Adapter.
 - b. Click the **Plug-ins** tab.
 - c. In the Deployed Plus-ins table, click the **changelog** plug-in, then click "Edit" in the plug-ins table. The plug-in editing window appears.
 - d. Verify that the parameter values are as follows:

Parameter	Value
directoryType	activedirectory
mapAttribute	targetGUID=objectGUID
requiredAttribute	samaccountname
sizeLimit	1000
targetDNFilter	cn=users,dc=idm,dc=ad,dc=com The users container in Active Directory
mapUserState	true
oamEnabled	true
virtualDITAdapter Name	user_J1;user_AD1

A.1.6 Verifying Changelog Adapter for Oracle Internet Directory

To use the changelog adapter, you must first enable changelog on the connected directory. To test whether the directory is changelog enabled, type:

```
ldapsearch -h directory_host -p ldap_port -D bind_dn -q -b '' -s base
'objectclass=*' lastchangenumber
```

for example:

```
ldapsearch -h ldaphost1 -p 389 -D "cn=orcladmin" -q -b '' -s base 'objectclass=*'
lastchangenumber
```

If you see `lastchangenumber` with a value, it is enabled. If it is not enabled, enable it as described in the Enabling and Disabling Changelog Generation by Using the Command Line section of *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

Follow these steps to verify the Changelog Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to an Oracle Virtual Directory instance.
3. On the Home page, click the **Adapter** tab.
4. Click the Changelog Adapter.
5. Verify the plug-in as follow.
 - a. Select the Changelog Adapter.
 - b. Click the **Plug-ins** tab.
 - c. In the Deployed Plug-ins table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
 - d. Verify that the parameter values are as follows:

Parameter	Value
directoryType	oid
mapAttribute	targetGUID=orclguid
requiredAttribute	orclGUID
modifierDNFilter	cn=orcladmin
sizeLimit	1000
targetDNFilter	dc=mycompany, dc=com
targetDNFilter	cn=shadowentries
mapUserState	true
oamEnabled	true
virtualDITAdapter Name	user_J1;shadow4AD1
virtualDITAdapter Name	User Adapter (The name of the User adapter's name)

A.1.7 Configuring a Global Consolidated Changelog Plug-in

Verify the global level consolidated changelog plug-in as follows

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to an Oracle Virtual Directory instance.
3. On the Home page, click the **Advanced** tab. The Advanced navigation tree appears.
4. Expand **Global Plugins**
5. Click the **ConsolidatedChglogPlugin**. The plug-in editing window appears.

A.1.8 Validate Oracle Virtual Directory Changelog

Run the following command to validate that the changelog adapter is working:

```
$IDM_ORACLE_HOME/bin/ldapsearch -p 6501 -D cn=orcladmin -q -b 'cn=changelog' -s  
base 'objectclass=*' lastchangenumber
```

The command should return a changelog result, such as:

```
Please enter bind password:  
cn=Changelog  
lastChangeNumber=changelog_OID:190048;changelog_AD1:363878
```

If `ldapsearch` does not return a changelog result, double check the changelog adapter configuration.

A.2 Verifying Adapters for Distinct User and Group Populations in Multiple Directories by Using ODSM

This section describes how to view the adapters created in [Section 7.3.2, "Configuring Oracle Virtual Directory Adapters for Distinct User and Group Populations in Multiple Directories."](#)

Verify the user adapter on the Oracle Virtual Directory instances running on LDAPHOST1 and LDAPHOST2 individually. Follow these steps to verify the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager:

1. If they are not already running, start the Administration Server and the WLS_ODSM Managed Servers.
2. In a web browser, go to Oracle Directory Services Manager (ODSM) at:
`http://admin.mycompany.com/odsm`
3. Verify connections to each of the Oracle Virtual Directory instances running on LDAPHOST1 and LDAPHOST2, if they do not already exist.
4. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.
5. On the Home page, click the **Adapter** tab.
6. Click the name of each adapter. Verify that it has the parameters shown in the following tables.

This section contains the following topics:

- [Section A.2.1, "User/Role Adapter A1"](#)
- [Section A.2.2, "User/Role Adapter A2"](#)

- [Section A.2.3, "Changelog Adapter C1"](#)
- [Section A.2.4, "Changelog Adapter for Active Directory"](#)
- [Section A.2.5, "Changelog Adapter C2"](#)
- [Section A.2.6, "Verifying Oracle Virtual Directory Global Plug-in"](#)
- [Section A.2.7, "Configuring a Global Consolidated Changelog Plug-in"](#)

A.2.1 User/Role Adapter A1

Verify the plug-in of the User/Role Adapter A1, as follows:

1. Select the OIM User Adapter.
2. Click the **Plug-ins** tab.
3. Click the **User Management** Plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
4. Verify that the parameter values are as follows:

Parameter	Value	Default
directoryType	activedirectory	Yes
exclusionMapping	orclappiduser,uid=samaccountname	
mapAttribute	orclguid=objectGuid	
mapAttribute	uniquemember=member	
addAttribute	user,samaccountname=%uid%,%orcls hortuid%	
mapAttribute	mail=userPrincipalName	
mapAttribute	ntgroupstype=groupstype	
mapObjectclass	groupofUniqueNames=group	
mapObjectclass	orclidxperson=user	
pwdMaxFailure	10	Yes
oamEnabled	True ¹	
mapObjectClass	inetorgperson=user	Yes
mapPassword	True	Yes
oimLanguages	Comma separated list of language codes, such as en, fr, ja	

¹ Set oamEnabled to true only if you are using Oracle Access Management Access Manager.

A.2.2 User/Role Adapter A2

Verify the plug-in of the User/Role Adapter A2 as follows:

1. Select the User Adapter.
2. Click the **Plug-ins** tab.
3. Click the **User Management** Plug-in in the plug-ins table, then click **Edit**. The plug-in editing window appears.
4. Verify that the parameter values are as follows:

Parameter	Value	Default
directoryType	oid	Yes
pwdMaxFailure	10	Yes
oamEnabled	true ¹	
mapObjectclass	container=orclContainer	Yes

¹ Set oamEnabled to true only if you are using Oracle Access Management Access Manager.

A.2.3 Changelog Adapter C1

To verify the Changelog Adapter C1 plug-in, follow these steps:

1. Select the OIM changelog adapter **Changelog_Adapter_C1**.
2. Click the **Plug-ins** tab.
3. In the **Deployed Plus-ins** table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
4. In the **Parameters** table, verify that the values are as shown.

Table A-1 Values in Parameters Table

Parameter	Value	Comments
modifierDNFilter	A bind DN that has administrative rights on the directory server, in the format: "!(modifiersname=cn=BindDN)" For example: "!(modifiersname=cn=orcladmin,cn=systemids,dc=mycompany,dc=com) "	Create
sizeLimit	1000	Create
targetDNFilter	dc=us,dc=mycompany,dc=com	Create
mapUserState	true	Update
oamEnabled	true	Update
virtualDITAdapterName	The adapter name of User/Role Adapter A1: User_Adapter_A1	Create

A.2.4 Changelog Adapter for Active Directory

Verify the plug-in as follows.

1. Select the OIM Changelog Adapter.
2. Click the **Plug-ins** tab.
3. In the Deployed Plus-ins table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
4. In the Parameters table, verify that the parameters are as follows:

Parameter	Value
directoryType	activedirectory

Parameter	Value
mapAttribute	targetGUID=objectGUID
requiredAttribute	samaccountname
sizeLimit	1000
targetDNFilter	dc=mycompany, dc=com Search base from which reconciliation must happen. This value must be the same as the LDAP SearchDN that is specified during Oracle Identity Manager installation.
mapUserState	true
oamEnabled	true ¹
virtualDITAdapter Name	The name of the User adapter's name

¹ Set oamEnabled to true only if you are using Oracle Access Management Access Manager.

Note: `virtualDITAdapterName` identifies the corresponding user profile adapter name. For example, in a single-directory deployment, you can set this parameter value to `User Adapter`, which is the user adapter name. In a split-user profile scenario, you can set this parameter to `J1;A2`, where `J1` is the JoinView adapter name, and `A2` is the corresponding user adapter in the `J1`.

A.2.5 Changelog Adapter C2

Verify the plug-in as follows:

1. Select the OIM changelog adapter **Changelog_Adapter_C2**.
2. Click the **Plug-ins** tab.
3. In the **Deployed Plus-ins** table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
4. In the **Parameters** table, verify that the parameters are as follows:

Table A-2 Values in Parameters Table

Parameter	Value	Comments
modifierDNFilter	A bind DN that has administrative rights on the directory server, in the format: "! (modifiersname=cn=BindDN)" For example: "! (modifiersname=cn=orcladmin, dc=mycompany, dc=com) "	Create
sizeLimit	1000	Create
targetDNFilter	dc=uk, dc=mycompany, dc=com	Create
mapUserState	true	Update
oamEnabled	true	Update

Table A–2 (Cont.) Values in Parameters Table

Parameter	Value	Comments
virtualDITAdapterName	The adapter name of User/Role adapter A2: User_Adapter_A2	Create

A.2.6 Verifying Oracle Virtual Directory Global Plug-in

To verify the Global Oracle Virtual Directory plug-in, proceed as follows

1. In a web browser, go to Oracle Directory Services Manager (ODSM) at:
<http://admin.mycompany.com/odsm>
2. Verify connections to each of the Oracle Virtual Directory instances running on LDAPHOST1 and LDAPHOST2, if they do not already exist.
3. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.
4. On the Home page, click the **Adapter** tab.
5. Click the **Plug-ins** tab.
6. Verify that the Global Consolidated Changelog Plug-in exists.
Click **OK** when finished.

A.2.7 Configuring a Global Consolidated Changelog Plug-in

Verify the global level consolidated changelog plug-in as follows

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to an Oracle Virtual Directory instance.
3. On the Home page, click the **Advanced** tab. The Advanced navigation tree appears.
4. Expand **Global Plugins**
5. Click the **ConsolidatedChglogPlugin**. The plug-in editing window appears.

The idm.conf File

This appendix explains the purpose and usage of the `idm.conf` file for applications with a web interface.

This appendix contains the following topics:

- [About the idm.conf File](#)
- [Example idm.conf File](#)

B.1 About the idm.conf File

In the Oracle Fusion Middleware environment, the highest level configuration file at the web tier is `httpd.conf`. This file configures Oracle HTTP Server, which processes the web transactions that use the `http` protocol. Oracle HTTP Server processes each incoming request and determines its routing based on the URL from which the request originates and the resource to be accessed.

Additional configuration files are specified in the `httpd.conf` file by means of the Apache HTTP Server's `Include` directive in an `IfModule` block.

Identity management applications in particular make use of the `idm.conf` configuration file, which is a template that administrators can modify to indicate how incoming requests for protected applications must be handled.

The `idm.conf` configuration file is divided into four parts, each addressing a distinct security area or zone. [Table B-1](#) lists the zones:

Table B-1 Zones in the `idm.conf` File

Zone	Type	Details
1	Default Access	Section B.1.1
2	External Access	Section B.1.2
3	Internal Services	Section B.1.3
4	Administrative Services	Section B.1.4

When updating the `idm.conf` file, be sure to edit only the zone definition applicable to your requirements.

B.1.1 The Default Access Zone

This zone is the default Oracle HTTP Server endpoint for all inbound traffic. The protocol is `http` and the context root is in the format `authohs.example.com:7777`.

B.1.2 The External Access Zone

This zone is the load-balancer (LBR) external end user endpoint. The protocol is https and the context root is in the format `sso.example.com:443`.

B.1.3 The Internal Services Zone

This zone is the LBR internal endpoint for applications. The protocol is http and the context root is in the format `idminternal.example.com:7777`.

B.1.4 The Administrative Services Zone

This zone is the LBR internal endpoint for administrative services. The protocol is https and the context root is in the format `admin.example.com:443`.

B.2 Example idm.conf File

The following sample shows the layout and different zones of the idm.conf file:

```
NameVirtualHost *:7777

## Default Access
## AUTHOHS.EXAMPLE.COM

<VirtualHost *:7777>
# ServerName http://authohs.example.com:7777 (replace the ServerName below with
the actual host:port)
    ServerName http://authohs.us.example.com:7777
    RewriteEngine On
    RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end_
url=/console" [R]
    RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em"
[R]
    RewriteRule ^/FSMIdentity/faces/pages/Self.jspx "/oim" [R]
    RewriteRule ^/FSMIdentity/faces/pages/pwdmgmt.jspx
"/admin/faces/pages/pwdmgmt.jspx" [R]
    RewriteOptions inherit
    UseCanonicalName On

# Admin Server and EM

    <Location /console>
        SetHandler weblogic-handler
        WebLogicHost us.example.com
        WeblogicPort 17001
    </Location>

    <Location /consolehelp>
        SetHandler weblogic-handler
        WebLogicHost us.example.com
        WeblogicPort 17001
    </Location>

    <Location /em>
        SetHandler weblogic-handler
        WebLogicHost us.example.com
        WeblogicPort 17001
    </Location>
```

```
# FA service

  <Location /fusion_apps>
    SetHandler weblogic-handler
    WebLogicHost us.example.com
    WebLogicPort 14100
  </Location>

#ODSM Related entries
  <Location /odsm>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WebLogicHost oidfa.us.example.com
    WeblogicPort 7005
  </Location>

# OAM Related Entries

  <Location /oamconsole>
    SetHandler weblogic-handler
    WebLogicHost us.example.com
    WebLogicPort 17001
  </Location>

  <Location /oam>
    SetHandler weblogic-handler
    WebLogicHost us.example.com
    WebLogicPort 14100
  </Location>

# OIM Related Entries

# oim identity self service console
<Location /identity>
  SetHandler weblogic-handler
  WLProxySSL ON
  WLProxySSLPassThrough ON
  WLCookieName oimjsessionid
  WebLogicHost us.example.com
  WeblogicPort 14000

  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# oim identity system administration console
<Location /sysadmin>
  SetHandler weblogic-handler
  WLProxySSL ON
  WLProxySSLPassThrough ON
  WLCookieName oimjsessionid
  WebLogicHost us.example.com
  WeblogicPort 14000

  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# oim identity advanced administration console - Legacy 11gR1 webapp
<Location /oim>
  SetHandler weblogic-handler
```

```

        WLProxySSL ON
        WLProxySSLPassThrough ON
        WLCookieName oimjsessionid
        WebLogicHost us.example.com
        WeblogicPort 14000
        WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# xlWebApp - Legacy 9.x webapp (struts based)
    <Location /xlWebApp>
        SetHandler weblogic-handler
        WLCookieName oimjsessionid
        WebLogicHost us.example.com
        WeblogicPort 14000

        WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# Nexaweb WebApp - used for workflow designer and DM
    <Location /Nexaweb>
        SetHandler weblogic-handler
        WLCookieName oimjsessionid
        WebLogicHost us.example.com
        WeblogicPort 14000

        WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# spml xsd profile
    <Location /spml-xsd>
        SetHandler weblogic-handler
        WLCookieName oimjsessionid
        WebLogicHost us.example.com
        WeblogicPort 14000

        WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# used for FA Callback service.
    <Location /callbackResponseService>
        SetHandler weblogic-handler
        WLCookieName oimjsessionid
        WebLogicHost us.example.com
        WeblogicPort 14000

        WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# Role-SOD profile
    <Location /role-sod>
        SetHandler weblogic-handler
        WLCookieName oimjsessionid
        WebLogicHost us.example.com
        WeblogicPort 14000

        WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# SOA Callback webservice for SOD - Provide the SOA Managed Server Ports
    <Location /sodcheck>

```

```

        SetHandler weblogic-handler
        WLCookieName oimjsessionid
        WebLogicHost us.example.com
        WeblogicPort 8001

        WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# Callback webservice for SOA. SOA calls this when a request is approved/rejected
# Provide the SOA Managed Server Port
    <Location /workflowservice>
        SetHandler weblogic-handler
        WLCookieName oimjsessionid
        WebLogicHost us.example.com
        WeblogicPort 14000

        WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# HTTP client service
    <Location /HTTPClnt>
        SetHandler weblogic-handler
        WLCookieName oimjsessionid
        WebLogicHost us.example.com
        WeblogicPort 14000

        WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# OIF Related Entries

    <Location /fed>
        SetHandler weblogic-handler
        WebLogicHost us.example.com
        WebLogicPort 7499
    </Location>

</VirtualHost>

## External Access
## SSO.EXAMPLE.COM

<VirtualHost *:7777>
# ServerName https://sso.example.com:443 (replace the ServerName below with the
actual host:port)
    ServerName https://sso.example.com:443
    RewriteEngine On
    RewriteRule ^/console/jsp/common/logout.jsp "/oamssso/logout.html?end_
url=/console" [R]
    RewriteRule ^/em/targetauth/emaslogout.jsp "/oamssso/logout.html?end_url=/em"
[R]
    RewriteRule ^/FSMIdentity/faces/pages/Self.jspx "/oim" [R]
    RewriteRule ^/FSMIdentity/faces/pages/pwdmgmt.jspx
"/admin/faces/pages/pwdmgmt.jspx" [R]
    RewriteOptions inherit
    UseCanonicalName On

# FA service
    <Location /fusion_apps>

```

```

        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON
        WebLogicHost us.example.com
        WebLogicPort 14100
    </Location>

# OAM Related Entries

    <Location /oam>
        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON
        WebLogicHost us.example.com
        WebLogicPort 14100
    </Location>

# OIM Related Entries

# oim identity self service console
<Location /identity>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid
    WebLogicHost us.example.com
    WeblogicPort 14000

    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# oim identity system administration console
<Location /sysadmin>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid
    WebLogicHost us.example.com
    WeblogicPort 14000

    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# oim identity advanced administration console - Legacy 11gR1 webapp
<Location /oim>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid
    WebLogicHost us.example.com
    WeblogicPort 14000
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# xlWebApp - Legacy 9.x webapp (struts based)
<Location /xlWebApp>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid

```

```
WebLogicHost us.example.com
WeblogicPort 14000

WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# Nexaweb WebApp - used for workflow designer and DM
<Location /Nexaweb>
  SetHandler weblogic-handler
  WLProxySSL ON
  WLProxySSLPassThrough ON
  WLCookieName oimjsessionid
  WebLogicHost us.example.com
  WeblogicPort 14000

  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# spml xsd profile
<Location /spml-xsd>
  SetHandler weblogic-handler
  WLProxySSL ON
  WLProxySSLPassThrough ON
  WLCookieName oimjsessionid
  WebLogicHost us.example.com
  WeblogicPort 14000

  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# used for FA Callback service.
<Location /callbackResponseService>
  SetHandler weblogic-handler
  WLProxySSL ON
  WLProxySSLPassThrough ON
  WLCookieName oimjsessionid
  WebLogicHost us.example.com
  WeblogicPort 14000

  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# OIF Related Entries
<Location /fed>
  SetHandler weblogic-handler
  WLProxySSL ON
  WLProxySSLPassThrough ON
  WebLogicHost weblogic-host.example.com
  WeblogicPort 7499
</Location>

</VirtualHost>

## IDM Internal services for FA
## IDMINTERNAL.EXAMPLE.COM

<VirtualHost *:7777>
# ServerName http://idminternal.example.com:7777 (replace the ServerName below
with the actual host:port)
  ServerName http://idminternal.example.com:7777
```

```

RewriteEngine On
RewriteRule ^/console/jsp/common/logout.jsp "/oamssso/logout.html?end_
url=/console" [R]
RewriteRule ^/em/targetauth/emaslogout.jsp "/oamssso/logout.html?end_url=/em"
[R]
RewriteRule ^/FSMIdentity/faces/pages/Self.jspx "/oim" [R]
RewriteRule ^/FSMIdentity/faces/pages/pwdmgmt.jspx
"/admin/faces/pages/pwdmgmt.jspx" [R]
RewriteOptions inherit
UseCanonicalName On

# FA service
<Location /fusion_apps>
    SetHandler weblogic-handler
    WebLogicHost us.example.com
    WebLogicPort 14100
</Location>

# OAM Related Entries

<Location /oam>
    SetHandler weblogic-handler
    WebLogicHost us.example.com
    WebLogicPort 14100
</Location>

# OIM Related Entries

# oim identity self service console
<Location /identity>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid
    WebLogicHost us.example.com
    WeblogicPort 14000

    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# oim identity system administration console
<Location /sysadmin>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid
    WebLogicHost us.example.com
    WeblogicPort 14000

    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# oim identity advanced administration console - Legacy 11gR1 webapp
<Location /oim>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid
    WebLogicHost us.example.com

```



```
    WeblogicPort 14000
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
  </Location>

# xlWebApp - Legacy 9.x webapp (struts based)
<Location /xlWebApp>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicHost us.example.com
  WeblogicPort 14000

  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# Nexaweb WebApp - used for workflow designer and DM
<Location /Nexaweb>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicHost us.example.com
  WeblogicPort 14000

  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# spml xsd profile
<Location /spml-xsd>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicHost us.example.com
  WeblogicPort 14000

  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# used for FA Callback service.
<Location /callbackResponseService>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicHost us.example.com
  WeblogicPort 14000

  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# Role-SOD profile
<Location /role-sod>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicHost us.example.com
  WeblogicPort 14000

  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# SOA Callback webservice for SOD - Provide the SOA Managed Server Ports
<Location /sodcheck>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicHost us.example.com
  WeblogicPort 8001
```

```

        WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# Callback webservice for SOA. SOA calls this when a request is approved/rejected
# Provide the SOA Managed Server Port
    <Location /workflowservice>
        SetHandler weblogic-handler
        WLCookieName oimjsessionid
        WebLogicHost us.example.com
        WeblogicPort 14000

        WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# HTTP client service
    <Location /HTTPClnt>
        SetHandler weblogic-handler
        WLCookieName oimjsessionid
        WebLogicHost us.example.com
        WeblogicPort 14000

        WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
    </Location>

# OIF Related Entries

    <Location /fed>
        SetHandler weblogic-handler
        WebLogicHost us.example.com
        WebLogicPort 7499
    </Location>

</VirtualHost>

## IDM Admin services for FA
## ADMIN.EXAMPLE.COM

<VirtualHost *:7777>
# ServerName https://admin.example.com:443 (replace the ServerName below with the
actual host:port)
    ServerName https://admin.example.com:443
    RewriteEngine On
    RewriteRule ^/console/jsp/common/logout.jsp "/oamssso/logout.html?end_
url=/console" [R]
    RewriteRule ^/em/targetauth/emaslogout.jsp "/oamssso/logout.html?end_url=/em"
[R]
    RewriteRule ^/FSMIdentity/faces/pages/Self.jspx "/oim" [R]
    RewriteRule ^/FSMIdentity/faces/pages/pwdmgmt.jspx
"/admin/faces/pages/pwdmgmt.jspx" [R]
    RewriteOptions inherit
    UseCanonicalName On

# Admin Server and EM

    <Location /console>
        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON

```

```
        WebLogicHost us.example.com
        WeblogicPort 17001
    </Location>

    <Location /consolehelp>
        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON
        WebLogicHost us.example.com
        WeblogicPort 17001
    </Location>

    <Location /em>
        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON
        WebLogicHost us.example.com
        WeblogicPort 17001
    </Location>

#ODSM Related entries
    <Location /odsm>
        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON
        WebLogicHost oidfa.us.example.com
        WeblogicPort 7005
    </Location>

# OAM Related Entries

    <Location /oamconsole>
        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON
        WebLogicHost us.example.com
        WebLogicPort 17001
    </Location>

# OIM Related Entries

# oim identity self service console
<Location /identity>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid
    WebLogicHost us.example.com
    WeblogicPort 14000

    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# oim identity system administration console
<Location /sysadmin>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid
```

```

    WebLogicHost us.example.com
    WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# oim identity advanced administration console - Legacy 11gR1 webapp
<Location /oim>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid
    WebLogicHost us.example.com
    WeblogicPort 14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# xlWebApp - Legacy 9.x webapp (struts based)
<Location /xlWebApp>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid
    WebLogicHost us.example.com
    WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# Nexaweb WebApp - used for workflow designer and DM
<Location /Nexaweb>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid
    WebLogicHost us.example.com
    WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# HTTP client service
<Location /HTTPClnt>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WLCookieName oimjsessionid
    WebLogicHost us.example.com
    WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>

# OIF Related Entries
<Location /fed>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WebLogicHost weblogic-host.example.com

```

```
    WebLogicPort 7499
  </Location>

</VirtualHost>
```

Integrating Oracle Adaptive Access Manager with Access Manager

Integrating Oracle Adaptive Access Manager (OAAM) with Oracle Access Management Access Manager (Access Manager) enables fine control over the authentication process and provides full capabilities of pre- and post-authentication checking against Oracle Adaptive Access Manager policies.

This chapter provides step-by-step instructions for integrating Access Manager with Oracle Adaptive Access Manager to secure resources via risk-based authentication. The exact steps can vary depending on your specific deployment. Adapt information as required for your environment.

The integration instructions assume Identity Management components have been configured on separate WebLogic domains, as discussed in "[Basic Integration Topology](#)." For prerequisite and detailed information on how the components were installed and configured in this example integration, see *Installation Guide for Oracle Identity and Access Management*.

If you are deploying Oracle Identity Management components in an enterprise integration topology, as discussed in "[The Enterprise Integration Topology](#)," see *Enterprise Deployment Guide for Oracle Identity and Access Management* for implementation procedures. If you are planning to design and deploy a high availability environment for Access Manager and Oracle Adaptive Access Manager, see *High Availability Guide* for concepts and configuration steps.

This appendix contains these sections:

- [About Access Manager and Oracle Adaptive Access Manager Integration](#)
- [Definitions, Acronyms, and Abbreviations](#)
- [OAAM Basic Integration with Access Manager](#)
- [OAAM Advanced Integration with Access Manager](#)
- [Access Manager and OAAM TAP Integration with DCC WebGate Using Tunneling](#)
- [Other Access Manager and OAAM Integration Configuration Tasks](#)
- [Resource Protection Scenario](#)
- [Troubleshooting Common Problems](#)

Note: Integration of Oracle Identity Manager provides additional features related to password collection. For information, see [Chapter 3, "Integrating Access Manager, OAAM, and OIM"](#).

C.1 About Access Manager and Oracle Adaptive Access Manager Integration

Oracle Access Management Access Manager (Access Manager) provides the core functionality of Web Single Sign On (SSO), authentication, authorization, centralized policy administration and agent management, real-time session management and auditing.

Oracle Adaptive Access Manager 11g safeguards vital online business applications with strong yet easily deployed risk-based authentication, anti-phishing, and anti-malware capabilities.

This integration scenario enables you to control access to resources with Access Manager and provide strong multi-factor authentication and advanced real-time fraud prevention with Oracle Adaptive Access Manager. Advanced login security includes the virtual authentication devices, device fingerprinting, real-time risk analysis, and risk-based challenge.

You can integrate Oracle Adaptive Access Manager with Access Manager in one of two ways:

- OAAM Basic
- OAAM Advanced using TAP

For more information about the scenarios that are supported by each deployment, and the flow that achieves each scenario see, [Section 1.5, "Common Integration Scenarios"](#).

Note: Oracle Access Management Access Manager and Oracle Adaptive Access Manager integrations using OAAMBasic and OAAMAdvanced authentication schemes are deprecated starting with 11.1.2.2 and will be desupported in 12.1.4 and future releases. The recommendation is to use the Oracle Access Management Access Manager and Oracle Adaptive Access Manager integration using Trusted Authentication Protocol (TAP) instead of OAAMBasic and OAAMAdvanced (without TAP) integrations.

[Table C-1](#) summarizes the Access Manager and Oracle Adaptive Access Manager integrations types.

Table C-1 Types of Access Manager and Oracle Adaptive Access Manager Integration

Details	OAAM Basic	OAAM Advanced	OAAM Advanced Using TAP
Available	11.1.1.3.0 to 12.1.4	11.1.1.3.0 and prior to 11.1.1.5	11.1.1.5.0 and above OAAM Advanced using TAP is the supported OAAM Advanced integration with Access Manager.
Access Manager Users	For Access Manager users who want to add login security, including Knowledge Based Authentication (KBA).	For Access Manager users who want advanced features and customizations beyond that available with OAAM Basic.	For Access Manager users who want advanced features and customizations beyond that available with OAAM Basic. This option includes Step Authentication, which OAAM Advanced (without TAP) does not offer.
Features	<p>Authentication schemes, device fingerprinting, risk analysis, KBA challenge mechanisms</p> <p>KBA is the only challenge mechanism available in this integration.</p> <p>Libraries and configuration interface for different flows (challenge, registration, and other flows). Many of the login security use cases available from Oracle Adaptive Access Manager</p>	<p>Authentication schemes, device fingerprinting, risk analysis, KBA challenge mechanisms</p> <p>Advanced features and extensibility such as OTP Anywhere, challenge processor framework, shared library framework, and secure self-service password management flows</p> <p>OAAM can also be integrated with third party single sign-on products via systems integrators if required.</p>	<p>Authentication schemes, device fingerprinting, risk analysis, KBA challenge mechanisms, and additional advanced security access features, such as Step Up Authentication</p> <p>Advanced features and extensibility such as OTP Anywhere, challenge processor framework, shared library framework, and secure self-service password management flows</p> <p>OAAM can also be integrated with third party single sign-on products via systems integrators if required.</p>
Deployment	<p>Native integration</p> <ul style="list-style-type: none"> ■ OAM Managed Server along with OAAM Admin Server in a domain ■ OAAM libraries are bundled with the OAM Server ■ Integration with OAAM through extension libraries <p>OAAM Admin Server is required.</p> <p>OAAM Managed Server is not needed in this deployment.</p> <p>KBA is the only challenge mechanism available in this integration.</p> <p>The functionality is accessed through native OAAM calls.</p>	<p>Integration via redirects and APIs</p> <p>OAAM Advanced requires full deployment of OAAM Admin and OAAM Managed Servers.</p> <p>Leverages the Java Oracle Access Protocol (OAP) library.</p>	<p>OAAM Advanced using TAP requires full deployment OAAM Admin and OAAM Managed Servers.</p> <p>Leverages the Java Oracle Access Protocol (OAP) library.</p>
OAAM Database	Required	Required	Required

Table C-1 (Cont.) Types of Access Manager and Oracle Adaptive Access Manager Integration

Details	OAAM Basic	OAAM Advanced	OAAM Advanced Using TAP
Supported Agents	10g WebGate and Single Sign-On (OSSO) Agent	10g WebGate	10g or 11g WebGates
Authentication Scheme	<p>OAAMBasic</p> <p>Protects OAAM-related resources with a default context type. This scheme should be used when basic integration with OAAM is required. Here, advanced features like OTP are not supported.</p> <p>For information about the OAAMBasic scheme, see "Managing Authentication Schemes" in <i>Administrator's Guide for Oracle Access Management</i>.</p>	<p>OAAMAdvanced</p> <p>Protects OAAM-related resources with an external context type. This authentication scheme is used when complete integration with OAAM is required. A Webgate must front end the partner.</p> <p>For information about the OAAMAdvanced scheme, see "Managing Authentication Schemes" in <i>Administrator's Guide for Oracle Access Management</i>.</p>	<p>TAPScheme</p> <p>Protects resources in an Access Manager and OAAM integration that uses TAP.</p> <p>This scheme delegates authentication to a third party and Access Manager asserts the token sent back.</p> <p>For information about the TAPScheme scheme, see "Managing Authentication Schemes" in <i>Administrator's Guide for Oracle Access Management</i>.</p>
Allows customization and extension of OAAM flows	<p>No</p> <p>OAAM Basic is not customizable beyond basic screen branding.</p>	<p>Yes</p> <p>More configurable user flows</p>	<p>Yes</p> <p>More configurable user flows</p>
Self-service password management flows	<p>No.</p> <p>OAAM Basic cannot integrate with Oracle Identity Manager</p>	<p>Yes</p> <p>OAAM Advanced can integrate with Oracle Identity Manager</p>	<p>Yes</p> <p>OAAM Advanced using TAP can integrate with Oracle Identity Manager.</p>
End of flow	<p>OAAM calls the OAAM APIs to execute post-authentication rules. Based on the results, renders the appropriate pages.</p>	<p>OAAM runs post-authentication rules to determine risk and execute actions. OAAM sets the SSO cookie and redirects the user to the requested resource.</p>	<p>OAAM runs post-authentication rules to determine risk and execute actions. Access Manager sets the SSO cookie and redirects the user to the requested resource.</p>
Deprecated	<p>Yes</p> <p>Deprecated starting with 11.1.2.2 and will be desupported in 12.1.4 and future releases.</p>	<p>Yes</p> <p>Deprecated starting with 11.1.2.2 and will be desupported in 12.1.4 and future releases.</p>	<p>No</p>
Where information is located	<p>Refer to Section C.3, "OAAM Basic Integration with Access Manager"</p>	<p>Refer to the <i>Oracle Fusion Middleware Integration Guide for Oracle Access Manager 11g Release 1 (11.1.1)</i> for this version of OAAM Advanced integration with Access Manager.</p>	<p>Refer to Section C.4, "OAAM Advanced Integration with Access Manager."</p>

For information on authentication flows, see "About OAAM Authentication, Password Management and Customer Care Flows" in *Administering Oracle Adaptive Access Manager*.

C.2 Definitions, Acronyms, and Abbreviations

This section provides key definitions, acronyms, and abbreviations that are related to this integration.

Table C-2 OAAM and Access Manager Integration Terms

Term	Definition
Action	<p>Oracle Adaptive Access Manager provides functionality to calculate the risk of an access request or an event or a transaction, and determines proper outcomes to prevent fraud and misuse. The outcome can be an action, which is an event activated when a rule is triggered. For example: block access, challenge question, ask for PIN or password, and other actions.</p> <p>For information, see "Managing Policies, Rules, and Conditions" in <i>Administering Oracle Adaptive Access Manager</i>.</p>
Alert	<p>Alerts are messages that indicate the occurrence of an event. An event can be that a rule was triggered, a trigger combination was met, or an override was used.</p> <p>Alert groups are used as results within rules so that when a rule is triggered all of the alerts within the groups are created.</p> <p>For information, see "Managing Policies, Rules, and Conditions" in <i>Administering Oracle Adaptive Access Manager</i>.</p>
Authentication	<p>The process of verifying a person's, device's, or application's identity. Authentication deals with the question "Who is trying to access my services?"</p>
Authentication Level	<p>Access Manager supports various authentication levels to which resources can be configured so as to provide discrete levels of security required to access various resources. Discrete authentication levels distinguish highly protected resources from other resources. The TAP token sent by Access Manager provides parameters related to the authentication level.</p> <p>Authentication level is the trust level of the authentication scheme. This reflects the challenge method and degree of trust used to protect transport of credentials from the user.</p> <p>The trust level is expressed as an integer value between 0 (no trust) and 99 (highest level of trust).</p> <p>Note: After a user is authenticated for a resource at a specified level, the user is automatically authenticated for other resources in the same application domain or in different application domains, if the resources have the same or a lower trust level as the original resource.</p> <p>Current Authentication level is the current authentication level of the user.</p> <p>Target Authentication level is the authentication level required to access the protected resource.</p>
Authorization	<p>Authorization regards the question "Who can access what resources offered by which components?"</p>
Authentication Scheme	<p>Access to a resource or group of resources can be governed by a single authentication process known as an authentication scheme. An authentication scheme is a named component that defines the challenge mechanism required to authenticate a user. Each authentication scheme must also include a defined authentication module.</p> <p>When you register a partner (either using the Oracle Access Management Console or the remote registration tool), the application domain that is created is seeded with a policy that uses the authentication scheme that is set as the default scheme. You can choose any of the existing authentication schemes as the default for use during policy creation.</p>
Authentipad Checkpoint	<p>The Authentipad checkpoint determines the type of device to use based on the purpose of the device.</p>

Table C-2 (Cont.) OAAM and Access Manager Integration Terms

Term	Definition
Blocked	If a user is blocked, it is because a policy has found certain conditions to be true and is set up to respond to these conditions with a Block action. If those conditions change, the user may no longer be blocked. The "Blocked" status is not necessarily permanent and therefore may or may not require an administrator action to resolve. For example, if the user was blocked because he was logging in from a blocked country, but he is no longer in that country, he may no longer be blocked.
Challenge Parameters	Challenge parameters are short text strings consumed and interpreted by WebGates and Credential Collector modules to operate in the manner indicated by those values. The syntax for specifying any challenge parameter is: <parameter>=<value> This syntax is not specific to any WebGate release (10g versus 11g). Authentication schemes are independent of WebGate release.
Challenge Questions	Challenge Questions are a finite list of questions used for secondary authentication. During registration, users are presented with several drop-down question lists called "menus." For example, he may be presented with three question menus. A user must select one question from each menu and enter answers for them during registration. Only one question from each question menu can be registered. These questions become the user's "registered questions." When rules in OAAM Admin trigger challenge questions, OAAM Server displays the challenge questions and accepts the answers in a secure way for users. The questions can be presented in the QuestionPad, TextPad, and other virtual authentication devices, where the challenge question is embedded into the image of the authenticator, or simple HTML.
Checkpoint	A checkpoint is a specified point in a session when Oracle Adaptive Access Manager collects and evaluates security data using the rules engine. Examples of checkpoints are: <ul style="list-style-type: none"> ■ Pre-authentication where rules are run before a user completes the authentication process. ■ Post-authentication where rules are run after a user is successfully authenticated. For information on various checkpoints, see "Managing Policies, Rules, and Conditions" in <i>Administering Oracle Adaptive Access Manager</i> .
Delegated Authentication Protocol	The Delegated Authentication Protocol (DAP) challenge mechanism indicates that Access Manager does an assertion of the token that it receives, which differs from the standard challenge "FORM" mechanism with the external option.
Device	A "device" is a PC, notebook, mobile phone, smart phone, or other web-enabled machine used by a user

Table C-2 (Cont.) OAAM and Access Manager Integration Terms

Term	Definition
Device fingerprinting	<p>Device fingerprinting collects information about the device such as browser type, browser headers, operating system type, locale, and other attributes. Fingerprint data represents the data collected for a device during the login process that can be used to identify the device whenever it is used to log in. The fingerprinting process produces a fingerprint that is unique to the user and designed to protect against the "replay attacks" and the "cookie-based registration bypass" process. The fingerprint details help in identifying a device, check whether it is secure, and determine the risk level for the authentication or transaction.</p> <p>A customer typically uses these devices to log in. Devices can be a PC, notebook, mobile phone, smart phone, or other web-enabled machine.</p>
IAMSuiteAgent	<p>The IAMSuiteAgent (Security Provider in WebLogic Server and corresponding 10g Webgate Profile in Access Manager) is installed out of the box when you install Access Manager. It is implemented directly on the WebLogic Server and evaluates all requests coming in to the WebLogic Server. IAMSuiteAgent is preconfigured to provide Single-Sign On (using the IAMSuiteAgent WebGate Profile in Access Manager) for the IdM domain consoles, Oracle Identity Manager, Oracle Adaptive Access Manager, and other Identity Management servers created during domain creation. It is like a WebGate, but it only protects internal URLs (configured out of the box with the IAM Suite application domain in Access Manager) provided by various products in the Identity and Access Management Suite. In enterprise deployments, there is usually a reverse proxy layer of web servers between the Identity and Access Management products and the end user. Because of this, you could remove the IAMSuiteAgent (Security Provider in WebLogic Server) and configure appropriate WebGate and Host Identifiers through the Oracle Access Management Administration Console and use the IAM Suite application domain with the newly created WebGate front ending Identity and Access Management components/products. If required, resources similar to IAM Suite application domain can be added to the authentication/authorization policies of the WebGate's application domain (if a new application domain is created with the creation of the WebGate Profile front ending Identity and Access Management components/products).</p> <p>Even after disabling/deleting IAMSuiteAgent Provider on WebLogic, the IAMSuite WebGate profile on Access Manager could be used. This IAMSuite WebGate profile is used in the Access Manager and OAAM integration using TAP.</p>
Knowledge Based Authentication (KBA)	<p>Knowledge-based authentication (KBA) is a secondary authentication method that provides an infrastructure based on registered challenge questions.</p> <p>It enables end-users to select questions and provide answers which are used to challenge them later on.</p> <p>Security administration include:</p> <ul style="list-style-type: none"> ■ Registration logic to manage the registration of challenge questions and answers ■ Answer Logic to intelligently detect the correct answers in the challenge response process ■ Validations for answers given by a user at the time of registration <p>For information, see "Managing Knowledge-Based Authentication" in the <i>Administering Oracle Adaptive Access Manager</i>.</p>
KeyPad	<p>A key pad is a virtual keyboard for entry of passwords, credit card number, and so on. The KeyPad protects against Trojan or keylogging.</p>

Table C-2 (Cont.) OAAM and Access Manager Integration Terms

Term	Definition
LDAPScheme	LDAPScheme is an authentication scheme used to protect Access Manager-related resources (URLs) for most directory types based on a form challenge method.
Multi-Level Authentication	<p>Every authentication scheme requires an authentication level. The lower this number, the less stringent the scheme. A higher level number indicates a more secure authentication mechanism.</p> <p>Single Sign-On (SSO) capability enables users to access more than one protected resource or application with a single sign in. After a successful user authentication at a specific level, the user can access one or more resources protected by one or more application domains. However, the authentication schemes used by the application domains must be at the same level (or lower). When a user accesses a resource protected with an authentication level that is greater than the level of his current SSO token, he is re-authenticated. In the Step Up Authentication case, the user maintains his current level of access even if failing the challenge presented for the higher level. This is "additional authentication".</p> <p>For information, see "Managing Authentication and Shared Policy Components" in <i>Administrator's Guide for Oracle Access Management</i>.</p>
Oracle Access Protocol (OAP)	Oracle Access Protocol (OAP) enables communication between Access System components (for example, OAM Server, WebGate) during user authentication and authorization. This protocol was formerly known as NetPoint Access Protocol (NAP) or COREid Access Protocol.
One-time Password (OTP)	<p>One-time Password is a risk-based challenge solution consisting of a server generated one time password delivered to an end user via a configured out of band channel. Supported OTP delivery channels include short message service (SMS), email, and instant messaging. OTP can be used to compliment KBA challenge or instead of KBA. As well both OTP and KBA can be used alongside practically any other authentication type required in a deployment. Oracle Adaptive Access Manager also provides a challenge processor framework. This framework can be used to implement custom risk-based challenge solutions combining third party authentication products or services with OAAM real-time risk evaluations.</p> <p>For information, see "Setting Up OTP Anywhere" in <i>Administering Oracle Adaptive Access Manager</i>.</p>
Access Manager and Oracle Adaptive Access Manager TAP Integration	In Access Manager and Oracle Adaptive Access Manager TAP Integration, OAAM Server acts as a trusted partner application. The OAAM Server uses the Trusted Authentication Protocol (TAP) to communicate the authenticated user name to OAM Server after it performs strong authentication, risk and fraud analysis and OAM Server will own the responsibility of redirecting to the protected resource.
OAAM Admin	Administration Web application for all environment and Adaptive Risk Manager and Adaptive Strong Authenticator features.
OAAMAdminConsoleScheme	Authentication scheme for Oracle Access Management Console.
OAAMAdvanced	Authentication scheme that protects resources with an external context type. This authentication scheme is used when complete integration of OAAM is required. A WebGate must front end the partner.
OAAMBasic	Authentication scheme that protects resources with a default context type. This scheme should be used when OAAM Basic integration with Access Manager is required. Here, advanced features like OTP are not supported.
OAAM Server	Adaptive Risk Manager and Adaptive Strong Authentication features, Web services, LDAP integration and user Web application used in all deployment types except native integration

Table C–2 (Cont.) OAAM and Access Manager Integration Terms

Term	Definition
Policies	<p>Policies contain security rules and configurations used to evaluate the level of risk at each checkpoint.</p> <p>For information, see "Managing Policies, Rules, and Conditions" in <i>Administering Oracle Adaptive Access Manager</i>.</p>
Post-authentication rules	<p>Rules are run after a user is successfully authenticated.</p> <p>For information, see "Managing Policies, Rules, and Conditions" in <i>Administering Oracle Adaptive Access Manager</i>.</p>
Pre-authentication rules	<p>Rules are run before a user completes the authentication process.</p> <p>For information, see "Managing Policies, Rules, and Conditions" in <i>Administering Oracle Adaptive Access Manager</i>.</p>
Profile	<p>The customer's registration information including security phrase, image, challenge questions, challenge (question and OTP) counters, and OTP.</p>
Protection level	<p>There are three protection levels in which to choose from:</p> <ul style="list-style-type: none"> ■ Protected (the default). Protected resources are associated with a protected-level Authentication policy that uses a variety of authentication schemes (LDAP, or example). Authorization policies are allowed for protected resources. Responses, constraints, auditing, and session management are enabled for protected resources using a policy that protects the resource. ■ Unprotected. Unprotected resources are associated with an unprotected-level Authentication policy (level 0) that can use a variety of authentication schemes (LDAP, for example). Authorization policies are allowed for unprotected resources, and a basic one is needed to allow such access. However, an elaborate policy with constraints and responses is irrelevant. Responses, constraints, and auditing are enabled for Unprotected resources using a policy that protects the resource. Only Session Management is not enabled. Access to Unprotected resources incur an OAM Server check from WebGate, which can be audited. ■ Excluded (these are public). Only HTTP resource types can be excluded. Typically security insensitive files like Images (*.jpg, *.png), protection level Excluded resources do not require an OAM Server check for Authentication, Authorization, Response processing, Session management, and Auditing. Excluded resources cannot be added to any user-defined policy in the Oracle Access Management Console. The WebGate does not contact the OAM Server while allowing access to excluded resources; therefore, such access is not audited. Most regular resource validations apply to Excluded resources. However, excluded resources are not listed when you add resources to a policy. There is no Authentication or Authorization associated with the resource. Note: If a resource protection level is modified from "Protected" to "Excluded" and a policy exists for that resource, modification will fail until the resource is first disassociated with the policy.
Registration	<p>Registration is the enrollment process, the opening of a new account, or other event where information is obtained from the user.</p> <p>During the Registration process, the user is asked to register for questions, image, phrase and OTP (email, phone, and so on) if the deployment supports OTP. Once successfully registered, OTP can be used as a secondary authentication to challenge the user.</p>

Table C-2 (Cont.) OAAM and Access Manager Integration Terms

Term	Definition
Risk score	<p>OAAM risk scoring is a product of numerous fraud detection inputs such as a valid user, device, location, and so on. These inputs are weighted and analyzed within the OAAM fraud analytics engine. The policy generates a risk score based on dozens of attributes and factors. Depending on how the rules in a policy are configured, the system can yield an elevated risk score for more risky situations and lower scores for lower-risk situations. The degree of elevation can be adjusted with the weight assigned to the particular risk. The risk score is then used as an input in the rules engine. The rules engine evaluates the fraud risk and makes a decision on the action to take.</p>
Rules	<p>Fraud rules are used to evaluate the level of risk at each checkpoint. For information on policies and rules, see the "OAAM Policy Concepts and Reference" chapter in the <i>Administering Oracle Adaptive Access Manager</i>.</p>
Step Up Authentication	<p>Step Up Authentication occurs when a user is attempting to access a resource more sensitive than ones he had already accessed in the session. To gain access to the more sensitive resource, a higher level of assurance is required. Access Manager resources are graded by authentication level, which defines the relative sensitivity of a resource.</p> <p>For example, if a user accesses a corporate portal home page that is defined as authentication level 3, a basic password authentication is required. The time card application that links off the portal home is more sensitive than the portal home page, so the application is defined as authentication level 4, which requires basic password and risk-based authentication provided by OAAM. So, if a user logs in to the portal with a valid user name and password, and then clicks the time card link, his device is fingerprinted and risk analysis determines if additional authentication, such as a challenge question, is required to allow him access.</p>
Strong Authentication	<p>An authentication factor is a piece of information and process used to authenticate or verify the identity of a person or other entity requesting access under security constraints. Two-factor authentication (T-FA) is a system wherein two different factors are used in conjunction to authenticate. Using two factors as opposed to one factor generally delivers a higher level of authentication assurance.</p> <p>Using more than one factor is sometimes called strong authentication or multi-factor authentication.</p>
TAP	<p>TAP stands for trusted authentication protocol. This is to be used when authentication is performed by a third party and Access Manager asserts the token sent back. After asserting the token, Access Manager creates its cookie and continues the normal single-sign on flow. A trust mechanism exists between the OAM Server and the external third party which performs the authentication. In this scenario, Access Manager acts as an asserter and not authenticator.</p>
TAPScheme	<p>This is the authentication scheme that is used to protect resources in an Access Manager and OAAM integration that uses TAP. If you want two TAP partners with different tapRedirectUrls, create a new authentication scheme using the Oracle Access Management Console and use that scheme.</p> <p>When configured, this authentication scheme can collect context-specific information before submitting the request to the Access Server. Context-specific information can be in the form of an external call for information.</p>

Table C-2 (Cont.) OAAM and Access Manager Integration Terms

Term	Definition
TextPad	Personalized device for entering a password or PIN using a regular keyboard. This method of data entry helps to defend against phishing. TextPad is often deployed as the default for all users in a large deployment then each user individually can upgrade to another device if they wish. The personal image and phrase a user registers and sees every time they login to the valid site serves as a shared secret between user and server.
Virtual authenticators	A personalized device for entering a password or PIN or an authentication credential entry device to protect users while interacting with a protected web application. The virtual authentication devices harden the process of entering and transmitting authentication credentials and provide end users with verification they are authenticating on the valid application. For information on virtual authenticators, see "Customizing Virtual Authentication Devices" in the <i>Developer's Guide for Oracle Adaptive Access Manager</i> .
Web Agent	<p>A single sign-on agent (also known as a policy-enforcement agent, or simply an agent) is any front-ending entity that acts as an access client to enable single sign-on across enterprise applications.</p> <p>To secure access to protected resources, a Web server, Application Server, or third-party application must be associated with a registered policy enforcement agent. The agent acts as a filter for HTTP requests, and must be installed on the computer hosting the Web server where the application resides.</p> <p>Individual agents must be registered with Access Manager 11g to set up the required trust mechanism between the agent and OAM Server. Registered agents delegate authentication tasks to the OAM Server.</p>
WebGate	Web server plug-in that acts as an access client. WebGate intercepts HTTP requests for Web resources and forwards them to the OAM Server for authentication and authorization

C.3 OAAM Basic Integration with Access Manager

OAAM Basic integration with Access Manager, which is a native integration, requires the OAM Server (which is embedded in Access Manager) and OAAM Admin Server in the Identity Management Middleware WebLogic Domain and a functional OAAM database. Knowledge-based Authentication (KBA) is the only challenge mechanism available in this integration.

The OAAM Admin Server is used by Access Manager Administrators to import and export policies, create new policies, view sessions, and configure Oracle Adaptive Access Manager functionality. When policies are imported, exported, or configured, the changes are saved to the OAAM database.

Oracle Adaptive Access Manager is integrated with Access Manager through the extension libraries and uses them directly. The OAAM Server is not needed in this deployment since the rules engine and the runtime functionality of Oracle Adaptive Access Manager are provided using these libraries. When a user enters the registration flow, Access Manager shows the user the virtual authentication devices and runs the pre-authentication policies by using the OAAM libraries to make API calls. The OAAM libraries internally make JDBC calls to save the data related to the user to the OAAM database.

This section explains how to configure OAAM Basic integration with Access Manager.

The following topics explain how this type of integration is implemented:

- [Prerequisites for OAAM Basic Integration with Access Manager](#)

- [Configuring OAAM Basic Integration with Access Manager](#)

C.3.1 Prerequisites for OAAM Basic Integration with Access Manager

Prior to integrating Oracle Adaptive Access Manager with Access Manager, you must have installed all the required components, including any dependencies, and configured the environment in preparation for the integration tasks that follow.

Note: Key installation and configuration information is provided in this section. However, not all component prerequisite, dependency, and installation instruction is duplicated here. Adapt information as required for your environment.

For complete installation information, follow the instructions in *Installation Guide for Oracle Identity and Access Management*.

Table C–3 lists the required components that must be installed and configured before the integration tasks are performed.

Table C–3 Required Components for Integration

Component	Information
Access Manager	Access Manager is installed and configured. For information on the installation and configuration Access Manager, see "Installing and Configuring Oracle Identity and Access Management (11.1.2)" and "Configuring Oracle Access Management" in <i>Installation Guide for Oracle Identity and Access Management</i> .
Oracle Adaptive Access Manager	Oracle Adaptive Access Manager is installed and configured. For information on the installation and configuration of Oracle Adaptive Access Manager, see "Installing and Configuring Oracle Identity and Access Management (11.1.2)" and "Configuring Oracle Adaptive Access Manager" in <i>Installation Guide for Oracle Identity and Access Management</i> .

C.3.2 Starting the Administration Server and Access Manager Managed Server

Start the Administration Server and Access Manager Managed Server.

1. Start the WebLogic Administration Server:

```
DOMAIN_HOME/bin/startWeblogic.sh
```

2. Start the managed server hosting the OAM Server:

```
DOMAIN_HOME/bin/startManagedWeblogic.sh oam_server1
```

For information on starting the Administration Server and Managed Servers, see "Starting the Stack" in *Installation Guide for Oracle Identity and Access Management*.

C.3.3 Configuring OAAM Basic Integration with Access Manager

Follow the steps in this section to implement the Access Manager and Oracle Adaptive Access Manager integration.

Creating a Resource in Access Manager

1. Log in to the Oracle Access Management Console:

`http://oam_adminserver_host:oam_adminserver_port/oamconsole`

2. In the Oracle Access Management Console, click **Application Security** at the top of the window.
3. In the Application Security console, click **Application Domains** in the Access Manager section.
4. In the Search Application Domains page that appears, enter `IAM Suite` in the Name field.
5. Click the **Search** button to initiate the search.
6. Click **IAM Suite** in the Search Results table and click **Edit**.
7. In the IAM Suite Application Domain, click the **Resources** tab, then click **Create** in the Search Results toolbar.
8. In the Create Resource page, create the protected resource.

For example, provide the following information for the resource:

- **Host Identifier:** IDMDomain
 - **Resource URL:** /higherriskresource
9. Click **Apply** to add this resource to the Application Domain.

For information on creating a resource see "Adding and Managing Policy Resource Definitions" in *Administrator's Guide for Oracle Access Management*.

Create a New Authentication Policy

Create a new Authentication Policy under IAMSuiteAgent and make sure to set the Authentication Scheme to `OAAMBasic`.

In this step, you are associating the protected resource with the `OAAMBasic` Authentication Scheme.

1. In the Oracle Access Management Console, click **Application Security** at the top of the window.
2. In the Application Security console, click **Application Domains** in the Access Manager section.
3. In the Search Application Domains page that appears, enter `IAM Suite` in the Name field.
4. Click the **Search** button to initiate the search.
5. Choose **IAM Suite** in the Search Results table and click **Edit**.
6. In the IAM Suite Application Domain page, click the **Authentication Policies** tab, then click the **Create** button in the Search Results toolbar to open the Create Authentication Policy page.
7. In the Create Authentication Policy page, add the required elements for the policy you are creating:

Name: A unique name used as an identifier. For example, `HighPolicy`.

Description (optional): Optional unique text that describes this authentication policy.

Authentication Scheme: OAAMBasic

Success URL: The redirect URL to be used upon successful authentication.

Failure URL: The redirect URL to be used if authentication fails.

8. In the Create Authentication Policy page, add the resource you have created:
 - a. Click the **Resources** tab.
 - b. Click the **Add** button in the Resources tab.
 - c. Click the **Search** button to display all the resources available.
 - d. Choose the URL of the resource you created in the IDMDomain. For example, /higherriskresource.

The listed URLs were added to this application domain earlier. You can add one or more resources to protect with this authentication policy. The resource definition must exist within the application domain before you can include it in a policy.

- e. Click **Add Selected**.

9. Click **Apply** to save changes.

10. In the Create Authentication Policy page, click the **Responses** tab to add responses.

Responses are the obligations (post authentication actions) to be carried out by the Web agent. After successful authentication, the application server hosting the protected application can assert the user identity based on these responses. After a failed authentication, the browser redirects the request to a pre-configured URL

For information on responses, see "Adding and Managing Policy Responses for SSO" in *Administrator's Guide for Oracle Access Management*.

11. Close the page when you finish.

For information on creating an authentication policy for a particular resource, see "Defining Authentication Policies for Specific Resources" in *Administrator's Guide for Oracle Access Management*.

Create a New Authorization Policy

Create a new authorization policy.

1. In the Oracle Access Management Console, click **Application Security** at the top of the window.
2. In the Application Security console, click **Application Domains** in the Access Manager section.
3. In the Search Application Domains page that appears, enter **IAM Suite** in the Name field.
4. Click the **Search** button to initiate the search.
5. Click **IAM Suite** in the Search Results table and click **Edit**.
6. In the IAM Suite Application Domain page, click the **Authorization Policies** tab, then click the **Create** button in the Search Results toolbar. to open the Create Authorization Policy page.
7. Click the **Summary** tab and enter a unique name for this authorization policy.
8. Click the **Resources** tab and click the **Add** button.

9. Click the **Search** button to display all the resources available.
10. From the Results table, click the resource URL in the IDMDomain.
Resource URL: /higherriskresource
11. Click **Add Selected**.
12. Click **Apply** to save changes and close the confirmation window.

For information on creating an authorization policy for a specific resource, see "Defining Authorization Policies for Specific Resources" in *Administrator's Guide for Oracle Access Management*.

Create User with Privileges to Log into the OAAM Administration Console

Create an OAAM user that has the correct privileges to log in to the OAAM Administration Console and then grant the necessary groups to the user.

For information on creating OAAM users and assigning them to groups, see [Section C.4.4, "Creating the OAAM Users and OAAM Groups."](#)

Modify oam-config.xml

Locate and modify the oam-config.xml file manually using a text editor.

The oam-config.xml file contains all Access Manager-related system configuration data and is located in the `DOMAIN_HOME/config/fmwconfig` directory.

Locate the following line and set the `OAAMEnabled` property to `true` as shown:

```
<Setting Name="OAAMEnabled" Type="xsd:boolean">true</Setting>
```

Note: In the oam-config.xml file, you must increment the version number given in the file for this integration to work. For example, if the version number is 1 in the file, change it to 2.

If you prefer to use the `configureOAAM WLST` command to create the data source, associate it as a target with the OAM Server, and enable the property in the oam-config.xml, refer to ["Using ConfigureOAAM WLST Command to Create the Data Source in OAAM Basic Integration with Access Manager"](#).

For information on the oam-config.xml file, see "About the Oracle Access Management Configuration Data File: oam-config.xml" in *Administrator's Guide for Oracle Access Management*.

Start the OAAM Admin Server

Start the OAAM Admin Server, `oaam_admin_server1`.

```
DOMAIN_HOME/bin/startManagedWeblogic.sh oaam_admin_server1
```

Import the OAAM Snapshot

A full snapshot of policies, rules, challenge questions, dependent components, and configurations is shipped with Oracle Adaptive Access Manager. This snapshot is required for the minimum configuration of OAAM. Import the snapshot into the system by following the instructions in [Section C.4.5, "Importing the Oracle Adaptive Access Manager Snapshot."](#)

Shut down the OAAM Administration Server

Shut down the OAAM Administration Server, `oaam_admin_server1`:

```
DOMAIN_HOME/bin/stopManagedWeblogic.sh oaam_admin_server1
```

Create a Data Source

1. Log in to the Oracle WebLogic Administration Console:

```
http://weblogic_admin_server:7001/console
```

2. Since Oracle Adaptive Access Manager is not installed in the same WebLogic Domain as Access Manager, perform the following steps for Access Manager:

- Create a data source with the following JNDI name:

```
jdbc/OAAM_SERVER_DB_DS
```

Note: The name of the data source can be any valid string, but the JNDI name should be as shown above.

- To the schema you created as part of the Oracle Adaptive Access Manager configuration, provide the connection details for the OAAM Database.
3. Click **Services** and then **Database Resources** and locate the **OAAM_SERVER_DB_DS** resource.
 4. Lock the environment by clicking the **Lock** button in the upper left corner of the WebLogic Administration Console.
 5. Open the **OAAM_SERVER_DB_DS** resource and click the **Target** tab. Once there, you are presented a list of WebLogic Servers that are available.
 6. Associate **Administration Server** and **oaam_server1** as targets with the data source.
 7. Click the **Activate** button in the upper left corner of the Oracle WebLogic Administration Console.

For information on configuring JDBC data sources, see "Configuring JDBC Data Sources" in *Oracle Fusion Middleware Configuring and Managing JDBC Data Sources for Oracle WebLogic Server*.

Test the Configuration

1. To verify the configuration, remote register two agents, each protecting a resource.
2. Use the Oracle Access Management Console to associate the first resource with the `OAAMBasic` policy for the authentication flow. Associate the second resource with the `LDAPScheme`.

See Also: "Managing Authentication Schemes" in *Administrator's Guide for Oracle Access Management*.

3. Access the protected resource configured earlier to verify the configuration.

You are prompted to enter a user name. Then, on a separate screen you are prompted for the password.

Once the user name and password are validated you are asked to select and answer three challenge questions. Once completed you are taken to the protected application.

C.4 OAAM Advanced Integration with Access Manager

Integrating Oracle Adaptive Access Manager with Access Manager provides an enterprise with advanced access security features that greatly improve the level of protection for applications. Features including anti-phishing, anti-malware, device fingerprinting, behavioral profiling, geolocation mapping, real-time risk analysis and multiple risk-based challenge mechanisms such as one-time password and knowledge based authentication questions provide an increased level of access security.

This section explains how to integrate Oracle Adaptive Access Manager with Access Manager in "OAAM Advanced using TAP."

In OAAM Advanced Integration using TAP, OAAM Server acts as a trusted partner application. The OAAM Server uses the Trusted authentication protocol (TAP) to communicate the authenticated username to OAM Server after it performs strong authentication and risk and fraud analysis. The OAM Server then redirects the user to the protected resource.

OAAM Advanced integration with Access Manager can involve scenarios with or without Oracle Identity Manager.

With Oracle Identity Manager

Integration with Oracle Identity Manager provides users with richer password management functionality, including secure "Forgot Password" and "Change Password" flows.

For integration details, see [Chapter 3, "Integrating Access Manager, OAAM, and OIM"](#).

Without Oracle Identity Manager

If Oracle Identity Manager is not part of your environment, follow the integration procedure described in this chapter.

C.4.1 Roadmap for OAAM Advanced Integration with Access Manager

[Table C-4](#) lists the high-level tasks for integrating Oracle Adaptive Access Manager with Access Manager.

The configuration instructions assume Oracle Adaptive Access Manager is integrated with Access Manager using the out-of-the box integration.

Table C-4 Roadmap for OAAM Advanced Integration with Access Manager

1	Verify that all required components have been installed and configured prior to integration.	For information, see "Prerequisites for OAAM Advanced Integration with Access Manager."
2	Ensure the Access Manager and OAAM Administration Consoles and managed servers are running.	For information, see "Restarting the Servers."
3	Create the OAAM users.	For information, see "Creating the OAAM Users and OAAM Groups."
4	Import the OAAM base snapshot.	For information, see "Importing the Oracle Adaptive Access Manager Snapshot."

Table C-4 (Cont.) Roadmap for OAAM Advanced Integration with Access Manager

5	Validate that Access Manager was set up correctly.	For information, see "Validating Initial Configuration of Access Manager."
6	Validate that OAAM was set up correctly.	For information, see "Validating Initial Configuration of Oracle Adaptive Access Manager."
7	Register the WebGate agent with Access Manager 11g to set up the required trust mechanism between the Agent and OAM Server.	For information, see "Registering the WebGate with Access Manager 11g Using the Oracle Access Management Console."
8	Register the OAAM Server to act as a trusted partner application to Access Manager.	For information, see "Registering the OAAM Server as a Partner Application to Access Manager."
9	Add the agent password to the Agent profile.	For information, see "Adding an Agent Password to the IAMSuiteAgent Profile."
10	Update IAMSuiteAgent.	For information, see "Updating the Domain Agent Definition If Using Domain Agent for IDM Domain Consoles."
11	Verify TAP partner registration using the Oracle Access Management tester.	For information, see "Verifying TAP Partner Registration."
12	Set up TAP integration properties in OAAM.	For information, see "Setting Up Access Manager TAP Integration Properties in OAAM."
13	Configure the integration to use OAAM TAPScheme to protect Identity Management product resources in the IAMSuiteAgent application domain.	For information, see "Configuring the Integration to Use TAPScheme to Protect Identity Management Resources in the IAMSuiteAgent Application Domain."
14	Configure the authentication scheme in the policy-protected resource policy to protect a resource with the OAAM TAPScheme.	For information, see "Configuring a Resource to be Protected with TAPScheme."
15	Validate the Access Manager and Oracle Adaptive Access Manager Integration.	For information, see "Validating the Access Manager and Oracle Adaptive Access Manager Integration."

C.4.2 Prerequisites for OAAM Advanced Integration with Access Manager

Prior to configuring Oracle Adaptive Access Manager with Access Manager, you must have installed all the required components, including any dependencies, and configured the environment in preparation of the integration tasks that follow.

Note: Key installation and configuration information is provided in this section. However, not all component prerequisite, dependency, and installation instruction is duplicated here. Adapt information as required for your environment.

For complete installation information, follow the instructions in *Installation Guide for Oracle Identity and Access Management*.

Table C-5 lists the required components that must be installed and configured before the integration tasks are performed.

Table C-5 Required Components for Integration

Component	Information
Access Manager	<p>Access Manager is installed and configured.</p> <p>Each Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) domain must be configured to have a Database Security Store. Irrespective of the number of domains in a logical Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) deployment (a logical deployment is a collection of Oracle Identity and Access Management products running in one or more domains and using a single database to hold product schemas), all domains share the same Database Security Store and use the same domain encryption key. The Database Security Store is created at the time of creating the first domain, and then each new domain created is joined with the Database Security Store already created. At installation, Access Manager is configured with the Database Security store. The Access Manager and Oracle Adaptive Access Manager wiring requires the Database Security Store.</p> <p>For information on the installation of Access Manager, see "Installing and Configuring Oracle Identity and Access Management (11.1.2.3.0)" in <i>Installation Guide for Oracle Identity and Access Management</i>.</p> <p>For information on the configuration of Access Manager in a new or existing WebLogic Domain and the configuration of the Database Security Store, see "Configuring Oracle Access Management" in the <i>Installation Guide for Oracle Identity and Access Management</i>.</p> <p>In addition, see "Securing Communication" in the <i>Administrator's Guide for Oracle Access Management</i> for information about the configuration of Access Manager in Open, Simple, or Cert mode.</p>
Oracle Adaptive Access Manager	<p>Oracle Adaptive Access Manager is installed and configured.</p> <p>For information on the installation and configuration of Oracle Adaptive Access Manager, see "Installing and Configuring Oracle Identity and Access Management (11.1.2.3.0)" and "Configuring Oracle Adaptive Access Manager" in <i>Installation Guide for Oracle Identity and Access Management</i>.</p> <p>Because the installations are in a split domain, the <code>oaam.csf.useMBeans</code> property must be set to <code>true</code>. See "Setting Up the Credential Store Framework (CSF) Configuration" in the <i>Administering Oracle Adaptive Access Manager</i> for information on setting this parameter.</p>
Oracle HTTP Server	<p>For more information on the installation of the Oracle HTTP Server (OHS), see <i>Oracle Fusion Middleware Installation Guide for Oracle Web Tier</i>.</p>

Table C-5 (Cont.) Required Components for Integration

Component	Information
Oracle Access Manager 10g or Access Manager 11g agent (WebGate)	<p>For information on the installation of the Oracle Access Management 11g WebGate, see "Installing Oracle HTTP Server 11g WebGate" in <i>Oracle Fusion Middleware Installing Webgates for Oracle Access Manager</i>.</p> <p>For information on the installation of the Oracle Access Manager 10g WebGate, see "Registering and Managing 10g WebGates with Access Manager 11g" in <i>Administrator's Guide for Oracle Access Management</i>.</p>

C.4.3 Restarting the Servers

Before you can perform tasks in this section, ensure that the Oracle Access Management Console and OAAM Administration Console and managed servers are running. To restart the servers, perform these steps:

1. Start the WebLogic Administration Server:

```
OAM_DOMAIN_HOME/bin/startWeblogic.sh
```

Since OAAM is installed and configured in a different WebLogic Domain from Access Manager, you must also start the WebLogic Administration Server located in *OAAM_Domain_Home*:

```
OAAM_DOMAIN_HOME/bin/startWeblogic.sh
```

OAM_DOMAIN_HOME is the WebLogic Domain which contains Access Manager and *OAAM_DOMAIN_HOME* is the WebLogic Domain which contains OAAM.

2. Start the managed server hosting the OAM Server:

```
OAM_DOMAIN_HOME/bin/startManagedWeblogic.sh oam_server1
```

3. Start the managed server hosting OAAM Admin Server:

```
OAAM_DOMAIN_HOME/bin/startManagedWeblogic.sh oaam_admin_server1
```

4. Start the managed server hosting the Oracle Adaptive Access Manager runtime server:

```
OAAM_DOMAIN_HOME/bin/startManagedWeblogic.sh oaam_server_server1
```

For information on starting the Administration Server and Managed Servers, see "Starting the Stack" in *Installation Guide for Oracle Identity and Access Management*.

C.4.4 Creating the OAAM Users and OAAM Groups

Note: Skip this step if you have already created OAAM users and OAAM groups during post-installation.

Before integrating Oracle Adaptive Access Manager with Access Manager, you must take into account whether the OAAM Administration Console is being protected. In order to access the OAAM Administration Console, you must create administration users.

- If you are protecting the OAAM Administration Console, you must create users and groups in the external LDAP store using the `idmConfigTool`. For details, see

Section D.4.2.3, "prepareIDStore mode=OAAM"

OR

- If you are not protecting the OAAM Administration Console, create the administration user using the WebLogic Administration Console.

To disable OAAM Administration Console protection, refer to [Section C.6.5, "Disabling OAAM Administration Console Protection."](#)

The following are instructions to create an administration user using the WebLogic Administration Console and associate that user to an OAAM group:

1. Create groups in the external LDAP store using the `idmConfigTool`. For details, see [Section D.4.2.3, "prepareIDStore mode=OAAM"](#)
2. Log in to the Oracle WebLogic Administration Console for your WebLogic Domain.
3. Under Domain Structure in the left pane, select **Security Realms**.
4. In the Summary of Security Realms page, select the realm that you are configuring (for example, *myrealm*).
5. In the Settings for Realm Name page select **Users and Groups** and then **Users**.
6. Click **New** and provide the required information to create a user, such as `user1`, in the security realm:
 - **Name:** `oaam_admin_username`
 - **Description:** optional
 - **Provider:** `DefaultAuthenticator`
 - **Password:** Enter a password for the administrator
 - **Confirmation:** Re-enter the password for the administrator

Important: User names must not include tabs or any of the following characters: semicolons, commas, plus signs, equal signs, and single backslash characters. In addition, it may not start with a pound sign or double quotations. If a user is created with any of the invalid characters, the WebLogic domain can become corrupted.
7. Click **OK** to save your changes.
`user1` appears in the User table.
8. In the Users table, select the newly created user, `user1`.
9. In the Settings for User Name page, click the **Groups** tab.
10. Select a group or groups from the Available list box with the OAAM keyword to the user, `user1`.
To add a `user1` to a group, click the right arrow to move the selection to the Chosen list box.
You must set up the OAAM groups in the external LDAP store prior to associating users to the groups; otherwise, they will not be available.
11. Click **Save**.

For information on creating users and assigning them to groups, see *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*.

C.4.5 Importing the Oracle Adaptive Access Manager Snapshot

Note: Skip this step if you have already imported the OAAM Snapshot during post-installation.

A full snapshot of policies, rules, challenge questions, dependent components, and configurations is shipped with Oracle Adaptive Access Manager. This snapshot is required for the minimum configuration of Oracle Adaptive Access Manager. Import the snapshot into the system by following these instructions:

1. Log in to the OAAM Administration Console with the newly created user.
`http://oaam_managed_server_host:oaam_admin_managed_server_port/oaam_admin`
2. Open **System Snapshot** under **Environment** in the Navigation tree.
The **System Snapshots Search** page is displayed.
3. Click the **Load from File** button in the upper right.
A Load and Restore Snapshot screen appears.
4. Deselect **Back up current system now** and click **Continue**.
5. When the dialog appears with the message that you have not chosen to back up the current system, and do you want to continue, click **Continue**.
6. Click the **Choose File** button.
7. Now that you are ready to load the snapshot, click the **Browse** button in the dialog in which you can enter the filename of the snapshot you want to load. A screen appears for you to navigate to the directory where the snapshot file is located. Click **Open**. Then, click the **Load** button to load the snapshot into the system.

The snapshot file, `oaam_base_snapshot.zip` is located in the `Oracle_IDM1/oaam/init` directory where the OAAM base content is shipped.
8. Click **OK**.

You have loaded the snapshot into memory, but the items in the snapshot are not effective yet. Unless you click the **Restore** button, the items in the snapshot have not been applied.
9. To apply the snapshot, click **Restore**.

Once you have applied the snapshot, make sure it appears in the System Snapshots page.

To ensure correct operation, make sure that the default base policies and challenge questions shipped with Oracle Adaptive Access Manager have been imported into your system. You may encounter a non-working URL if policies and challenge questions are not available as expected in your Oracle Adaptive Access Manager environment.

For information on searching for OAAM policies, see "Searching for a Policy" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

For information on searching for challenge questions, see "Searching for a Challenge Question" in *Administering Oracle Adaptive Access Manager*.

For information on the location of the base policies and default question zip files shipped with Oracle Adaptive Access Manager, see "Importing the OAAM Snapshot" in *Administering Oracle Adaptive Access Manager*.

C.4.6 Validating Initial Configuration of Access Manager

Verify that Access Manager is set up correctly by accessing the Welcome to Oracle Access Management page.

1. Log in to the Oracle Access Management Console:

```
http://oam_adminserver_host:oam_adminserver_port/oamconsole
```

You should be redirected to the OAM Server for login.

2. Provide the WebLogic Admin user name and password.

If the login is successful, the Welcome to Oracle Access Management page is displayed.

C.4.7 Validating Initial Configuration of Oracle Adaptive Access Manager

Verify that Oracle Adaptive Access Manager is set up correctly by accessing the OAAM Server.

1. Log in to the OAAM Server:

```
http://host:port/oaam_server
```

2. Provide any user name and click **Continue**.
3. Provide the password as `test` because the Access Manager and Oracle Adaptive Access Manager integration has not yet been performed. You must change the password immediately after the integration.
4. Complete the registration.

A successful login indicates that you have configured the initial configuration correctly.

Note: The test login URL `/oaam_server` is used to verify that the OAAM configuration is working before proceeding with the integration of Access Manager. This URL is not intended for use after the integration of Access Manager and OAAM. For information, see [Section C.8.2.5, "OAAM Test Login URL /oaam_server Fails After Access Manager and Oracle Adaptive Access Manager Integration."](#)

C.4.8 Registering the WebGate with Access Manager 11g Using the Oracle Access Management Console

Register the WebGate agent with Access Manager 11g to set up the required trust mechanism between the Agent and OAM Server. After registration, the Agent collaborates communication between the OAM Server and its services and acts as a filter for HTTP/HTTPS requests. The Agent intercepts requests for resources protected by Access Manager and works with Access Manager to fulfill access requirements.

Prior to installing the WebGate with Access Manager, review *Oracle Fusion Middleware Supported System Configurations* from the Oracle Technology Network to locate the certification information for the 10g or 11g WebGate you want to use for your deployment. This section provides information on registering the 11g WebGate with

Access Manager 11g. For information on installing and registering 10g WebGates to use with Access Manager 11g, see "Registering and Managing 10g WebGates with Access Manager 11g" in *Administrator's Guide for Oracle Access Management*.

C.4.8.1 Prerequisites for WebGate Registration

To register WebGate with Access Manager, ensure that the following required components, including any dependencies, are installed and configured:

- WebLogic Server for Oracle HTTP Server.
- Oracle HTTP Server installed and configured using the Oracle Web Tier installer. The following is an example of the *OHS_Home* location:

```
MW_Home/Oracle_WT1
```

Oracle HTTP Server provides a listener for Oracle WebLogic Server and the framework for hosting static pages, dynamic pages, and applications over the Web.

For information about installing and configuring Oracle HTTP Server 11g, see the *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*.

- Oracle HTTP Server WebGate for Access Manager installed. The following is an example of the *WebGate_Home* location:

```
MW_Home/Oracle_OAMWebGate1
```

Oracle HTTP Server WebGate installation packages are found on media and virtual media that is separate from the core components. You can download the Oracle HTTP Server WebGate software from the Oracle Technology Network (OTN):

```
http://www.oracle.com/technetwork/index.html
```

For detailed information on installing the Oracle HTTP Server WebGate, see "Installing and Configuring Oracle HTTP Server 11g WebGate for OAM" in *Oracle Fusion Middleware Installing Webgates for Oracle Access Manager*.

- If you are using Windows 2003 or Windows 2008 64-bit operating systems, you must install Microsoft Visual C++ 2005 libraries on the machine hosting the Oracle HTTP Server 11g WebGate for Access Manager. These libraries are required for the WebGate.
- Java runtime environment (JRE) 1.6 or higher installed.

C.4.8.2 Configure Oracle HTTP Server with WebGate

After installing the Oracle HTTP Server 11g WebGate for Access Manager, you must create an instance of WebGate which has the same instance home as the Oracle HTTP Server and update the Oracle HTTP Server configuration file with the WebGate configuration. For detailed instructions, see "Post-Installation Steps for Oracle HTTP Server 11g WebGate" in *Oracle Fusion Middleware Installing Webgates for Oracle Access Manager*.

Following the directions in "Post-Installation Steps for Oracle HTTP Server 11g WebGate," you will:

1. Create a WebGate instance and copy the Agent configuration files from the *WebGate_Home* directory to the WebGate instance location.

WebGate_Home is the directory where you have installed Oracle HTTP Server WebGate and defined it as the Oracle Home for WebGate, as in the following example:

```
MW_HOME/Oracle_OAMWebGate1
```

The WebGate Instance Home must be the Instance Home of Oracle HTTP Server, as in the following example:

```
MW_HOME/Oracle_WT1/instances/instance1/config/OHS/ohs1
```

2. Update `httpd.conf` with the WebGate configuration.

C.4.8.3 Register the WebGate as a Partner with Access Manager 11g Using the Oracle Access Management Console

To register the WebGate as a partner with Access Manager 11g:

1. Log in to the Oracle Access Management Console:

```
http://oam_adminserver_host:oam_adminserver_port/oamconsole
```

2. Register the new WebGate agent with Access Manager by using the Oracle Access Management Console. For information, see "Registering an OAM Agent Using the Console" in the *Administrator's Guide for Oracle Access Management*.
3. Click the **Edit** button in the tool bar to display the configuration page.
4. Set the Access Client Password and click **Apply**. Note the Artifacts location in the confirmation message.

The Access Client Password is the unique password for Agent. When the Agent connects to an OAM Server, it uses the password to authenticate itself to the server. This prevents unauthorized agents from connecting and obtaining policy information.

5. In the Artifacts Location, locate the `ObAccessClient.xml` configuration file and `cwallet.sso` file and copy them to the following directory:

```
OHS_Home/instances/instance/config/OHS/component/webgate/config
```

C.4.8.4 Restarting the Oracle HTTP Server WebGate

Restart Oracle HTTP Server for the changes to take effect.

1. Navigate to the `OHS_HOME/instances/instance/bin` directory.
2. Restart the Oracle HTTP Server instance by using the following command:

```
opmnctl stopall
opmnctl startall
```

C.4.8.5 Validating the WebGate Setup

Once the setup of WebGate is complete, validate the registration as follows:

1. Verify the WebGate configuration by accessing the protected URL:

```
http://ohs_host:ohs_port/
```

You should be redirected to Access Manager single sign-on (SSO) login page for authentication.

2. Enter user name and password.

The Oracle HTTP Server Welcome page is displayed.

This is the partner that will be protected using Oracle Adaptive Access Manager.

C.4.9 Registering the OAAM Server as a Partner Application to Access Manager

A partner application is any application that delegates the authentication function to Access Manager 11g. After registering with Access Manager as a partner application, OAAM can communicate with Access Manager using Trusted Authentication Protocol (TAP) and validate user authentications with Access Manager so Access Manager can create the required cookies and continue the normal single-sign on flow in which it redirects the user to the protected resource.

To register the OAAM Server as a trusted partner, follow these steps:

1. Ensure that the OAM Administration Server is running.
2. Create a keystore directory to hold the OAAM Keystore by executing the following:

```
mkdir IAM_ORACLE_HOME/TAP/TapKeyStore
```

3. Set up the environment for the Oracle WebLogic Scripting Tool (WLST).

- a. Navigate to the `IAM_ORACLE_HOME/common/bin` directory:

```
cd IAM_ORACLE_HOME/common/bin
```

- b. Enter the WLST shell environment by executing:

```
./wlst.sh
```

- c. Enter `connect` to connect to the WebLogic Administration Server.

- d. Enter username. For example, `admin_username`.

- e. Enter password. For example, `admin_password`.

- f. Enter `t3://hostname:port`

For example:

```
t3://AdminHostname:7001
```

4. Using the WLST shell, run the `registerThirdPartyTAPPartner` command:

```
registerThirdPartyTAPPartner(partnerName = "partnerName", keystoreLocation=  
"path to keystore", password="keystore password", tapTokenVersion="v2.0",  
tapScheme="TAPScheme", tapRedirectUrl="OAAM login URL")
```

An example is provided below.

```
registerThirdPartyTAPPartner(partnerName = "OAAMTAPPartner", keystoreLocation=  
"IAM_ORACLE_HOME/TAP/TapKeyStore/mykeystore.jks", password="password",  
tapTokenVersion="v2.0", tapScheme="TAPScheme", tapRedirectUrl="http://OAAM_  
Managed_server_host:14300/oaam_server/oamLoginPage.jsp")
```


Table C-6 TAP Partner Registration Parameters

Parameters	Descriptions
partnerName	The name of the partner should be unique. It can be any name used for identifying the third party partner. If the partner exists in Access Manager, the configuration will be overwritten.
keystoreLocation	The keystore location is an existing location. If the directory path specified is not present, an error occurs. You must provide the complete path including the keystore file name. In the example shown earlier, the keystore location was <code>IAM_ORACLE_HOME/TAP/TapKeyStore/mykeystore.jks</code> . Another example is <code>keystoreLocation="/scratch/jsmith/dwps1tap/TapKeyStore/mykeystore.jks"</code> . When you run the command <code>registerThirdPartyTAPPartner</code> , the keystore file is created in that location specified. On Windows, the path must be escaped. For example: <code>"C:\\oam-oaam\\tap\\tapkeystore\\mykeystore.jks"</code>
password	The keystore password used to encrypt the keystore. The keystore is created by running command <code>registerThirdPartyTAPPartner</code> in the location as specified for parameter <code>keystoreLocation</code> . Make a note of the password as you will need it later.
tapTokenVersion	Version of the Trusted Authentication Protocol. <code>tapTokenVersion</code> is always <code>v2.0</code> for 11.1.1.5.0 and 11.1.2.0. If using IDContext Claims, it is <code>v2.1</code> .
tapScheme	Trusted Authentication Protocol Authentication Scheme (TAPScheme out of the box.) This is the authentication scheme that will be updated. If you want two tap partners with different <code>tapRedirectUrls</code> , create a new authentication scheme using the Oracle Access Management Console and use that scheme here. The authentication scheme will be created automatically while you are running the <code>registerThirdPartyTAPPartner</code> command in the instructions above. The name of <code>TAPScheme</code> will be passed as parameter to that command. The example command has <code>tapScheme="TAPScheme"</code> .
tapRedirectUrl	Third party access URL. The TAP redirect URL should be accessible. If it is not, registration of the partner fails with the message: <code>Error! Hyperlink reference not valid.</code> <code>tapRedirectUrl</code> is constructed as follows: <code>http://oamserver_host:oaamserver_port/oaam_server/oamLoginPage.jsp</code> Ensure that the OAAM Server is running; otherwise registration will fail. The credential collector page will be served by the OAAM Server. The authentication scheme created by <code>registerThirdPartyTAPPartner (TAPScheme)</code> points to the OAAM Server credential collector page as the <code>redirectURL</code> .

C.4.10 Adding an Agent Password to the IAMSuiteAgent Profile

When Access Manager is installed, the IAMSuiteAgent (Security Provider in WebLogic and corresponding 10g Webgate Profile in Access Manager) is created. By default there is no password set. In OAAM and Access Manager integration using TAP, when OAAM connects to Access Manager, it uses the IAMSuiteAgent profile (configured while setting up TAP integration in OAAM using the OAAM CLI) and that connection requires an agent password.

You must set an agent password for the IAMSuiteAgent profile in Access Manager. It is a required step for Access Manager and Oracle Adaptive Access Manager

integration since the password is used in multiple places. To set the password, proceed as follows:

1. Log in to the Oracle Access Management Console:
`http://oam_adminserver_host:oam_adminserver_port/oamconsole`
2. In the Oracle Access Management Console, click **Application Security** at the top of the window.
3. In the Application Security console, click **Agents** in the Agents section.
 The Search SSO Agents page opens with the WebGates tab active.
4. In the Search SSO Agents page that appears, enter IAMSuiteAgent as the name of the agent you want to find.
5. Click the **Search** button to initiate the search.
6. Choose **IAMSuiteAgent** in the Search Results table and click **Edit**.
7. In the IAMSuiteAgent Webgate page, specify the password in the Access Client Password field and click **Apply** to save the changes.

C.4.11 Updating the Domain Agent Definition If Using Domain Agent for IDM Domain Consoles

IAMSuiteAgent is implemented directly on the WebLogic Server and preconfigured to provide Single-Sign On (using IAMSuiteAgent Webgate Profile in Access Manager) for the IDM domain consoles

If the IAMSuiteAgent provider in WebLogic is not disabled/deleted and the IAMSuiteAgent profile in Access Manager is working in Open mode, after completing the steps in [Section C.4.10, "Adding an Agent Password to the IAMSuiteAgent Profile,"](#) you must update the IAMSuiteAgent provider configuration in WebLogic with the password if you want to continue using the IAMSuiteAgent for the IDM domain consoles.

Note: The IAMSuiteAgent is now in **Open Mode** with password authentication.

To update the domain agent definition, proceed as follows:

1. Log in to WebLogic Administration Console:
`http://oam_adminserver_host:port/console`
2. Select **Security Realms** from the Domain Structure menu.
3. Click **myrealm**.
4. Click the **Providers** tab.
5. Select **IAMSuiteAgent** from the list of authentication providers.
6. Click **Provider Specific**.
7. Enter the agent password and confirm the password.
 This is a required step.
8. Click **Save**.
9. Click **Activate Change** in the top left corner.
10. Restart the WebLogic Administration Server, OAAM Admin and managed servers, and OAM Server.

C.4.12 Verifying TAP Partner Registration

To verify the TAP partner registration, follow the instructions below.

C.4.12.1 Verifying the Challenge URL

To validate the Access Manager configuration, perform the following steps:

1. Log in to the Oracle Access Management Console:

```
http://oam_adminserver_host:oam_adminserver_port/oamconsole
```

2. In the Oracle Access Management Console, click **Application Security** at the top of the window.
3. In the Application Security Console, click **Authentication Schemes** in the **Access Manager** section.
4. In the Search Authentication Schemes page, enter TAPScheme in the Name field.
5. Click the **Search** button to initiate the search.
6. Choose **TAPScheme** in the Search Results table and click **Edit**.

For specific details on the TAPScheme, see "Pre-configured Authentication Schemes" in *Administrator's Guide for Oracle Access Management*.

7. In the TAPScheme Authentication Scheme page, verify that the **Challenge Method** is DAP and the **Authentication Module** is DAP.

For information on the DAP challenge method, see "About Challenge Methods" in *Administrator's Guide for Oracle Access Management*.

8. If the tapRedirectUrl is, for example, `http://OAM_Managed_server_host:14300/oaam_server/oaamLoginPage.jsp`, verify that the Challenge URL is set to:

```
/oaam_server/oaamLoginPage.jsp
```

The Challenge URL shows the tapRedirectUrl that had been specified when OAM was registered with Access Manager as a partner application. The host and port part of the URL is parameterized in Challenge Parameter.

The parameters TAPPartnerId=OAMTAPPartner and SERVER_HOST_ALIAS=OAMSERVER should already be listed as Challenge Parameters.

Server host alias is a logical hostname generated for the given OAM server host name and port in the registerThirdPartyPartner WLST command. The physical hostname and port is stored under \$DOMAIN_HOME/config/fmwconfig/oaam-config.xml in

```
/NGAMConfiguration/DeployedComponent/Server/NGAMServer/Profile/OAMServerProfile/HostAlias/HOST_ALIAS_<NUMBER> path
```

9. Check that the challenge parameters are set correctly.

For information on Authentication Scheme elements, see "About Authentication Schemes and Pages" in the *Administrator's Guide for Oracle Access Management*.

C.4.12.2 Adding the MatchLDAPAttribute Challenge Parameter in the TAPScheme

You must add the MatchLDAPAttribute challenge parameter and set it to the User Name Attribute as specified in the LDAP Identity Store.

1. In the Authentication Scheme page, position your cursor in the **Challenge Parameter** field and press **Enter** using your keyboard.
2. In the new line, add an entry for the challenge parameter.

For example, MatchLDAPAttribute=uid

MatchLDAPAttribute must be set to the User Name Attribute as specified in the LDAP Identity Store. For example, uid, mail, cn, and so on.

Note: The challenge parameter is case-sensitive.

For information, see "Managing User Identity Stores" in *Administrator's Guide for Oracle Access Management*.

3. Click **Apply** to submit the change.
4. Close the confirmation window.

C.4.12.3 Validating the IAMSuiteAgent Setup

To test the IAMSuiteAgent profile in Access Manager, proceed as follows:

1. Restart the managed server hosting the OAM Server.

- a. Stop the managed server hosting the OAM Server:

```
OAM_DOMAIN_HOME/bin/stopManagedWeblogic.sh oam_server1
```

- b. Start the managed server hosting the OAM Server:

```
OAM_DOMAIN_HOME/bin/startManagedWeblogic.sh oam_server1
```

2. Ensure that JAVA_HOME is set in your environment.
3. Add JAVA_HOME/bin to your PATH, for example:

```
export PATH=$JAVA_HOME/bin:$PATH
```

4. Change the directory to:

```
IAM_ORACLE_HOME/oam/server/tester
```

5. Launch Oracle Access Management tester:

```
java -jar oamtest.jar
```

The Oracle Access Management Tester Console appears.

6. In the Server Connection section provide server connection details as follows:

- a. **IP Address:** Access Manager Managed Server Host
- b. **Port:** Oracle Access Management Oracle Access Protocol (OAP) Port
- c. **Agent ID:** IAMSuiteAgent
- d. **Agent Password:** Password provided in [Section C.4.10, "Adding an Agent Password to the IAMSuiteAgent Profile."](#)

The Server Connection section provides fields for the information required to establish a connection to the OAM Server.

7. Click **Connect**.

If you can connect to the server, the next section, **Protected Resource URI**, will be enabled.

8. The Protected Resource URI section provides information about a resource whose protected status needs to be validated.

In this section, provide the protected resource URI as follows:

- a. **Host:** IAMSuiteAgent
- b. **Port:** 80
- c. **Resource:** /oamTAPAuthenticate

Note: You can test any other resource protected using TAPScheme other than oamTAPAuthenticate.

9. Click **Validate**.

The Validate button is used to submit the Validate Resource server request. If the validation is successful, the next section for **User Identity** will be enabled.

10. In the User Identity section, provide User Identity and click **Authenticate**. If the authentication is successful, the setup is successful.

For information on the Oracle Access Management Tester, see "Validating Connectivity and Policies Using the Access Tester" in *Administrator's Guide for Oracle Access Management*.

C.4.13 Setting Up Access Manager TAP Integration Properties in OAAM

In OAAM and Access Manager integration using TAP, when OAAM connects to Access Manager, it uses the IAMSuiteAgent profile, which is configured while setting up TAP integration in OAAM.

To run `setupOAMTapIntegration.sh` to configure Access Manager for TAP Integration, proceed as follows:

Note: If the OAAM command line script fails to run, then execute it as follows:

```
bash script_name
```

1. Ensure that the OAAM managed server is running.
2. Copy the OAAM `cli` folder to a temporary directory:

```
cp -r OAAM_HOME/oaam/cli /temp/oaam_cli
```

3. Open the `oaam_cli.properties` located in `temp/oaam_cli/conf/bharosa_properties`.
4. Using a text editor, set the properties as described in [Table C-7](#).

Table C-7 OAAM CLI Properties

Parameter	Details
oaam.adminserver.hostname	This is the Admin Server host of the WebLogic Server Domain where OAAM is installed.
oaam.adminserver.port	This is the Admin Server port of the WebLogic Server Domain where OAAM is installed.
oaam.db.url	This is the valid JDBC URL of the OAAM database in the format: <code>jdbc:oracle:thin:@db_host:db_port:db_sid</code>
oaam.uio.oam.tap.keystoreFile	This is the location of keystore file generated by the <code>registerThirdPartyTAPPartner</code> WLST command. Copy the file from the location specified in the above WLST command for parameter <code>keystoreLocation</code> . If Access Manager and OAAM are on different machines, you will need to manually copy the keystore file created in the OAM Server to the OAAM Server and provide the location on the OAAM Server here. On Windows, the file path value must be escaped. For example: <code>C:\\oam-oaam\\tap\\keystore\\store.jks</code>
oaam.uio.oam.tap.partnername	This is <code>partnerName</code> used in the WLST command <code>registerThirdPartyTAPPartner</code> command. For example, <code>OAAMPartner</code> .
oaam.uio.oam.host	This is the Access Manager Primary Host.
oaam.uio.oam.port	This is the Access Manager Primary Oracle Access Protocol (OAP) Port. This is the OAM Server port, with the default port number 5575.
oaam.uio.oam.webgate_id	This is the <code>IAMSuiteAgent</code> value. Do not change this.
oaam.uio.oam.secondary.host	Name of the secondary OAM Server Host machine. This property is used for high availability. You could specify the fail-over hostname using this property.
oaam.uio.oam.secondary.host.port	This is the Access Manager Secondary OAP Port. This property is used for high availability. You could specify the fail-over port using this property.
oaam.uio.oam.security.mode	This depends on the Access Manager security transport mode in use. The value can be 1 (for Open), 2 (for Simple), or 3 (for Cert). The default, if not specified, is 1 (Open).

Table C-7 (Cont.) OAAM CLI Properties

Parameter	Details
oam.uio.oam.rootcertificate.keystore.filepath	<p>The location of the Keystore file generated for the root certificate:</p> <p><i>DOMAIN_</i> <i>HOME/output/webgate-ssl/oamclient-truststore.jks</i></p> <p>This is required only for security modes 2 (Simple) and 3 (Cert).</p>
oam.uio.oam.privatekeycertificate.keystore.filepath	<p>The location of the Keystore file generated for private key:</p> <p><i>DOMAIN_</i> <i>HOME/output/webgate-ssl/oamclient-keystore.jks.</i></p> <p>Private key is only required if you set up Access Manager and OAAM in Simple and Cert mode.</p>
oam.csf.useMBeans	<p>For a multiple domain installation, the <code>oam.csf.useMBeans</code> property must be set to true. For information on setting this parameter, see "Set Up the Credential Store Framework (CSF) Configuration" in <i>Administering Oracle Adaptive Access Manager</i>.</p>

5. Save the changes and quit the editor.

6. Set Middleware and Java Home environment variables.

For bash:

```
export ORACLE_MW_HOME=Location_of_WebLogic_installation_where_Oracle_Adaptive_Access_Manager_is_installed
export JAVA_HOME=Location_of_JDK_used_for_the_WebLogic_installation
```

or

For csh:

```
setenv ORACLE_MW_HOME Location_of_WebLogic_installation_where_Oracle_Adaptive_Access_Manager_is_installed
setenv JAVA_HOME Location_of_JDK_used_for_the_WebLogic_installation
```

7. Change directory to `temp/oaam_cli/`.

8. Run the OAAM setup integration script using the following command:

```
./setupOAMTapIntegration.sh conf/bharosa_properties/oaam_cli.properties
```

This script sets the properties required for the integration in OAAM.

9. When the command runs, it prompts you for the following information:

- **Weblogic Server Home Directory:** Usually `$ORACLE_MW_HOME/wlserver_10.3`
- **OAAM Admin server username:** This is the Admin Server user name of the WebLogic Server Domain (WebLogic Admin user name).
- **OAAM Admin server password:** This is the password for the Administration Server user (WebLogic Admin password).
- **OAAM database username:** OAAM database user.

- **OAAM database password:** Password for the OAAM database user.
- Access Manager **WebGate Credentials to be stored in CSF:** Enter WebGate password.
- **Access Manager TAP Key store file password:** The password you assigned when you registered the TAP partner. For information, see [Registering the OAAM Server as a Partner Application to Access Manager](#).

Note: You must provide the WebLogic Admin user name and password when running the `setupOAMTAPIntegration` script. If you provide the OAAM Admin user name and password, the script fails because the OAAM Admin user does not have the permissions required to run the script.

When you set up Access Manager and Oracle Adaptive Access Manager integration in simple or Cert mode, the additional inputs you will have to provide are as follows:

- **Access Manager Private Key certificate Keystore file password:** The Simple Mode Pass Phrase. You can obtain it by executing the WLST command `displaySimpleModeGlobalPassphrase`.
- **Oracle Access Management Global Pass phrase:** The Simple Mode Pass Phrase. You can obtain it by executing the WLST command `displaySimpleModeGlobalPassphrase`.

For information, refer to "Retrieving the Global Passphrase for Simple Mode" in the *Administrator's Guide for Oracle Access Management*.

C.4.14 Configuring the Integration to Use TAPScheme to Protect Identity Management Resources in the IAMSuiteAgent Application Domain

Note: The instructions in this section should only be performed if you want to use TAPScheme in the IAMSuiteAgent application domain.

If you want to protect Identity Management resources in the IAM Suite domain with TAPScheme, proceed as follows:

1. Log in to the Oracle Access Management Console:
`http://oam_adminserver_host:oam_adminserver_port/oamconsole`
2. In the Oracle Access Management Console, click **Application Security** at the top of the window.
3. In the Application Security console, click **Application Domains** in the Access Manager section.
4. In the Search Application Domains page that appears, enter `IAM Suite` in the Name field.
5. Click the **Search** button to initiate the search.
6. Click **IAM Suite** in the Search Results table and click **Edit**.
7. In the IAM Suite Application Domain page, click the **Authentication Policies** tab.

8. Click **Protected HigherLevel Policy** to display its configuration.
9. In the Resources tab, click **/oamTAPAuthenticate** in the Resources table.
10. Click the **Delete** button in the table.
11. Click **Apply** to submit changes and close the confirmation window.
12. In the IAM Suite Application Domain page, click the **Authentication Policies** tab, then click the **Create** button to open the Create Authentication Policy page.
13. Enter a unique name in the Name field.
14. For authentication scheme, choose **LDAPScheme**.
15. Click the **Resources** tab.
16. Click the **Add** button in the Resources tab.
17. Click the **Search** button.
18. Click **/oamTAPAuthenticate** in the Results table.
19. Click **Add Selected**.
20. Click **Apply** to save changes and close the confirmation window.

For Access Manager to be able to override the resource URL before handing it off to OAAM, you must set up the `TAPOverrideResource` challenge parameter in `TAPScheme`.

1. In the Oracle Access Management Console, click **Application Security** at the top of the window.
2. In the Application Security Console, click **Authentication Schemes** in the **Access Manager** section.
3. In the Search Authentication Schemes page, enter `TAPScheme` in the Name field.
4. Click the **Search** button to initiate the search.
5. Choose **TAPScheme** in the Search Results table and click **Edit**.
For specific details on the `TAPScheme`, see "Pre-configured Authentication Schemes" in *Administrator's Guide for Oracle Access Management*.
6. In the Authentication Scheme page, position your cursor in the **Challenge Parameter** field and press **Enter** using your keyboard.
7. In the new line, add
`TAPOverrideResource=http://IAMSuiteAgent:80/oamTAPAuthenticate` for a challenge parameter of `TAPScheme`.
8. Click **Apply** to save changes and close the confirmation window.

C.4.15 Configuring a Resource to be Protected with `TAPScheme`

To protect a resource with the OAAM `TAPScheme`, proceed as follows:

C.4.15.1 Creating a New Resource under the Application Domain

To create a new resource to protect, proceed as follows:

1. In the Oracle Access Management Console, click **Application Security** at the top of the window.
2. In the Application Security console, click **Application Domains** in the Access Manager section.

3. In the Search Application Domains page that appears, enter `IAM Suite` in the Name field.
4. Click the **Search** button to initiate the search.
5. Choose **IAM Suite** in the Search Results table and click **Edit**.
6. In the IAM Suite Application Domain page, click the **Resources** tab, then click **Create** in the Search Results toolbar.
7. In the Resource Definition page, add the following information:

Type: `http`. The HTTP type is the default; it covers resources that are accessed using either the HTTP or HTTPS protocol. Policies that govern a particular resource apply to all operations.

Description: An optional unique description for this resource.

Host identifier: `IAMSuiteAgent`

Resource URL: The URL value must be expressed as a single relative URL string that represents a path component of a full URL composed of a series of hierarchical levels separated by the '/' character. The URL value of a resource must begin with / and must match a resource value for the chosen host identifier.

For example: `/higherriskresource`

Protection Level: `Protected`
8. Click **Apply** to add this resource to the Application Domain.

For information on creating a resource see "Adding and Managing Policy Resource Definitions" in *Administrator's Guide for Oracle Access Management*.

C.4.15.2 Creating a New Authentication Policy that Uses TAPScheme to Protect the Resource

To create a new authentication policy that uses the TAPScheme authentication to protect the resource, proceed as follows:

1. In the Oracle Access Management Console, click **Application Security** at the top of the window.
2. In the Application Security console, click **Application Domains**.
3. In the Search Application Domains page that appears, enter `IAM Suite` in the Name field.
4. Click the **Search** button to initiate the search.
5. Choose **IAM Suite** in the Search Results table and click **Edit**.
6. In the IAM Suite Application Domain page, click the **Authentication Policies** tab, and then click the **Create** button to open the Create Authentication Policy page.
7. In the Create Authentication Policy page, add the required elements for the policy you are creating:

Name: A unique name used as an identifier. For example, `HighPolicy`.

Description (optional): Optional unique text that describes this authentication policy.

Authentication Scheme: `TAPScheme`

Success URL: The redirect URL to be used upon successful authentication.

Failure URL: The redirect URL to be used if authentication fails.

8. On the same page, add the resource you have created:
 - a. Click the **Resources** tab.
 - b. Click the **Add** button in the Resources tab.
 - c. Click the **Search** button to display all the resources available.
 - d. Choose the URL of a resource from those listed. For example, `/higherriskresource`.

The listed URLs were added to this application domain earlier. You can add one or more resources to protect with this authentication policy. The resource definition must exist within the application domain before you can include it in a policy.

- e. Click **Add Selected**.
9. Click **Apply** to save changes and close the confirmation window.
10. In the Create Authentication Policy page, click the **Responses** tab to add responses.

Responses are the obligations (post authentication actions) to be carried out by the Web agent. After successful authentication, the application server hosting the protected application can assert the user identity based on these responses. After a failed authentication, the browser redirects the request to a pre-configured URL

For information on responses, see "Adding and Managing Policy Responses for SSO" in *Administrator's Guide for Oracle Access Management*.

11. Close the page when you finish.

For information on creating an authentication policy for a particular resource, see "Defining Authentication Policies for Specific Resources" in *Administrator's Guide for Oracle Access Management*.

C.4.16 Validating the Access Manager and Oracle Adaptive Access Manager Integration

Try to access the protected resource. You should be redirected to OAAM for registration and challenge. The OAAM login page is shown instead of the Access Manager login page.

C.5 Access Manager and OAAM TAP Integration with DCC WebGate Using Tunneling

This section describes the steps to set up a Detached Credential Collector (DCC) WebGate with tunneling in an environment that has Access Manager integrated with Oracle Adaptive Access Manager using TAP.

For information on credential collection, see the "Understanding Credential Collection and Login" chapter in *Administrator's Guide for Oracle Access Management*.

Prior to configuring Oracle Adaptive Access Manager with Access Manager, you must have installed all the required components, including any dependencies, and configured the environment in preparation of the integration tasks that follow. For prerequisites, see [Section C.4.2, "Prerequisites for OAAM Advanced Integration with Access Manager."](#)

C.5.1 Roadmap for Access Manager and OAAM TAP Integration with DCC WebGate

Table C–8 lists the high-level tasks for integrating Oracle Adaptive Access Manager with Access Manager using TAP with a DCC WebGate.

Table C–8 Integration for Access Manager and Oracle Adaptive Access Manager Using TAP with DCC

Number	Task	Information
1	Integrate Access Manager with OAAM using TAP integration.	For information, see " Integrating Access Manager with OAAM using TAP integration. "
2	Set up a DCC WebGate and enable tunneling.	For information, see " Setting Up a DCC WebGate and Enabling Tunneling. "
3	Configure the /oam resource in the application domain of the DCC WebGate.	For information, see " Configuring Resources in the Application Domain of the DCC WebGate. "
4	Edit the TAP Authentication Scheme to use the DCC WebGate.	For information, see " Editing the TAP Authentication Scheme to Use the DCC WebGate. "
5	Configure an authentication scheme to use the DCC WebGate. This step is performed if you want to set up step up authentication.	For information, see " Configure an Authentication Scheme to Use the DCC WebGate (Optional). "

C.5.2 Integrating Access Manager with OAAM using TAP integration

To integrate Access Manager with OAAM using TAP integration, follow the instructions in [Section C.4, "OAAM Advanced Integration with Access Manager."](#)

C.5.3 Setting Up a DCC WebGate and Enabling Tunneling

To configure a WebGate as a DCC WebGate and enable DCC and tunneling:

1. Install the Oracle HTTP Server WebGate.

Oracle HTTP Server WebGate installation packages are found on media and virtual media that is separate from the core components. You can download the Oracle HTTP Server WebGate software from the Oracle Technology Network (OTN):

<http://www.oracle.com/technetwork/index.html>

For detailed information on installing the Oracle HTTP Server WebGate, see "Installing Oracle HTTP Server 11g WebGate" in *Oracle Fusion Middleware Installing Webgates for Oracle Access Manager*.

2. Log in to the Oracle Access Management Console:

http://oam_adminserver_host:oam_adminserver_port/oamconsole

3. Register the new WebGate with Access Manager. For information, see "Registering an OAM Agent Using the Console" in the *Administrator's Guide for Oracle Access Management*.
4. In the Application Security console, click **Agents** in the Agents section to find and open the registration page for the 11.1.2 Webgate that will function as the DCC.
5. Enable detached credential collection and tunneling on this WebGate as follows:

Table C-9 DCC WebGate Agent Profile Changes

Agent Parameter	Agent Value
User Defined Parameters	TunneledUrls=/oam proxySSLHeaderVar=IS_SSL URLInUTF8Format=true client_request_retry_attempts=1 inactiveReconfigPeriod=10 maxSessionTimeUnits=minutes
Allow Credential Collector Operations	Select this.

6. Click **Apply** to save changes and close the confirmation window.

For more information on configuring 11g WebGates for DCC, see "Enabling DCC Credential Operations" in *Administrator's Guide for Oracle Access Management*.

C.5.4 Configuring Resources in the Application Domain of the DCC WebGate

To configure the /oam resource in the DCC WebGate, proceed as follows:

1. In the Oracle Access Management Console, click **Application Security** at the top of the window.
2. In the Application Security console, click **Application Domains** in the Access Manager section.
3. In the Search Application Domains page that appears, enter the name of the Application Domain related to the DCC WebGate.
4. Click the **Search** button to initiate the search.
5. Choose the Application Domain in the Search Results table and click **Edit**.
6. In the Application Domain page, click the **Resources** tab.
7. Configure the resource /oam/** as a public resources by setting the Authentication Policy as **Public Resource Policy** and the Authorization Policy as **Public Resource Policy**.
8. Set /oam/** to unprotected.
9. Set /favicon.ico as excluded resource.

C.5.5 Editing the TAP Authentication Scheme to Use the DCC WebGate

Edit the TAP Authentication Scheme as follows:

1. In the Oracle Access Management Console, click **Application Security** at the top of the window.
2. In the Application Security Console, click **Authentication Schemes** in the **Access Manager** section.
3. In the Search Authentication Schemes page, enter TAPScheme in the Name field.
4. Click the **Search** button to initiate the search.
5. Choose **TAPScheme** in the Search Results table and click **Edit**.

For specific details on the TAPScheme, see "Pre-configured Authentication Schemes" in *Administrator's Guide for Oracle Access Management*.

6. In the Challenge Redirect URL field, enter:
`http://DCC_WG_host:DCC_WG_port/oam/server/`
7. Click **Apply** to save changes and close the confirmation window.

C.5.6 Configure an Authentication Scheme to Use the DCC WebGate (Optional)

If you want to set up the step-up authentication, create an LDAP scheme as follows:

1. In the Oracle Access Management Console, click **Application Security** at the top of the window.
2. In the Application Security Console, click **Authentication Schemes** in the **Access Manager** section.
3. In the Search Authentication Schemes page, click **Create**.
4. Fill in the Create Authentication Scheme page by supplying the following information:
 - **Name:** DCC Authentication Scheme
 - **Authentication Level:** 2
 - **Challenge Method:** FORM
 - **Challenge Redirect URL:**
`http://DCC_WG_host:DCC_WG_port/oam/server/`
 - **Authentication Module:** LDAPPlugin
 - **Challenge URL:** /pages/login.jsp
 - **Context Type:** Default
 - **Context Value:** /oam
 - **Challenge Parameters:**
`OverrideRetryLimit=0`
5. Click **Apply** to submit the new scheme.
6. Close the confirmation window.

C.6 Other Access Manager and OAAM Integration Configuration Tasks

This section describes other configuration procedures that you may need depending on your deployment.

C.6.1 Changing the Authentication Level of the TAPScheme Authentication Scheme

To change the authentication level of the TAPScheme authentication scheme, proceed as follows:

1. Log in to the Oracle Access Management Console:
`http://oam_adminserver_host:oam_adminserver_port/oamconsole`
2. In the Oracle Access Management Console, click **Application Security** at the top of the window.

3. In the Application Security Console, click **Authentication Schemes** in the **Access Manager** section.
4. In the Search Authentication Schemes page, enter `TAPScheme` in the Name field.
5. Click the **Search** button to initiate the search.
6. Choose **TAPScheme** in the Search Results table and click **Edit**.
For specific details on the TAPScheme, see "Pre-configured Authentication Schemes" in *Administrator's Guide for Oracle Access Management*.
7. Change the authentication level.
8. Click **Apply** to save changes and close the confirmation window.

C.6.2 Setting Up Oracle Adaptive Access Manager and Access Manager Integration When Access Manager is in Simple Mode

To set up Oracle Adaptive Access Manager and Access Manager integration in Simple mode, proceed as follows.

C.6.2.1 Configuring Simple Mode Communication with Access Manager

Securing communication between OAM Servers and clients (WebGates) means defining the transport security mode for the OAP channel within the component registration page. The transport security communication mode is chosen during Access Manager installation. In Simple mode, the installer generates a random global passphrase initially, which can be edited as required later.

Simple mode is used if you have some security concerns, such as not wanting to transmit passwords as plain text, but you do not manage your own Certificate Authority (CA). In this case, Access Manager 11g Servers and WebGates use the same certificates, issued and signed by Oracle CA.

For information on configuring Access Manager for Simple mode communication, see *Administrator's Guide for Oracle Access Management*.

C.6.2.2 Setting OAAM Properties for Access Manager for Simple Mode

Follow the steps in [Section C.4.13, "Setting Up Access Manager TAP Integration Properties in OAAM."](#) When you edit the `oaam_cli.properties` file, set the following properties in addition to ones specified in [Table C-7](#).

Table C-10 Properties for Security Mode

Parameters	Details
oaam.uio.oam.security.mode	This depends on the Access Manager security transport mode in use. The value can be 1 (for Open), 2 (for Simple), or 3 (for Cert). The default, if not specified, is 1 (Open).
oaam.uio.oam.rootcertificate.keystore.filepath	The location of the Keystore file generated for the root certificate: <i>DOMAIN_</i> <i>HOME/output/webgate-ssl/oaamclient-truststore.jks</i> This is required only for security modes 2 (Simple) and 3 (Cert).
oaam.uio.oam.privatekeycertificate.keystore.filepath	The location of the Keystore file generated for private key: <i>DOMAIN_</i> <i>HOME/output/webgate-ssl/oaamclient-keystore.jks</i> This is required for security modes 2 (Simple) and 3 (Cert)

C.6.3 Configuring Identity Context Claims in the Access Manager and OAAM TAP Integration

Identity Context allows organizations to meet growing security threats by leveraging the context-aware policy management and authorization capabilities built into the Oracle Access Management platform. Identity Context secures access to resources using traditional security controls (such as roles and groups) as well as dynamic data established during authentication and authorization (such as authentication strength, risk levels, device trust and the like).

To use identity context claims in the Access Manager and OAAM TAP integration, follow the below steps:

1. In *Domain_Home/config/fmw-config/oaam-config.xml*, search for the setting with the TAP partner name. You would have specified the TAP Partner name while registering the TAP partner for Access Manager. For example, *OAAMPartner*. Change the OAAM partner's *TapTokenVersion* from *v2.0* to *v2.1*.
2. Change the version setting on the OAAM side from *v2.0* to *v2.1* by adding/editing a property through the OAAM Administration Console. To do this, proceed as follows:
 - a. Log in to the OAAM Administration Console:
http://oaam_managed_server_host:oaam_admin_managed_server_port/oaam_admin
 - b. In the left pane, click **Environment** and double-click **Properties**. The Properties search page is displayed.
 - c. Search for property with the name *oaam.uio.oam.dap_token.version* and set its value to *v2.1*.
 - d. In case the property does not exist, add a new property with the name *oaam.uio.oam.dap_token.version* and the value as *v2.1*.
 - e. Click **Save**.
3. In the TAP Scheme of the Access Management policy, add the following challenge parameter:

TAPOverrideResource=http://IAMSuiteAgent:80/oamTAPAuthenticate. To do that, proceed as follows:

- a. Log in to the Oracle Access Management Console:
`http://oam_adminserver_host:oam_adminserver_port/oamconsole`
- b. In the Oracle Access Management Console, click **Application Security** at the top of the window.
- c. In the Application Security Console, click **Authentication Schemes** in the **Access Manager** section.
- d. In the Search Authentication Schemes page, enter TAPScheme in the Name field.
- e. Click the **Search** button to initiate the search.
- f. Choose **TAPScheme** in the Search Results table and click **Edit**.
 For specific details on the TAPScheme, see "Pre-configured Authentication Schemes" in *Administrator's Guide for Oracle Access Management*.
- g. In the Authentication Scheme page, position your cursor in the **Challenge Parameter** field and press **Enter** using your keyboard.
- h. In the new line, add
`TAPOverrideResource=http://IAMSuiteAgent:80/oamTAPAuthenticate` for a challenge parameter of TAPScheme.
- i. Click **Apply** to save changes and close the confirmation window.

C.6.4 Enabling Oracle Adaptive Access Manager to Transfer Data to Access Manager over HTTP Post-Based Front Channel

The Access Manager and Oracle Adaptive Access Manager integration flow involves transferring information required to perform authentication, preserving Access Manager context information, providing the TAP token, and so on.

During this integration flow, Access Manager can preserve its context as a cookie. In cases where this context is large such as form data, Access Manager can send its context information through POST data to Oracle Adaptive Access Manager and Oracle Adaptive Access Manager can transfer this data back to Access Manager over an HTTP POST-based front channel message. The mechanism used in the Oracle Adaptive Access Manager side to preserve Access Manager context allows preserving at least 8K of data. This ensures that Access Manager can preserve the end application's form data during re-authentication so the end user does not have to retype it again.

For Oracle Adaptive Access Manager to be able to generate a POST-based response back to Access Manager and preserve at least 8K of Access Manager's context data, you must set `oam.uio.oam.dopost` to `true`.

To change the setting, proceed as follows:

1. Log in to the OAAM Administration Console:
`http://oam_managed_server_host:oam_admin_managed_server_port/oam_admin`
2. In the left pane, click **Environment** and double-click **Properties**. The Properties search page is displayed.
3. Search for property with the name `oam.uio.oam.dopost` and set its value to `true`.

4. In case the property does not exist, add a new property with the name `oaam.uio.oam.dopost` and the value as `true`.
5. Click **Save**.

C.6.5 Disabling OAAM Administration Console Protection

You can disable OAAM Administration Console protection by disabling the IAMSuiteAgent that protects it.

To do so, either the `WLSAGENT_DISABLED` system property or environment variable must be set to `true` for the servers on which the agent should be disabled.

For instructions on disabling the IAMSuiteAgent, see "Disabling IAMSuiteAgent" in *Administrator's Guide for Oracle Access Management*.

C.6.6 Disabling Step Up Authentication

If you want to disable the Step Up Authentication scenario, the following property has to be set to `false`:

```
oaam.uio.oam.integration.stepup.enabled
```

By default this property is set to `true`. To change the setting on the Oracle Adaptive Access Manager side by adding/editing a property through the OAAM Administration Console, proceed as follows:

1. Log in to the OAAM Administration Console.

```
http://oaam_managed_server_host:oaam_admin_managed_server_port/oaam_admin
```

2. In the left pane, click **Environment** and double-click **Properties**. The Properties search page is displayed.
3. Search for property with the name `oaam.uio.oam.integration.stepup.enabled` and set its value to `false`.

In case the property does not exist, add a new property.

If set to `false`, the user is prompted for credentials when he tries to access a higher protected resource after he had been authenticated for the lower protected resource.

4. Click **Save**.

C.6.7 Changing the Oracle Adaptive Access Manager Password Length Limit

Oracle Adaptive Access Manager accepts a limit of 25 characters for passwords. If users log in to OAAM Server for the first time and the password they enter is more than 25 bytes, they are returned to the user name page with an error that their password is invalid.

To change the character limit for passwords entered in to OAAM Server, you must update the following property using the OAAM Administration Console:

```
bharosa.authentipad.textpad.datafield.maxLength
```

Instructions to update the character limit using the OAAM Administration Console are as follows:

1. Log in to the OAAM Administration Console:

`http://oaam_managed_server_host:oaam_admin_managed_server_port/oaam_admin`

2. In the left pane, click **Environment** and double-click **Properties**. The Properties search page is displayed.
3. Search for property with the name `bharosa.authentipad.textpad.datafield.maxLength` and change its value.
4. Click **Save**.

C.6.8 Adding Customizations Using the OAAM Extensions Shared Library

If you are configuring integration with Access Manager 11g using the TAP scheme and adding customizations using the OAAM Extensions Shared Library, the property `bharosa.uio.proxy.mode.flag` must be set to `false`.

If the property is set to `true`, the Oracle Adaptive Access Manager and Access Manager integration using TAP will fail with the following message:

Sorry, the identification you entered was not recognized.

In cases where the property has been set to `true`, change the setting as follows:

1. Log in to the OAAM Administration Console:

`http://oaam_managed_server_host:oaam_admin_managed_server_port/oaam_admin`

2. In the left pane, click **Environment** and double-click **Properties**. The Properties search page is displayed.
3. Search for property with name `bharosa.uio.proxy.mode.flag` and set its value to `false`.
4. In cases where the property does not exist, add a new property with the name `bharosa.uio.proxy.mode.flag` and the value as `false`.
5. Click **Save**.

For information on Oracle Adaptive Access Manager customization, see:

- "Using the OAAM Extensions Shared Library to Customize OAAM" in *Developer's Guide for Oracle Adaptive Access Manager*
- "Customizing OAAM Web Application Pages" in *Developer's Guide for Oracle Adaptive Access Manager*

C.6.9 Enabling the Single Login Page Flow

For details, see "Enabling the Single Login Page Flow" in *Developer's Guide for Oracle Adaptive Access Manager*.

C.7 Resource Protection Scenario

This scenario illustrates an example where a user changes the authentication levels for the TAPScheme. Login and Step Up authentication flows are also illustrated based on these settings.

C.7.1 Resource Protection Scenario: Changing Authentication Level of TAPScheme

To change the authentication level, proceed as follows:

1. Log in to the Oracle Access Management Console:
`http://oam_adminserver_host:oam_adminserver_port/oamconsole`
2. In the Oracle Access Management Console, click **Application Security** at the top of the window.
3. In the Application Security Console, click **Authentication Schemes** in the **Access Manager** section.
4. In the Search Authentication Schemes page, enter `TAPScheme` in the Name field.
5. Click the **Search** button to initiate the search.
6. Choose **TAPScheme** in the Search Results table and click **Edit**.
For specific details on the TAPScheme, see "Pre-configured Authentication Schemes" in *Administrator's Guide for Oracle Access Management*.
7. Increase the value for the Authentication Level. For example if the value is 2, change it to 4.
TAPScheme will be protecting the higher protected resource.
8. Click **Apply** to save the changes.
9. In the Search Authentication Schemes page, search for **OAMAdminConsoleScheme**.
10. Click the **OAMAdminConsoleScheme** link.
11. Ensure that the Authentication Level value is lower than that of TAPScheme.
OAMAdminConsoleScheme will be protecting the lower protected resource.

C.7.2 Resource Protection Scenario: Removing OAAM Administration Console from Protected Higher Level Policy

In this example, the OAAM Administration Console is moved from the Protected Higher Level Policy.

1. In the Oracle Access Management Console, click **Application Security** at the top of the window.
2. In the Application Security console, click **Application Domains** in the Access Manager section.
3. In the Search Application Domains page that appears, enter `IAM Suite` in the Name field.
4. Click the **Search** button to initiate the search.
5. Choose **IAM Suite** in the Search Results table and click **Edit**.
6. In the IAM Suite Application Domain page, click the **Resources** tab, then click **Create** in the Search Results toolbar.
7. Click the **Authentication Policies** tab.
8. Click **Protected HigherLevel Policy** to display its configuration.
9. In the Resources tab, remove `/oam_admin/**` and click **Apply** to apply the change.

C.7.3 Resource Protection Scenario: Creating a New Policy that Uses TAPScheme to Protect the Resource

Create a new policy with TAPScheme and protect Oracle Adaptive Access Manager as a higher protected resource.

1. Click the **Authentication Policies** tab, then click the **Create** button to open the Create Authentication Policy page.
2. Specify a policy name in the Name field. For example, `TestPolicy`.
3. In Authentication Scheme, select **TAPScheme** from the Authentication Scheme drop-down list.
4. Add resources:
 - a. Click the **Resources** tab in the Authentication Policy page.
 - b. Click the **Add** button in the Resources tab.
 - c. Click the **Search** button.
 - d. Select `/oaam_admin/**` as the resource.
 - e. Click **Add Selected**.
5. Click **Apply** to create the authentication policy.

Now the higher protected resource is the OAAM Administration Console protected by TAPScheme and the lower protected resource is the Oracle Access Management Console protected by OAMAdminConsoleScheme.

C.7.4 Resource Protection Scenario: Creating a New OAAM User

For information on creating a user, see [Section C.4.4, "Creating the OAAM Users and OAAM Groups."](#)

C.7.5 Resource Protection Scenario: Login Flow

This section presents an example of a Login flow where the user registers his virtual authentication device and challenge questions. The example is based on the setup that was performed in [Section C.7.1, "Resource Protection Scenario: Changing Authentication Level of TAPScheme"](#) through [Section C.7.4, "Resource Protection Scenario: Creating a New OAAM User."](#)

In this example, the higher protected resource is the OAAM Administration Console protected by TAPScheme and the lower protected resource is the Oracle Access Management Console protected by OAMAdminConsoleScheme.

The Login flow is as follows:

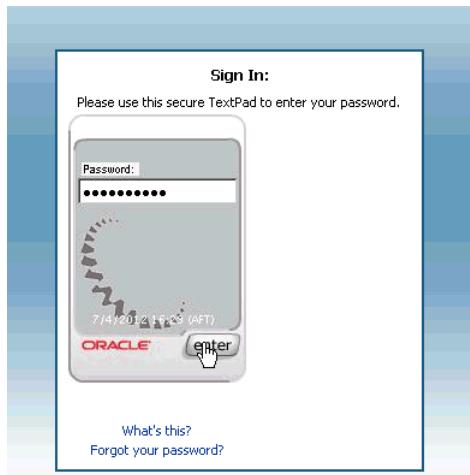
1. Access the protected resource, the OAAM Administration Console, by entering its URL in a web browser.
The Access Manager user name page appears.
You are redirected to OAAM Server.
2. In the Access Manager user name page, as shown in [Figure C-1](#), enter the user name and click **Continue**.

Figure C-1 Access Management User Name Page



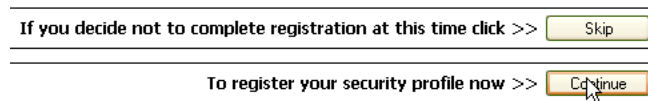
3. The Password page appears with TextPad for you to enter the password, as shown in [Figure C-2](#). Enter the password and click **Enter**.

Figure C-2 Password Page with TextPad



4. In the Registration page, click **Continue** for the option to begin registering a profile for the user, as shown in [Figure C-3](#).

Figure C-3 Register Profile



5. In the Security Device registration page, as shown in [Figure C-4](#), select your security device and click **Continue**.

Figure C-4 Security Device Selection

6. In the Security Questions registration page register challenge questions.

Figure C-5 Challenge Question Registration

Security Questions

We will use your security questions and answers to confirm your identity at times when extra safety is needed.

Questions (Choose a question from each list below.)

1)

2)

3)

Answers

7. You are allowed to access the protected resource, the OAAM Administration Console.

Figure C–6 OAAM Administration Console Cases Page: Accessing the Protected Resource

The screenshot displays the 'Cases' page in the OAAM Administration Console. At the top, there are tabs for 'Cases', 'Sessions', and 'Search Transact...'. Below the tabs, there is a 'New Case' button. The main area is a search tool with the instruction: 'Use the search tool to find cases or click the New Case button to create a new case.' The search tool includes a 'Search' dropdown, a 'Saved Search' field, and a 'Search Cases' button with a checkmark. A '* Required' label is present. The search criteria are organized into two columns:

- Left Column:** Organization ID (dropdown), User Name (text), User ID (text), Case ID (text), Description (text), Case Type (dropdown), Severity Level (dropdown), Case Status (dropdown).
- Right Column:** Expired (dropdown), Create Date (range: 2012-07-03 05:01:01 AM to 2012-07-04 11:59:59 PM), Disposition (dropdown), Last Action (dropdown), Notes (text), Created By (text), Current Owner (dropdown).

Buttons for 'Search', 'Reset', and 'Save...' are located at the bottom right of the search tool. Below the search tool is the 'Search Results' section, which includes a toolbar with 'Actions', 'View', 'Create Like', 'Bulk Edit', 'Export to spreadsheet', and 'Detach'. A table header is visible with columns: Row/Case ID, User Name, Description, Case Type, Last Action, Case Severity, Case Status, Last Action Date, and Expiration Date. A note below the table reads: 'Click the Search button with appropriate search criteria.'

C.7.6 Resource Protection Scenario: Step Up Authentication Flow

This section presents an example of the Step Up Authentication flow for the user who registered his profile and was allowed access to the higher protected resource in [Section C.7.5, "Resource Protection Scenario: Login Flow."](#) The example is based on the setup performed in [Section C.7.1, "Resource Protection Scenario: Changing Authentication Level of TAPScheme"](#) through [Section C.7.4, "Resource Protection Scenario: Creating an New OAAM User."](#)

In this example, the higher protected resource is the OAAM Administration Console protected by TAPScheme and the lower protected resource is the Oracle Access Management Console protected by OAMAdminConsoleScheme.

The Step Up Authentication flow is as follows:

1. Access the lower protected resource, the Oracle Access Management Console, by entering the URL in a web browser.

At this point in the Step Up example, you have not been authenticated yet. When you access the lower risk resource, you are shown the Oracle Access Management login page, which has the user name and password on the same page.

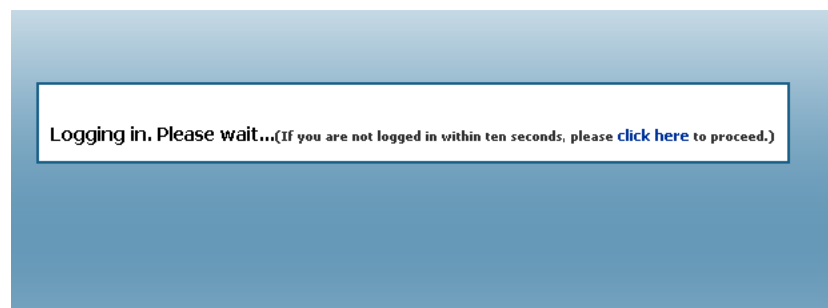
Figure C–7 Access Management Login: Logging In to the Lower Risk Resource

The screenshot shows a login page with a blue border. At the top, it says 'Welcome'. Below that, it says 'Enter your Single Sign-On credentials below'. There are two input fields: 'Username:' and 'Password:'. A 'Login' button is located at the bottom right of the form area.

2. Enter the credentials of the user who has registered a profile (see [Section C.7.5, "Resource Protection Scenario: Login Flow"](#)) and click **Login**.
3. After providing credentials and being successfully authenticated, you now have access to the lower protected resource. The Oracle Access Management Console, as shown.
4. Access the higher protected resource, the OAAM Administration Console, by entering the URL in a Web browser.

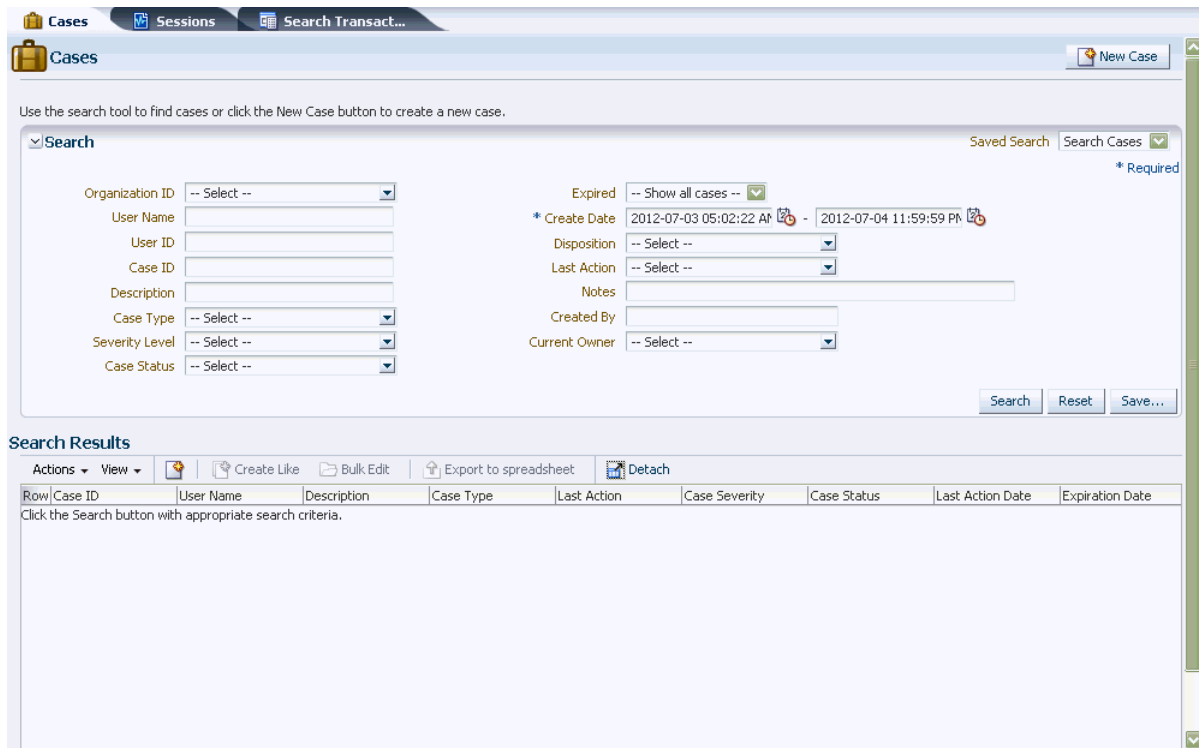
Since you have already been authenticated, OAM Server does not present the Login page. However, Oracle Adaptive Access Manager will run its fraud detection policies. In this example, Oracle Adaptive Access Manager runs the post-authentication rules and determines that your risk score is low, so it does not execute any actions (for example, KBA or OTP) or generate any alerts that were specified in the policy. [Figure C-8](#) shows the Step Up Authentication process where you are being logged in to the higher protected resource since you have already been authenticated earlier when you accessed the lower protected resource, and the post-authentication rules have determined that your risk score is low.

Figure C-8 Step Up Authentication: Log In to the Higher Protected Resource



You now have access to the higher protected resource, the OAAM Administration Console.

Figure C–9 Higher Protected Resource



C.8 Troubleshooting Common Problems

This section describes common problems you might encounter in an Oracle Adaptive Access Manager and Access Manager integrated environment and explains how to solve them. It is organized by common problem types and contains the following topics

- [OAAM Basic Integration with Access Manager](#)
- [Login Failure](#)
- [Identity Store](#)
- [Miscellaneous](#)

In addition to this section, review the *Oracle Fusion Middleware Error Messages Reference* for information about the error messages you may encounter.

For information about additional troubleshooting resources, see [Section 1.7, "Using My Oracle Support for Additional Troubleshooting Information."](#)

C.8.1 OAAM Basic Integration with Access Manager

This provides solutions for integration issues pertaining to OAAM Basic integration with Access Manager.

C.8.1.1 Internet Explorer 7 and OAAM Basic Integration with Access Manager

In the OAAM Basic integration with Access Manager, you are forwarded to the OAAM page when you access a protected resource.

Cause

If you are using Microsoft Internet Explorer 7, when you enter a user name and click **Submit**, you are stuck on the next page (/oam/pages/oaam/handleLogin.jsp) instead of being redirected to the password page automatically.

Solution

To resolve this problem, you can use the following workaround.

Click the **Continue** link to take you to

/oam/pages/oaam/handleJump.jsp?clientOffset=-7.

C.8.1.2 Access Manager and Oracle Adaptive Access Manager Integration and Changes in the Console

An error occurs during the OAAM Basic integration with Access Manager flow.

Cause

The OAAMEnabled value is configured incorrectly.

Solution

In an environment where OAAM Basic integration with Access Manager is enabled, the following entry OAAMEnabled under oam-config.xml must be set to true:

```
<Setting Name="OAAM" Type="htf:map">
  <Setting Name="OAAMEnabled" Type="xsd:boolean">true</Setting>
</Setting>
...
```

If an error occurs in OAAM Basic integration with Access Manager flows, check the value of this flag. In certain environments (Windows) or scenarios, such as creating a new Oracle Internet Directory and associating it with the OAAMBasic scheme, the original flows might be broken. OAAM Basic integration with Access Manager does not work because the OAAMEnabled flag is reset to false.

C.8.1.3 OTP Challenge Not Supported in OAAM Basic integration with Access Manager

In OAAM Basic integration with Access Manager, during registration with Access Manager after registering the challenge questions, you are forwarded to a contact page to enter a mobile number.

In this mode of integration, with OTP unsupported, this page is not significant. You complete the registration by entering a mobile number in the following form, and **Submit**.

:09900502139

Cause

The OAAM Challenge SMS policy has been configured to run instead of the OAAM Challenge policy.

Solution

To resolve this issue, replace the OAAM Challenge SMS policy with the OAAM Challenge policy, to prevent a challenge flow request to OTP:

1. Search for OAAM Challenge Policy.

2. Under Action Group, replace **OAAM Challenge SMS** with **OAAM Challenge** every where you find it.
3. Save the policy.

C.8.1.4 Using ConfigureOAAM WLST Command to Create the Data Source in OAAM Basic Integration with Access Manager

You can use the `configureOAAM WLST` command to create the data source, associate it as a target with the OAM Server, and the `OAAMEnabled` property in the `oam-config.xml` file. The syntax is as follows:

```
configureOAAM(dataSourceName,paramNameValueList)
```

where:

- `dataSourceName` is the name of the data source to be created
- `paramNameValueList` is a comma-separated list of parameter name-value pairs. The format of each name-value pair is as follows:

```
paramName='paramValue'
```

The mandatory parameters are:

- `hostName`: The name of the database host
- `port`: The database port
- `sid`: The database identifier (database sid)
- `userName`: The OAAM schema name
- `passWord`: The OAAM schema password

The optional parameters are:

- `maxConnectionSize`: The maximum connection reserve time out size
- `maxPoolSize`: The maximum size of connection pool

For example:

```
configureOAAM(dataSourceName = "MyOAAMDS", hostName = "host.mycorp.example.com",
port = "1521", sid = "sid", userName = "username", passWord = "password",
maxConnectionSize = None, maxPoolSize = None, serverName = "oam_server1")
```

Note: SID = requires the service name.

C.8.2 Login Failure

This section provides solutions for login issues.

C.8.2.1 Login Page Does Not Display Error

When the OAM login page is tunneled (`/oam/**`), the login page does not display an error message when the login fails.

Cause

The resources in the Application Domain of the DCC WebGate were not configured correctly.

Solution

You must configure the properties in the Application Domain of the DCC WebGate as follows:

```
/oam/** as an unprotected resource
/favicon.ico as an excluded resource
```

C.8.2.2 Non-ASCII Credentials

When using a non-ASCII user name or password in the native authentication flow, a message similar to the following is displayed:

```
Sorry, the identification you entered was not recognized. Please try again.
```

Cause

The non-ASCII characters are in the credentials.

Solution

To resolve the problem:

1. Set the `PRE_CLASSPATH` variable to `${ORACLE_HOME}/common/lib/nap-api.jar`.

For C shell:

```
setenv ORACLE_HOME "IAMSUITE INSTALL DIR"
setenv PRE_CLASSPATH "${ORACLE_HOME}/common/lib/nap-api.jar"
```

For bash/ksh shell:

```
export ORACLE_HOME=IAMSUITE INSTALL DIR
export PRE_CLASSPATH="${ORACLE_HOME}/common/lib/nap-api.jar"
```

2. Start the managed server related to `OAAM_SERVER`.

C.8.2.3 Mixed Case Logins

After successful authentication on Access Manager and Oracle Adaptive Access Manager, a registered user was asked to register his profile again after he entered his mixed-case user name in a different case combination than what he registered.

Cause

The user name is case-sensitive. By default, if a user enters a mixed-case user name in a case combination that is different from the registered user, the OAAM Server will consider the user to be unregistered. For example, if user `userxy` tries to log in by entering user name `userXY`, he will be asked to register his profile again.

Solution

To ensure that logins are successful on both OAM Server and OAAM Server, you must configure the OAAM Server to consider user names as case-insensitive. To achieve this set the following property:

```
bharosa.uio.default.username.case.sensitive=false
```

Change the setting as follows:

1. Log in to the OAAM Administration Console:

```
http://oaam_managed_server_host:oaam_admin_managed_server_port/oaam_admin
```

2. In the left pane, click **Environment** and double-click **Properties**. The Properties search page is displayed.
3. Search for property with name `bharosa.uio.default.username.case.sensitive` and set its value to `false`.
4. In cases where the property does not exist, add a new property with the name `bharosa.uio.default.username.case.sensitive` and the value as `false`.
5. Click **Save**.

C.8.2.4 Cookie Domain Definition

Incorrect value of the cookie domain in your configuration can result in login failure.

For correct WebGate operation, ensure that the property `oaam.uio.oam.obsso_cookie_domain` is set to match the corresponding value in Access Manager.

In the agent configuration page in the Oracle Access Management Console, the Primary Cookie Domain parameter describes the Web server domain on which the Agent is deployed, for instance, `.example.com`. The cookie domain was configured to enable single sign-on among Web servers. The Web servers for which you configure single sign-on must have the same Primary Cookie Domain value. WebGate uses this parameter to create the ObSSOCookie authentication cookie.

To change the `oaam.uio.oam.obsso_cookie_domain` setting as follows:

1. Log in to the OAAM Administration Console:
`http://oaam_managed_server_host:oaam_admin_managed_server_port/oaam_admin`
2. In the left pane, click **Environment** and double-click **Properties**. The Properties search page is displayed.
3. Search for property with name `oaam.uio.oam.obsso_cookie_domain` and set its value to match the Primary Cookie Domain setting.
4. Click **Save**.

C.8.2.5 OAAM Test Login URL /oaam_server Fails After Access Manager and Oracle Adaptive Access Manager Integration

The test login URL `/oaam_server` is used to verify that the Oracle Adaptive Access Manager configuration is working before proceeding with the integration of Access Manager and Oracle Adaptive Access Manager using the TAP scheme. This URL is not intended for use after the integration, at which point, the user should not have direct access to the OAAM Server. If the user navigates to the URL and enters his user name, he is directed to the page where the password is entered. After submitting the password, the login will fail and the following error will be displayed:

Error Sorry, the identification you entered was not recognized. Please try again

C.8.2.6 Login to a Protected Resource May Fail in an Access Manager Release 2 PS2 and Oracle Adaptive Access Manager Release 2 TAP Integrated Environment

Log in to a protected resource may fail with an invalid class exception in an Access Manager Release 2 PS2 and Oracle Adaptive Access Manager Release 2 TAP integrated environment if a user session is still active prior to the Access Manager upgrade from Release 2 to Release 2 PS2 and the pre-upgrade session information is used post-upgrade. For the integration to work properly, before shutting down or starting the servers prior to the upgrade, you must stop all existing stale pre-upgrade sessions

by clicking **Delete All User Sessions** in the Session Management page. For more information about session management, refer to the "About the Session Management Pages" section in the "Maintaining Access Manager Sessions" chapter of the *Administrator's Guide for Oracle Access Management 11g Release 2*.

C.8.3 Identity Store

This section provides solutions for identity store issues.

C.8.3.1 Username Attribute Incorrect Setting

The user experiences a login failure.

Cause

If the username attribute in the identity store is not `cn`, a login failure occurs.

Solution

To fix this problem, proceed as follows:

1. Log in to the Oracle Access Management Console:

```
http://oam_adminserver_host:oam_adminserver_port/oamconsole
```

2. In the Oracle Access Management Console, click **Application Security** at the top of the window.
3. In the Application Security Console, click **Authentication Schemes** in the **Access Manager** section.
4. In the Search Authentication Schemes page, enter `TAPScheme` in the Name field.
5. Click the **Search** button to initiate the search.
6. Choose **TAPScheme** in the Search Results table and click **Edit**.

For specific details on the TAPScheme, see "Pre-configured Authentication Schemes" in *Administrator's Guide for Oracle Access Management*.

7. In the Authentication Scheme page, position your cursor in the **Challenge Parameter** field and press **Enter** using your keyboard.
8. Add the challenge parameter `MatchLDAPAttribute` and set the value to the username attribute specified in your identity store. The challenge parameter is case-sensitive so ensure that you have enter it correctly.

For example, you could set it to `uid, mail, cn`, and so on

If the username attribute is `uid`, you would add `MatchLDAPAttribute=uid`

Note: To add another parameter to an existing parameter, you must position your cursor in the **Challenge Parameter** field and press **Enter** using your keyboard.

9. Click **Apply** to submit the change.

C.8.3.2 In the Access Manager and Oracle Adaptive Access Manager Integration TAP Could Not Modify User Attribute

Authentication succeeds but the final redirect fails with the following errors:

```
Module oracle.oam.user.identity.provider
Message Principal object is not serializable; getGroups call will result in
an extra LDAP call
```

```
Module oracle.oam.engine.authn
Message Cannot assert the username from DAP token
```

```
Module oracle.oam.user.identity.provider
Message Could not modify user attribute for user : cn, attribute :
userRuleAdmin, value : {2} .
```

Cause

In integration scenarios coupled with multiple identity stores, the user identity store that is set as the Default Store is used for authentication and assertion.

For the Access Manager and Oracle Adaptive Access Manager integration which uses the TAP, the assertion for the TAPScheme Authentication scheme is made against the Default Store. In this case the backend channel authentication made against the LDAP module uses a specific user identity store (OID, for example). When the user name is returned to Access Manager, the assertion occurs against the Default Store (not the same OID that was used for the authentication).

Note: For Session Impersonation, the Oracle Internet Directory instance that is used for the user and grants must be the Default Store.

Solution

If you change the Default Store to point to a different store, ensure that TAPScheme also points to same store.

C.8.3.3 No Synchronization Between Database and LDAP

Registered status records remain in the OAAM database even if registered users are removed from LDAP. When the user is added to LDAP again, the old image, phrase, and challenge questions are used, because the OAAM database and LDAP are not synchronized.

C.8.4 Miscellaneous

This section provides solutions and tips for miscellaneous issues.

C.8.4.1 Multiple Sessions Created for a Particular User Instead of a Unified Session

In an Access Manager and OAAM integrated environment, if multiple sessions are created instead of a unified session for a particular user, set the following OAAM property to work around this issue:

```
oam.uio.oam.authenticate.withoutsession=false
```

C.8.4.2 Integration Failure Due to Network Delay

Increase `TokenValiditySeconds` using Oracle Access Management Console if the integration fails.

1. Log in to the Oracle Access Management Console:

```
http://oam_adminserver_host:oam_adminserver_port/oamconsole
```


2. In the Oracle Access Management Console, click **Application Security** at the top of the window.
3. In the Application Security Console, click **Authentication Schemes** in the **Access Manager** section.
4. In the Search Authentication Schemes page, enter `TAPScheme` in the Name field.
5. Click the **Search** button to initiate the search.
6. Choose **TAPScheme** in the Search Results table and click **Edit**.

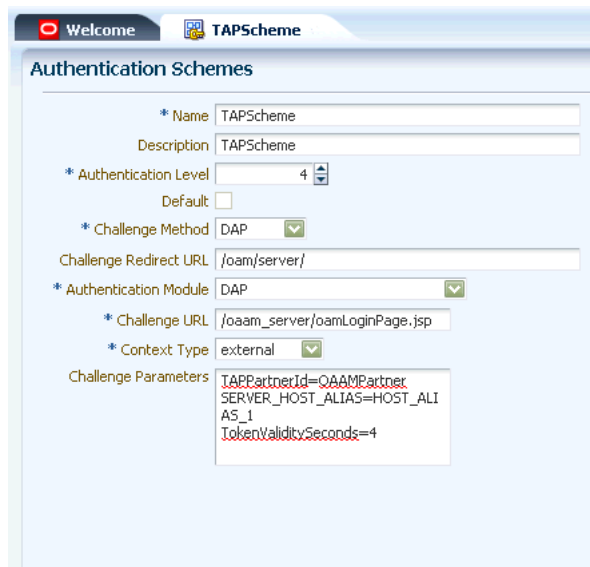
For specific details on the TAPScheme, see "Pre-configured Authentication Schemes" in *Administrator's Guide for Oracle Access Management*.

7. Add the challenge parameter `TotalValiditySeconds` and set the value to the desired number. The default value is 1 second. The challenge parameter is case-sensitive so ensure that you have entered it correctly.

For example, `TotalValiditySeconds=4`

Note: To add a parameter when there are existing parameters, you must position your cursor in the **Challenge Parameter** field and press **Enter** using your keyboard, and then enter the new parameter.

Figure C–10 TAPScheme Authentication Scheme



8. Click **Apply** to apply the changes.

C.8.4.3 Changing the TAP Token Version to 2.1

The `oam-config.xml` file contains all Access Manager-related system configuration data and is located in the `DOMAIN_HOME/config/fmwconfig` directory.

1. Open the `oam-config.xml` file in a text editor.

```
vi DOMAIN_HOME/config/fmwconfig/oam-config.xml
```

2. Search for `OAAMPartner`.

3. Change the value of the `TapTokenVersion` from `v2.0` to `v2.1`.
4. Save the changes.
`:wq!`
5. Log in to the OAAM Administration Console.
`http://oam_managed_server_host:oam_admin_managed_server_port/oam_admin`
6. In the left panel, click **Properties** under the Environment node.
7. Click the **New Property** button in the Properties page.
8. Specify the new property as:
Name: `oam.uio.oam.dap_token.version`
Value: `v2.1`
9. Click **Create**.
10. Log in to the Oracle Access Management Console.
`http://oam_adminserver_host:oam_adminserver_port/oamconsole`
11. In the Oracle Access Management Console, click **Application Security** at the top of the window.
12. In the Application Security Console, click **Authentication Schemes** in the **Access Manager** section.
13. In the Name field, enter `TAPScheme` as the target scheme name.
14. Click the **Search** button to initiate the search.
15. In the list of search results, select **TAPScheme** as the target scheme.
16. Add the challenge parameter
`TAPOverrideResource=http://IAMSuiteAgent:80/oamTAPAuthenticate`. The challenge parameter is case-sensitive so ensure that you have enter it correctly.

Note: To add a parameter when there are existing parameters, you must position your cursor in the **Challenge Parameter** field and press **Enter** using your keyboard, and then enter the new parameter.

17. Click **Apply** to apply the changes.

C.8.4.4 Resource Protected by OAAMAdvanced Scheme Is Not Accessible in Access Manager 11.1.1.4.0 and OAAM 11.1.1.5.0 Integration

You cannot access a resource protected by the OAAMAdvanced authentication scheme in an Access Manager 11.1.1.4.0 and OAAM 11.1.1.5.0 integration.

Cause

In an Access Manager 11.1.1.4.0 and OAAM 11.1.1.5.0 integration, you must set the WebGate password for OAAM and several parameters in addition to those documented in this chapter in order for the integration to work properly.

Solution

To resolve this problem:

- Set the WebGate password for OAAM.
- Set `oaam.uio.oam.authenticate.withoutsession` to `false`. By default, this is set to `true`.

C.8.4.5 Additional Properties to Set If Using OAAMAdvanced Scheme

If you are using the `OAAMAdvanced` scheme in OAAM Advanced integration with Access Manager, ensure that these properties are set:

- For Access Management 11g:
`oaam.uio.oam.authenticate.withoutsession = false`
- For Access Management 11g and 10g:
`oracle.oam.httputil.usecookieapi = true`

C.8.4.6 Accessing LDAP Protected Resource as a Test

When setting up the environment, you may want to first verify that you can access a page protected by Access Manager using the LDAP authentication scheme. If you cannot access the page, try to resolve this issue before proceeding with the configuration.

Using the `idmConfigTool` Command

The IdM configuration tool (`idmConfigTool`) performs a number of tasks to assist in installing, configuring, and integrating Oracle identity management (IdM) components. This appendix explains how to use the tool.

-
-
- Notes:**
- This appendix does not contain actual integration procedures; rather, it contains `idmConfigTool` command syntax and related details. Use this appendix as a reference whenever you are executing `idmConfigTool` as directed by your integration procedure or task.
 - Ensure that the LDAP server, as well as the admin servers hosting OAM, OIM are up before you run `idmConfigTool`
-
-

This appendix contains these sections:

- [About `idmConfigTool`](#)
- [Set Up Environment Variables](#)
- [Syntax and Usage](#)
- [Command Options and Properties](#)
- [Additional Tasks for OUD Identity Store in an HA Environment](#)

D.1 About `idmConfigTool`

This section contains these topics:

- [When to Use the Tool](#)
- [Tasks performed by the Tool](#)
- [Components Supported by `idmConfigTool`](#)
- [Location of `idmConfigTool`](#)
- [Webgate Types Supported](#)
- [Single- and Cross-Domain Scenarios](#)

D.1.1 Components Supported by `idmConfigTool`

`idmConfigTool` supports these 11g components:

- Oracle Internet Directory

- Oracle Virtual Directory
- Oracle Access Management Access Manager
- Oracle Identity Manager
- Oracle Unified Directory (OUD)
- Oracle Access Management Mobile and Social

D.1.2 When to Use the Tool

Use `idmConfigTool` in these situations:

- Prior to installing Oracle Identity Manager and Oracle Access Management Access Manager
- After installing Oracle Identity Manager and Oracle Access Management Access Manager
- After installing Oracle Access Management Mobile and Social
- When dumping the configuration of IdM components Oracle Internet Directory, Oracle Unified Directory, Oracle Virtual Directory, Oracle Identity Manager, and Oracle Access Manager
- When validating the configuration parameters for Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Manager, and Oracle Access Manager

[Section D.1.3](#) explains the tasks the tool performs in each situation.

D.1.3 Tasks performed by the Tool

The `idmConfigTool` helps you to perform the following tasks efficiently:

- To validate configuration properties representing the Identity Management components Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), Oracle Unified Directory (OUD), Oracle Access Management Access Manager (OAM) and Oracle Identity Manager (OIM).
- To pre-configure the Identity Store components (OID, OVD, and OUD) to install the other Identity Management components, including OAM, OIM, and Oracle Access Management Mobile and Social.
- To post-configure the OAM, OIM components and wiring of those components.
- To extract the configuration of the Identity Management components OID, OVD, OUD, OAM, and OIM.

See Also: [Section D.3.1](#).

D.1.4 Location of idmConfigTool

The `idmConfigTool` is located at:

```
IAM_ORACLE_HOME/idmtools/bin
```

where `IAM_ORACLE_HOME` is the directory in which OIM and OAM are installed.

To execute idmConfigTool on Linux

```
cd <IAM_ORACLE_HOME>/idmtools/bin
./idmConfigTool.sh
```

To execute idmConfigTool on Windows

```
cd <IAM_ORACLE_HOME>\idmtools\bin
idmConfigTool.cmd
```

D.1.5 Webgate Types Supported

The idmConfigTool supports OAM 11g Webgates by default. It also supports 10g Webgates.

D.1.6 Single- and Cross-Domain Scenarios

The tool supports two types of scenarios with regard to Weblogic domains:

- A single-domain configuration in which both Access Manager and Oracle Identity Manager servers are configured in the same Weblogic domain
- A dual or cross-domain configuration in which Access Manager and Oracle Identity Manager servers are configured on separate Weblogic domains

See Also: [Section 1.2](#) for architecture details.

D.2 Set Up Environment Variables

You must configure the environment before running the IdM configuration tool.

Set the following variables:

Table D-1 Environment Variables for IdM Configuration Tool (idmConfigTool)

Variable	Description
MW_HOME	This is the full path of the installation's Middleware home. Enter the path to the Oracle Middleware Home that was created when you installed Oracle WebLogic Server on your system. For example, if you install in /scratch/mytest, then: MW_HOME: /scratch/mytest/mw_idm WL_HOME: MW_HOME/wlserver_10.3
WL_HOME	Not mandatory. It is set to MW_HOME/wlserver_10.3 by default, and this setting is used. See MW_HOME for an example.
JAVA_HOME	This is the full path of the JDK directory. If running on IBM WebSphere, this variable must point to the IBM JDK. Set the value to the full path of the JDK. For example: /WASSH/WebSphere/AppServer/java <i>Important:</i> On IBM WebSphere, do not use a JDK other than the IBM JDK.
IDM_HOME	IDM_ORACLE_HOME, where Oracle Internet Directory is installed (optional)
ORACLE_HOME	Set to the full path of the Oracle home. For IdM integrations, set to IAM_ORACLE_HOME.
APPSERVER_TYPE	Required on IBM WebSphere. Set to was.

Table D-1 (Cont.) Environment Variables for IdM Configuration Tool (idmConfigTool)

Variable	Description
WAS_HOME	Required on IBM WebSphere. Set the value to the full path of the WebSphere application server home directory. For example: /WASSH/WebSphere/AppServer
WAS_DMGR_PROFILE_HOME	Required on IBM WebSphere. Specifies the deployment manager profile home directory. The deployment manager deploys applications to a cell of application servers which it manages. A profile defines the runtime environment and includes all the configurable files that the server processes in the run-time environment. Set to an absolute path, for example: /WASSH/WebSphere/AppServer/profiles/Dmgr01

D.3 Syntax and Usage

This section contains these topics:

- [Command Syntax](#)
- [Requirements](#)
- [Generated Files](#)
- [Using the Properties File](#)
- [Working with the idmConfigTool Log File](#)

D.3.1 Command Syntax

The tool has the following syntax on Linux:

```
idmConfigTool.sh -command
input_file=filename log_file=logfileName log_level=log_level
```

The tool has the following syntax on Windows:

```
idmConfigTool.bat -command
input_file=filename log_file=logfileName log_level=log_level
```

Values for *command* are as follows:

Command	Component name	Description
preConfigIDStore	Identity Store	Configures the identity store and policy store by creating the groups and setting ACIs to the various containers.
prepareIDStore mode= OAM OIM WLS WAS FUSION OAM APM all	Identity Store	Configures the identity store by adding necessary users and associating users with groups. Modes enable you to configure for a specific component. You can run this command on Oracle WebLogic Server (mode=WLS) or IBM WebSphere (mode=WAS).

Command	Component name	Description
configPolicyStore	Policy Store	Configures policy store by creating read-write user and associates them to the groups.
configOAM	Oracle Access Manager Oracle Identity Manager	Prepares Access Manager for integration with Oracle Identity Manager.
configOIM	Oracle Access Manager Oracle Identity Manager	Sets up wiring between Access Manager and Oracle Identity Manager.
configOMSS	Oracle Access Management Mobile and Social	Performs post-install configuration for Oracle Access Management Mobile and Social
configOVD	Oracle Virtual Directory	Creates OVD adapters.
disableOVDAccessConfig	Oracle Virtual Directory	Disables anonymous access to the OVD server. Post-upgrade command. <i>Note:</i> configOVD performs this task automatically when run.
postProvConfig	Identity Store	Performs post-provisioning configuration of the identity store.
validate IDSTORE POLICYSTORE OAM11g OAM10g OIM	Various	Validates the set of input properties for the named entity.
ovdConfigUpgrade	Oracle Virtual Directory	Updates the configuration for an upgraded OVD with split profile.
upgradeLDAPUsersForSSO	Oracle Identity Manager Access Manager	Updates existing users in OID by adding certain object classes which are needed for Oracle Identity Manager-Access Manager integration.
upgradeOIMTo11gWebgate	Oracle Identity Manager Access Manager	Upgrades an existing configuration consisting of integrated Oracle Identity Manager-Access Manager, using Webgate 10g, to use Webgate 11g

D.3.2 Requirements

You must run this tool as a user with administrative privileges when configuring the identity store or the policy store.

The `validate` command requires a component name.

Caution: The commands cannot be run in isolation. Run them in the context of explicit integration procedures; use this appendix only as a command reference.

D.3.3 Generated Files

idmConfigTool creates or updates certain files upon execution.

Parameter File

When you run the `idmConfigTool`, the tool creates or appends to the file `idmDomainConfig.param` in the directory from which you run the tool. To ensure that the same file is appended to each time the tool is run, always run `idmConfigTool` from the directory:

```
IAM_ORACLE_HOME/idmtools/bin
```

Log File

You can specify a log file using the `log_file` attribute of `idmConfigTool`.

If you do not explicitly specify a log file, a file named `automation.log` is created in the directory where you run the tool.

Check the log file for any errors or warnings and correct them.

D.3.4 Using the Properties File

This section describes the properties file that can be used with `idmConfigTool`.

D.3.4.1 About the properties File

A properties file provides a convenient way to specify command properties and enable you to save properties for reference and later use. You can specify a properties file, containing execution properties, as input command options. The properties file is a simple text file which must be available at the time the command is executed.

For security you are advised not to insert passwords into the properties file. The tool prompts you for the relevant passwords at execution.

D.3.4.2 List of Properties

[Table D-2](#) lists the properties used by integration command options in the `idmConfigTool` command. The properties are listed in alphabetical order.

WARNING: For security, do not put password values in your properties files. `idmConfigTool` prompts for passwords upon execution.

Table D-2 Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
ACCESS_GATE_ID	IdentityManagerAccessGate	The Access Manager access gate ID with which Oracle Identity Manager needs to communicate.
ACCESS_SERVER_HOST	mynode.us.example.com	Access Manager Access Server host name
ACCESS_SERVER_PORT	5575	Access Manager NAP port.
APNS_FILE	/scratch/silent_omsm/keystores/APNS.p12	Apple Push Notification Service (APNS) keystore file; used to establish secure connection to Apple server to send notifications.
APNS_KEYSTORE_PASSWD		APNS keystore password.

Table D–2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
APPLE_CACERT_FILE	/scratch/omss/keystores/app lerootca.crt	File location of Apple root CA. Required during iOS device enrollment in Oracle Mobile Security Suite (OMSS).
AUTOLOGINURI	/obrar.cgi	URI required by Oracle Platform Security Services (OPSS). Default value is /obrar.cgi
COOKIE_DOMAIN	.us.example.com	Web domain on which the Oracle Identity Manager application resides. Specify the domain in the format .cc.example.com.
COOKIE_EXPIRY_INTERVAL	-1	Cookie expiration period. Set to -1 to denote that the cookie expires when the session is closed.
DB_PASSWD		Database password, used in conjunction with JDCB_URL.
DOMAIN_LOCATION	ORACLE_BASE /admin/IDMDomain/aserver/ID MDomain	The location of the Oracle Identity Manager domain (and OMSM, if applicable).
DOMAIN_NAME	IDM_Domain	The Oracle Identity Manager domain name.
EMAIL_ADMIN_USER	admin@example.com	E-mail admin user; must be an e-mail address.
EMAIL_ADMIN_PASSWD		Email admin user's password
EXCHANGE_DOMAIN_NAME	example.com	Domain name of the exchange server.
EXCHANGE_SERVER_URL	http://testuri.com	URL of the exchange server.
EXCHANGE_LISTENER_URL	http://testuri.com	URL of the exchange listener.
EXCHANGE_SERVER_VERSION	2.0	The version of the exchange server.
EXCHANGE_ADMIN_USER	serviceuser	Admin user of the exchange server.
EXCHANGE_ADMIN_PASSWD		Password of the exchange server's admin user.
GCM_API_KEY	AIzaSyCh_JALj5Y	GCM notification API key.
GCM_SENDER_ID	6.10046E+11	GCM notification sender ID.
IDSTORE_ADMIN_PORT	4444	The admin port for an Oracle Unified Directory (OUD) identity store. idmConfigTool needs to connect on the OUD admin port for all operations changing OUD configuration structures: <ul style="list-style-type: none"> ■ creation of global ACIs ■ creation of indexes
IDSTORE_HOST	idstore.example.com	Host name of the LDAP identity store directory (corresponding to the IDSTORE_DIRECTORYTYPE). If your identity store is in Oracle Unified Directory or Oracle Unified Directory, then IDSTORE_HOST points directly to the Oracle Internet Directory or Oracle Unified Directory host. If the Identity Store is fronted by Oracle Virtual Directory, then IDSTORE_HOST points to the Oracle Virtual Directory host, which is IDSTORE.example.com.
IDSTORE_PORT	1389	Port number of the LDAP identity store (corresponding to the IDSTORE_DIRECTORYTYPE).

Table D-2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
IDSTORE_BINDDN	cn=orcladmin	Administrative user in the identity store directory.
IDSTORE_USERNAMEATTRIBUTE	cn	Username attribute used to set and search for users in the identity store. Set to part of the user DN. For example, if the user DN is cn=orcladmin, cn=Users, dc=us, dc=example, dc=com, this property is set to cn.
IDSTORE_LOGINATTRIBUTE	uid or email	Login attribute of the identity store which contains the user's login name. This is the attribute the user uses for login.
IDSTORE_USERSEARCHBASE	cn=Users,dc=us,dc=example,dc=com	Location in the directory where users are stored. This property tells the directory where to search for users.
IDSTORE_SEARCHBASE	dc=us,dc=example,dc=com	Search base for users and groups contained in the identity store. Parent location that contains the USERSEARCHBASE and the GROUPSEARCHBASE. For example: IDSTORE_SEARCHBASE: cn=oracleAccounts, dc=example, dc=com IDSTORE_USERSEARCHBASE: cn=Users, cn=oracleAccounts, dc=example, dc=com IDSTORE_GROUPSEARCHBASE: cn=Groups, cn=oracleAccounts, dc=example, dc=com
IDSTORE_GROUPSEARCHBASE	cn=Groups,dc=us,dc=example,dc=com	The location in the directory where groups (or <i>roles</i>) are stored. This property tells the directory where to search for groups or roles.
IDSTORE_OAMSOFTWAREUSER	oamLDAP	The username used to establish the Access Manager identity store connection. This user is created by the idmconfigtool.
IDSTORE_OAMADMINUSER	oamadmin	The identity store administrator you want to create for Access Manager. Required only if the identity store is set as the system identity store. The administrator is created by the idmconfigtool.
IDSTORE_OAAMADMINUSER	oaamadmin	The identity store administrator for Oracle Adaptive Access Manager.
IDSTORE_PROFILENAME	idsprofile	Name of the identity store profile.
IDSTORE_SYSTEMIDBASE	cn=system, dc=test	Location of a container in the directory where system operations users are stored so that they are kept separate from enterprise users stored in the main user container. There are only a few system operations users. One example is the Oracle Identity Manager reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.
IDSTORE_READONLYUSER		User with read-only permissions to the identity store.

Table D–2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
IDSTORE_READWRITEUSER		User with read-write permissions to the identity store.
IDSTORE_SUPERUSER		The Oracle Fusion Applications superuser in the identity store.
IDSTORE_XELSYSADMINUSER		The administrator of the xelsysadm system account.
IDSTORE_OIMADMINUSER		The identity store administrator for Oracle Identity Manager. User that Oracle Identity Manager uses to connect to the identity store
IDSTORE_OIMADMINGROUP		The Oracle Identity Manager administrator group you want to create to hold your Oracle Identity Manager administrative users.
IDSTORE_SSL_ENABLED		Whether SSL to the identity store is enabled. Valid values: true false
IDSTORE_KEYSTORE_FILE	<pre> OUD_ORACLE_INSTANCE /OUD/config/admin-keystore </pre>	<p>Location of the keystore file containing identity store credentials.</p> <p>Applies to and required for Oracle Unified Directory identity stores.</p>
IDSTORE_KEYSTORE_PASSWORD	<pre> 4VYGtJLG61V5OjDWKe94e601 x7tgLFs </pre>	<p>Password of the identity store directory administrator. Not plain-text.</p> <p>Applies to and required for Oracle Unified Directory identity stores.</p> <p>This value can be found in the file <code>OID_ORACLE_INSTANCE/OUD/config/admin-keystore.pin</code>.</p>
IDSTORE_NEW_SETUP		Used for identity store validation.
IDSTORE_DIRECTORYTYPE	OVD	<p>Used in Oracle Fusion Applications environment.</p> <p>Directory type of the identity store for which the authenticator must be created.</p> <p>Set to <code>OVD</code> if you are using Oracle Virtual Directory server to connect to either a non-OID directory, Oracle Internet Directory or Oracle Unified Directory.</p> <p>Set it to <code>OID</code> if your identity store is in Oracle Internet Directory and you are accessing it directly rather than through Oracle Virtual Directory.</p> <p>Set to <code>OID</code> if your identity store is Oracle Unified Directory and you are accessing it directly rather than through Oracle Virtual Directory.</p> <p>Valid values: <code>OID</code>, <code>OVD</code>, <code>OID</code>, <code>AD</code></p>
IDSTORE_ADMIN_USER	<pre> cn=systemids,dc=example,dc= com </pre>	The administrator of the identity store directory. Provide the complete LDAP DN of the same user specified for <code>IDSTORE_OAMSOFTWAREUSER</code> . The username alone is not sufficient.
IDSTORE_WLSADMINUSER	weblogic_idm	The identity store administrator for Oracle WebLogic Server; usually <code>weblogic_idm</code> .
IDSTORE_WLSADMINUSER_PWD		The password of the identity store administrator for Oracle WebLogic Server.

Table D–2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
IDSTORE_WLSADMININGROUP	WLS Administrators	The identity store administrator group for Oracle WebLogic Server.
IDSTORE_WASADMINUSER		The "wasadmin" user (IBM WebSphere).
JDBC_URL	jdbc:oracle:thin:@example.com:5521:msmdb	JDBC URL used to seed APNS/GCM data.
LDAPn_HOST	.	The host name of the LDAP server
LDAPn_PORT		The LDAP server port number.
LDAPn_BINDDN	.	The bind DN for the LDAP server
LDAPn_SSL		Indicates whether the connection to the LDAP server is over SSL. Valid values are True or False
LDAPn_BASE		The base DN of the LDAP server.
LDAPn_OVD_BASE		The OVD base DN of the LDAP server.
LDAPn_TYPE		The directory type for the LDAP server. n is 1, 2, and so on. For a single-node configuration specify LDAP1.
LOGINURI	/\${app.context}/adfAuthentication	URI required by OPSS. Default value is /\${app.context}/adfAuthentication
LOGOUTURI	/oamssso/logout.html	URI required by OPSS. Default value is /oamssso/logout.html
MDS_DB_URL	jdbc:oracle:thin:@DBHOST:1521:SID	URL of the MDS database. It represents a single instance database. The string following the '@' symbol must have the correct values for your environment. SID must be the actual SID, <i>not</i> a service name. If you are using a single instance database, then set MDS_URL to: jdbc:oracle:thin:@DBHOST:1521:SID.
MDS_DB_SCHEMA_USERNAME	edg_mds	Username of the MDS schema user. MDS schema which Oracle Identity Manager is using.
MSM_SCHEMA_USER	DEV87_OMSM	Mobile Security Manager (MSM) database schema username.
MSM_SERVER_KEY_LENGTH	2048	Key length for the self-signed CA and generated keys for the MSM server. Defaults to 2048.
MSM_SERVER_NAME	omsm_server1	Name of the MSM server. Provide this only if the MSM server is renamed to a different value during domain configuration.
MSAS_SERVER_HOST	server1.example.com	MSAS server host name.
MSAS_SERVER_PORT	11001	MSAS server's SSL port.
OAM_SERVER_VERSION	10g	Set to 10g if using Oracle Access Manager 10g, or 11g if using Access Manager 11g. Required when Access Manager server does not support 11g webgate in Oracle Identity Manager-Access Manager integration. In that case, provide the value as '10g'. Valid values are 10g, 11g.

Table D–2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
OAM_TRANSFER_MODE	SIMPLE	The transfer mode for the Access Manager agent being configured. If your access manager servers are configured to accept requests using the simple mode, set OAM_TRANSFER_MODE to SIMPLE. Valid values are OPEN, SIMPLE or CERT.
OAM11G_OAM_SERVER_TRANSFER_MODE	OPEN	The security model in which the Access Manager 11g server functions. Valid values: OPEN or SIMPLE.
OAM11G_SSO_ONLY_FLAG	false	Configures Access Manager 11g as authentication only mode or normal mode, which supports authentication and authorization. Default value is true (OAM performs no authorization). If set to true, the Access Manager 11g server operates in authentication only mode, where all authorizations return true by default without any policy validations. In this mode, the server does not have the overhead of authorization handling. This is recommended for applications which do not depend on authorization policies and need only the authentication feature of the Access Manager server. If the value is false, the server runs in default mode, where each authentication is followed by one or more authorization requests to the OAM Server. WebGate allows the access to the requested resources or not, based on the responses from the OAM server.
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	OAMAdministrators	Name of the group that is used to allow access to the Oracle Access Management Administration Console to administer role security in identity store.
OAM11G_OIM_INTEGRATION_REQ	false	Specifies whether to integrate with Oracle Identity Manager or configure Access Manager in stand-alone mode. Set to true for integration. Valid values: true (integration) false
OAM11G_SERVER_LBR_HOST	sso.example.com	Host name of the load balancer to the Oracle HTTP (OHS) server front-ending the Access Manager server. This and the following two parameters are used to construct your login URL.
OAM11G_SERVER_LBR_PORT	443	Port number of the load balancer to the OHS server front-ending the Access Manager server.
OAM11G_SERVER_LBR_PROTOCOL	https	Protocol of the load balancer to the OHS server front-ending the Access Manager server. Valid values: HTTP, HTTPS
OAM11G_SERVER_LOGIN_ATTRIBUTE	uid	At a login attempt, the username is validated against this attribute in the identity store. Setting to uid ensures that when users log in their username is validated against the uid attribute in LDAP.
OAM11G_SERVER_GLOBAL_SESSION_TIMEOUT		The global session timeout for sessions in the Access Manager server.

Table D–2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
OAM11G_SERVER_GLOBAL_SESSION_EXPIRY_TIME		Global session expiry time for a session in the Access Manager server.
OAM11G_SERVER_GLOBAL_MAX_SESSION_PER_USER		Global maximum sessions per user in the Access Manager server.
OAM11G_IDSTORE_NAME		The identity store name. If you already have an identity Store in place which you wish to reuse (rather than allowing the tool to create a new one for you), set this parameter to the name of the Identity Store. The default value is "OAMIDStore".
OAM11G_IMPERSONATION_FLAG		Enable or disable impersonation in Access Manager server. Applicable to Oracle Fusion Applications environment. Valid values: true (enable) false The default is false. If you are using impersonalization, you must manually set this value to true.
OAM11G_IDM_DOMAIN_OHS_HOST	sso.example.com	Host name of the load balancer which is in front of OHS in a high-availability configuration.
OAM11G_IDM_DOMAIN_OHS_PORT	443	Port number on which the load balancer specified as OAM11G_IDM_DOMAIN_OHS_HOST listens.
OAM11G_IDM_DOMAIN_OHS_PROTOCOL	https	Protocol for IDM OHS. Protocol to use when directing requests to the load balancer. Valid values: HTTP HTTPS
OAM11G_OIM_OHS_URL	https://sso.example.com:443/test	URL of the load balancer or OHS fronting the OIM server.
OAM11G_WG_DENY_ON_NOT_PROTECTED	true	Deny on protected flag for 10g webgate Valid values: true false
OAM11G_OAM_SERVER_TRANSFER_MODE	simple	Transfer mode for the IDM domain agent. Valid values: OPEN SIMPLE CERT
OAM11G_IDM_DOMAIN_LOGOUT_URLS	/console/jsp/common/logout.jsp,/em/targetauth/emaslogout.jsp	Comma-separated list of Access Manager logout URLs.
OAM11G_WLS_ADMIN_HOST	myhost.example.com	On WebLogic Server: Host name of the Access Manager domain admin server. On IBM WebSphere: The Access Manager application server host.
OAM11G_WLS_ADMIN_PORT	7001	On WebLogic Server: Port on which the Access Manager domain admin server is running. On IBM WebSphere: Deployment Manager bootstrap port for Access Manager cell.
OAM11G_WLS_ADMIN_USER	wlsadmin, wasadmin	On WebLogic Server: The username of the Access Manager domain administrator. On IBM WebSphere: Primary administrative user name for Access Manager cell.

Table D-2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
OAM_ADMIN_WAS_DEFAULT_PORT	1443	On IBM WebSphere, OAM node's OracleAdminServer default port number
OAM_POLICY_MGR_SERVER_NAME	oam_policy_mgr1	Name of the Access Manager policy manager server. Provide this only if the policy manager server is renamed to a different value during domain configuration.
OIM_DB_URL		The URL needed to connect to the Oracle Identity Manager database.
OIM_DB_SCHEMA_USERNAME		The schema user for the Oracle Identity Manager database.
OIM_FRONT_END_HOST	host123.example.com	The host name of the LBR server front-ending Oracle Identity Manager.
OIM_FRONT_END_PORT	7011	The port number of the LBR server front-ending Oracle Identity Manager.
OIM_MANAGED_SERVER_NAME	WLS_OIM1	The name of the Oracle Identity Manager managed server. If clustered, any of the managed servers can be specified.
OIM_MANAGED_SERVER_HOST		The host name of the Oracle Identity Manager managed server.
OIM_MANAGED_SERVER_PORT		The port number of the Oracle Identity Manager managed server.
OIM_MSM_REST_SERVER_URL	https://msm.example.com:1234/	The URL of the Oracle Mobile Security Manager server. Required only if MSM URL needs to be seeded in Oracle Identity Manager and the system property OMSS Enabled set. OIM_MSM_REST_SERVER_URL enables the Mobile Security Manager task flows in the Oracle Identity Manager console. If not set, configOIM will continue the configuration without configuring the Mobile Security Manager. The prerequisite for OMSS Enabled is that the Oracle Identity Manager server should be up.
OIM_T3_HOST		The host name for the Oracle Identity Manager T3 server.
OIM_T3_PORT		The port number of the Oracle Identity Manager T3 server.
OIM_WAS_CELL_CONFIG_DIR		The location of the <code>fmwconfig</code> directory within the Oracle Identity Manager cell on IBM WebSphere.
OMSS_KEYSTORE_PASSWORD		Password used to generate OMSM keystores and keys
OMSM_IDSTORE_ROLE_SECURITY_ADMIN	MSMAdmin	Name of the admin group whose members have admin privileges for OMSM operations. Default is "IDM Administrators".
OMSM_IDSTORE_ROLE_SECURITY_HELPDESK	MSMHelpDeskUsers	Name of the msm helpdesk group, whose members get helpdesk privileges for OMSM operations. Default is "MSMHelpdeskUsers".
ovd.host		OVD Server host name
ovd.port		OVD Server port number

Table D-2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
ovd.binddn		OVD Server bind DN
ovd.ssl		Indicates whether the connection is over SSL. Valid values are True or False
ovd.oamenabled		Indicates whether Oracle Access Manager is enabled. Valid values are True or False
POLICYSTORE_SHARES_IDSTORE	true	Denotes whether the policy store and identity store share the directory. Always true in Release 11g. Valid values: true, false
POLICYSTORE_HOST	mynode.us.example.com	The host name of your policy store directory.
POLICYSTORE_PORT	1234	The port number of your policy store directory.
POLICYSTORE_BINDDN	cn=orcladmin	Administrative user in the policy store directory.
POLICYSTORE_SEARCHBASE	dc=example,dc=com	The location in the directory where users and groups are stored.
POLICYSTORE_SYSTEMIDBASE	cn=systemids, dc=example,dc=com	The read-only and read-write users for policy store are created in this location. Default value is cn=systemids, policy_store_search_base
POLICYSTORE_READONLYUSER	PolStoreROUser	A user with read privileges in the policy store.
POLICYSTORE_READWRITEUSER	PolStoreRWUser	A user with read and write privileges in the policy store.
POLICYSTORE_CONTAINER	cn=jpsroot	The name of the container used for OPSS policy information
POLICYSTORE_SSL_ENABLED		Whether the policy store is SSL-enabled.
POLICYSTORE_KEYSTORE_FILE		The location of the keystore file for an SSL-enabled policy store.
PROXY_SERVER_HOST	www-proxy.example.com	Proxy server's host name.
PROXY_SERVER_PORT	80	Proxy server's port.
PROXY_USER	proxyuserA	User for proxy.
PROXY_PASSWD		Password for proxy user.
SCEP_DYNAMIC_CHALLENGE_USER		OMSM uses a Simple Certificate Enrollment Protocol (SCEP) dynamic challenge for external SCEP authentication during the enrollment phase. This user account is used for authentication.
SCEP_DYNAMIC_CHALLENGE_PASSWD		SCEP dynamic challenge user's password

Table D–2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
SPLIT_DOMAIN	true	Flag to force configOAM to create security providers in the domain against which it is run. Valid values are true, false. Setting to true is required to suppress the double authentication of Oracle Access Management administration console in a split domain scenario.
SSO_ENABLED_FLAG	false	Flag to determine if SSO should be enabled. Valid values are true, false.
WEBGATE_TYPE	javaWebgate	The type of WebGate agent you want to create. Set to: <ul style="list-style-type: none"> ■ ohsWebgate10g if using Webgate version 10 ■ ohsWebgate11g if using Webgate version 11
PRIMARY_OAM_SERVERS	idmhost1.example.com:5575,idmhost2.example.com:5575	A comma-separated list of your Access Manager servers and their proxy ports. To determine the proxy ports your Access Manager servers: <ol style="list-style-type: none"> 1. Log in to the Oracle Access Management administration console at <code>http://admin.example.com:7001/oamconsole</code> 2. At the top of the Oracle Access Management Console, click Configuration. 3. In the Configuration console, click Server Instances. 4. In the page that appears, click Search, then double-click the target instance to display its configuration. For example, WLS_OAM1. The proxy port is shown as Port.
SMTP_HOST	exchangeurl.us.example.com	E-mail host.
SMTP_PORT	80	E-mail port.
TOPIC	com.apple.mgmt.External.2544264e-aa8a-4654-bfff-9d897ed39a87	Topic used in Apple's APNS certificate; used to send APNS notification. The value should match the UID of the APNS key.
USE_PROXY	true	Indicates whether to use a proxy. Valid values are true, false.
WLSHOST	node01.example.com	WebLogic Server host name (host name of your administration server).
WLSPORT	7001	The WebLogic Server port number
WLSADMIN	wlsadmin	The administrator login, depending on the application server context.
WLSPASSWD		The WebLogic Server administrator password.

D.3.5 Working with the idmConfigTool Log File

idmConfigTool logs execution details to a file called `automation.log`, which is helpful in verifying the results of a run.

- [Searching the idmConfigTool Log File](#)
- [Maintaining the idmConfigTool Log File](#)

D.3.5.1 Searching the idmConfigTool Log File

The log file contains initialization and informational messages:

```
Feb 18, 2015 8:38:14 PM oracle.idm.automation.util.Util setLogger
WARNING: Logger initialized in warning mode
Feb 18, 2015 8:38:19 PM
oracle.idm.automation.impl.oim.handlers.OIMPreIntegrationHandler <init>
INFO: Appserver type: null
Feb 18, 2015 8:38:20 PM
oracle.idm.automation.impl.oim.handlers.OIMPreIntegrationHandler <init>
WARNING: Cannot connect to the OUD Admin connector
Feb 18, 2015 8:38:29 PM
oracle.idm.automation.impl.oim.handlers.OIMPreIntegrationHandler
createOIMAdminUser
INFO: OIM Admin User has been created
Feb 18, 2015 8:38:29 PM
oracle.idm.automation.impl.oim.handlers.OIMPreIntegrationHandler
addPwdResetPrivilegeToOIMAdminUser
INFO: Password reset privilege added
```

Checking for WARNING messages after a run can help you identify potential problems with the run.

D.3.5.2 Maintaining the idmConfigTool Log File

idmConfigTool appends to the log file upon each run. The presence of older entries can lead to a misunderstanding if you see an error in the log and correct it, since the original error detail is present in the log even after you rectify the error.

WARNING: Back up existing log files frequently to avoid confusion caused by old log entries.

D.4 Command Options and Properties

This section lists the properties for each command option. Topics include:

- [preConfigIDStore Command](#)
- [prepareIDStore Command](#)
- [configPolicyStore Command](#)
- [configOAM Command](#)
- [configOIM Command](#)
- [configOMSS Command](#)
- [postProvConfig Command](#)
- [upgradeLDAPUsersForSSO Command](#)
- [validate IDStore Command](#)
- [validate PolicyStore Command](#)
- [validate OAM Command \(11g\)](#)

- [validate OAM Command \(10g\)](#)
- [validate OIM command](#)
- [configOVD Command](#)
- [ovdConfigUpgrade Command](#)
- [disableOVDAccessConfig Command](#)
- [upgradeOIMTo11gWebgate](#)

Notes:

- The command options show the command syntax on Linux only. See [Section D.3.1](#) for Windows syntax guidelines.
 - The tool prompts for passwords.
-
-

D.4.1 preConfigIDStore Command

Syntax

On Linux, the command syntax is:

```
idmConfigTool.sh -preConfigIDStore input_file=input_properties
```

On Windows, the command syntax is:

```
idmConfigTool.bat -preConfigIDStore input_file=input_properties
```

For example:

```
idmConfigTool.sh -preConfigIDStore input_file=extendOAMPropertyFile
```

Note: The `-preConfigIDStore` command option supports Oracle Internet Directory, Oracle Unified Directory, and Oracle Virtual Directory.

Properties

[Table D-3](#) lists the properties for this mode:

Table D-3 *Properties of preConfigIDStore*

Property	Required?
IDSTORE_HOST	YES
	IDSTORE_HOST and IDSTORE_PORT are the host and port, respectively, of your identity store directory. If your identity store is in Oracle Unified Directory or Oracle Internet Directory, then IDSTORE_HOST should point directly to the Oracle Unified Directory or Oracle Internet Directory host. If your Identity Store is fronted by Oracle Virtual Directory, then IDSTORE_HOST should point to the Oracle Virtual Directory host, which should be IDSTORE.example.com.
IDSTORE_PORT	YES

Table D-3 (Cont.) Properties of preConfigIDStore

Property	Required?
IDSTORE_BINDDN	YES
IDSTORE_DIRECTORYTYPE	YES (if target identity store is an instance of Oracle Unified Directory (OUD).)
IDSTORE_LOGINATTRIBUTE	
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_SYSTEMIDBASE	
POLICYSTORE_SHARES_IDSTORE	
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).) This property is required to connect to and configure OUD configuration structures: <ul style="list-style-type: none"> ■ creation of global ACIs ■ creation of indexes
IDSTORE_KEYSTORE_FILE	YES, if target identity store is OUD. Use the format: <i>OID-instance-path</i> <i>/OUD/config/admin-keystore</i> where <i>OID-instance-path</i> is the path to the directory instance. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is OUD. Not plain-text. Resides in the file <i>OID_ORACLE_INSTANCE/OUD/config/admin-keystore.pin</i> . IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.

Example properties File

Here is a sample properties file for this option:

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
```

If you are using Oracle Unified Directory as the identity store, include the additional properties indicated in the properties table. The sample properties file then contains the additional properties:

```
IDSTORE_DIRECTORYTYPE: OUD
IDSTORE_ADMIN_PORT : 4444
IDSTORE_KEYSTORE_FILE : /u01/config/instances/oud1/OUJ/config/admin-keystore
IDSTORE_KEYSTORE_PASSWORD : K8BYCo0FHBwDYa1F6vUBgcGr1TK1Rz26W9Bz70F0UwsZ5XLGOB
```

Using prepareIDStore for Oracle Unified Directory

When using `prepareIDStore` for Oracle Unified Directory, global ACI and indexes are re-created only in the instance(s) specified in the property file; they are not replicated by Oracle Unified Directory. You must manually re-create (remove, then create) the global ACI and indexes on all other Oracle Unified Directory instances of the replication domain.

For details, see [Section D.5](#).

See Also: [Table D-2](#) for details of the properties.

D.4.2 prepareIDStore Command

Syntax

The `prepareIDStore` command takes `mode` as an argument to perform tasks for the specified component.

```
idmConfigTool.sh -prepareIDStore mode=mode
input_file=filename_with_Configproperties
```

where `mode` must be one of the following:

- OAM
- OIM
- OAAM
- WLS
- FUSION
- WAS
- APM
- all (performs all the tasks of the above modes combined)

Note: WLS mode must be run before OAM.

See Also: [Table D-2](#) for details of the properties.

D.4.2.1 prepareIDStore mode=OAM

The following are created in this mode:

- Perform schema extensions as required by the Access Manager component
- Add the oblix schema
- Create the OAMSoftware User
- Create OblixAnonymous User
- Optionally create the Access Manager Administration User
- Associate these users to their respective groups

- Create the group "orclFAOAMUserWritePrivilegeGroup"

Syntax

On Linux, the command syntax is:

```
idmConfigTool.sh -prepareIDStore mode=OAM input_file=filename_with_
Configproperties
```

On Windows, the command syntax is:

```
idmConfigTool.bat -prepareIDStore mode=OAM input_file=filename_with_
Configproperties
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=OAM input_file=preconfigOAMPropertyFile
```

Properties

Table D-4 lists the properties for this mode:

Table D-4 prepareIDStore mode=OAM Properties

Parameter	Required?
IDSTORE_HOST	YES IDSTORE_HOST and IDSTORE_PORT are the host and port, respectively, of your Identity Store directory. If your Identity Store is in Oracle Internet Directory or Oracle Unified Directory, then IDSTORE_HOST should point to Oracle Internet Directory or Oracle Unified Directory, even if you are fronting Oracle Internet Directory with Oracle Virtual Directory. If you are using a directory other than Oracle Internet Directory or Oracle Unified Directory, specify the Oracle Virtual Directory host.
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_OAMSOFTWAREUSER	
IDSTORE_OAMADMINUSER	
IDSTORE_SYSTEMIDBASE	

Table D–4 (Cont.) prepareIDStore mode=OAM Properties

Parameter	Required?
IDSTORE_ADMIN_PORT	<p>YES (if target identity store is an instance of Oracle Unified Directory (OUD).)</p> <p>This property is required to connect to and configure OUD configuration structures:</p> <ul style="list-style-type: none"> ■ creation of global ACIs ■ creation of indexes
IDSTORE_KEYSTORE_FILE	<p>YES, if target identity store is OUD.</p> <p>Use the format: <i>OUD-instance-path</i> / OUD / config / admin-keystore</p> <p>where <i>OUD-instance-path</i> is the path to the directory instance.</p> <p>IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.</p>
IDSTORE_KEYSTORE_PASSWORD	<p>YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.</p>

Example properties File

Here is a sample properties file for this option. This parameter set would result in OAMADMINUSER and OAMSOFTWARE user being created in the identity store:

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
IDSTORE_OAMSOFTWAREUSER: oamLDAP
IDSTORE_OAMADMINUSER: oamadmin
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
```

See Also: [Table D–2](#) for details of the properties.

D.4.2.2 prepareIDStore mode=OIM

The following are created in this mode:

- Create Oracle Identity Manager Administration User under SystemID container
- Create Oracle Identity Manager Administration Group
- Add Oracle Identity Manager Administration User to Oracle Identity Manager Administration Group
- Add ACIs to Oracle Identity Manager Administration Group
- Create reserve container
- Create xelsysadmin user

Syntax

On Linux, the command syntax is:

```
idmConfigTool.sh -prepareIDStore mode=OIM input_file=filename_with_
Configproperties
```

On Windows, the command syntax is:

```
idmConfigTool.bat -prepareIDStore mode=OIM input_file=filename_with_
Configproperties
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=OIM input_file=preconfigOIMPropertyFile
```

Properties

Table D-5 lists the properties in this mode:

Table D-5 *prepareIDStore mode=OIM Properties*

Parameter	Required?
IDSTORE_HOST	YES IDSTORE_HOST and IDSTORE_PORT are the host and port, respectively, of your Identity Store directory. If your Identity Store is in Oracle Internet Directory or Oracle Unified Directory, then IDSTORE_HOST should point directly to the Oracle Internet Directory or Oracle Unified Directory host. If your Identity Store is fronted by Oracle Virtual Directory, then IDSTORE_HOST should point to the Oracle Virtual Directory host, which should be IDSTORE.example.com.
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_OIMADMINUSER	
IDSTORE_OIMADMINGROUP	
IDSTORE_SYSTEMIDBASE	
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).) This property is required to connect to and configure OUD configuration structures: <ul style="list-style-type: none"> ■ creation of global ACIs ■ creation of indexes
IDSTORE_KEYSTORE_FILE	YES (if target identity store is an instance of OUD) IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.

Table D–5 (Cont.) prepareIDStore mode=OIM Properties

Parameter	Required?
IDSTORE_KEYSTORE_PASSWORD	YES (if target identity store is an instance of OUD.) Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/ODD/config/admin-keystore.pin..
OIM_DB_URL	Required on IBM WebSphere.
OIM_DB_SCHEMA_USERNAME	Required on IBM WebSphere.
OIM_WAS_CELL_CONFIG_DIR	Required on IBM WebSphere.

Example properties File

Here is a sample properties file for this option:

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_OIMADMINUSER: oimadmin
IDSTORE_OIMADMINGROUP: OIMAdministrators
OIM_DB_URL: jdbc:oracle:thin:@xyz5678.us.example.com:5522:wasdb1
OIM_DB_SCHEMA_USERNAME: dev_oim
OIM_WAS_CELL_CONFIG_DIR:
/wassh/WebSphere/AppServer/profiles/Dmgr04/config/cells/xyz5678Cell104/fmwconfig
```

See Also: [Table D–2](#) for details of the properties.

D.4.2.3 prepareIDStore mode=OAAM

This mode:

- Creates Oracle Adaptive Access Manager Administration User
- Creates Oracle Adaptive Access Manager Groups
- Adds the Oracle Adaptive Access Manager Administration User as a member of Oracle Adaptive Access Manager Groups

Syntax

```
idmConfigTool.sh -prepareIDStore mode=OAAM
input_file=filename_with_Configproperties
```

Properties

[Table D–6](#) shows the properties in this mode:

Table D–6 prepareIDStore mode=OAAM Properties

Parameter	Required?
IDSTORE_HOST	YES

Table D-6 (Cont.) prepareIDStore mode=OAAM Properties

Parameter	Required?
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	YES
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_OAAMADMINUSER	YES
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).) This property is required to connect to and configure OUD configuration structures: <ul style="list-style-type: none"> ■ creation of global ACIs ■ creation of indexes
IDSTORE_KEYSTORE_FILE	YES, if target identity store is OUD. Use the format: <i>OID-instance-path</i> /OUD/config/admin-keystore where <i>OID-instance-path</i> is the path to the directory instance. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.

Example properties File

Here is a sample properties file for this option:

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_OAAMADMINUSER: oaadmin
POLICYSTORE_SHARES_IDSTORE: true
```

See Also: [Table D-2](#) for details of the properties.

D.4.2.4 prepareIDStore mode=WLS

This mode:

- Creates Weblogic Administration User

- Creates Weblogic Administration Group
- Adds the Weblogic Administration User as a member of Weblogic Administration Group

Syntax

On Linux, the command syntax is:

```
idmConfigTool.sh -prepareIDStore mode=WLS input_file=filename_with_
Configproperties
```

On Windows, the command syntax is:

```
idmConfigTool.bat -prepareIDStore mode=WLS input_file=filename_with_
Configproperties
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=WLS input_file=preconfigWLSPropertyFile
```

Properties

[Table D-7](#) lists the properties in this mode:

Table D-7 *prepareIDStore mode=WLS Properties*

Parameter	Required?
IDSTORE_HOST	YES IDSTORE_HOST and IDSTORE_PORT are the host and port, respectively, of your Identity Store directory. If your Identity Store is in Oracle Internet Directory or Oracle Unified Directory, then IDSTORE_HOST should point to the Oracle Internet Directory or Oracle Unified Directory host, even if you are fronting Oracle Internet Directory with Oracle Virtual Directory. If you are using a directory other than Oracle Internet Directory or Oracle Unified Directory, specify the Oracle Virtual Directory host (which should be <i>IDSTORE.example.com</i> .)
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	YES
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_WLSADMINUSER	YES. Do not set any default, out-of-the-box users such as weblogic/xelsysadm for this property.
IDSTORE_WLSADMINGROUP	YES

Table D-7 (Cont.) prepareIDStore mode=WLS Properties

Parameter	Required?
IDSTORE_ADMIN_PORT	<p>YES (if target identity store is an instance of Oracle Unified Directory (OUD).)</p> <p>This property is required to connect to and configure OUD configuration structures:</p> <ul style="list-style-type: none"> ■ creation of global ACIs ■ creation of indexes
IDSTORE_KEYSTORE_FILE	<p>YES, if target identity store is OUD.</p> <p>Use the format: <i>OUD-instance-path</i> /OUD/config/admin-keystore</p> <p>where <i>OUD-instance-path</i> is the path to the OUD instance.</p> <p>IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.</p>
IDSTORE_KEYSTORE_PASSWORD	<p>YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.</p>

Example properties File

Here is a sample properties file for this option. With this set of properties, the IDM Administrators group is created.

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users, dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_WLSADMINUSER: weblogic_idm
IDSTORE_WLSADMINGROUP: wlsadmingroup
```

See Also: [Table D-2](#) for details of the properties.

D.4.2.5 prepareIDStore mode=WAS

This mode:

- Creates WebSphere Administration User
- Creates WebSphere Administration Group
- Adds the WebSphere Administration User as a member of WebSphere Administration Group

Syntax

```
idmConfigTool.sh -prepareIDStore mode=WAS
input_file=filename_with_Configproperties
```

Properties

Table D-8 lists the properties in this mode:

Table D-8 *prepareIDStore mode=WAS Properties*

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_WASADMINUSER	YES (wsadmin user)
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD). This property is required to connect to and configure OUD configuration structures: <ul style="list-style-type: none"> ■ creation of global ACIs ■ creation of indexes
IDSTORE_KEYSTORE_FILE	YES, if target identity store is OUD. Use the format: <i>OID-instance-path</i> /OUD/config/admin-keystore where <i>OID-instance-path</i> is the path to the OUD instance. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.

Example properties File

Here is a sample properties file for this option, which creates the IDM Administrators group.

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users, dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_WASADMINUSER: webspHERE_idm
```

See Also: [Table D-2](#) for details of the properties.

D.4.2.6 prepareIDStore mode=APM

This mode:

- Creates Oracle Privileged Account Manager Administration User
- Adds the Oracle Privileged Account Manager Administration User as a member of Oracle Privileged Account Manager Groups

You are prompted to enter the password of the account that you are using to connect to the identity store.

Syntax

```
idmConfigTool.sh -prepareIDStore mode=APM
input_file=filename_with_Configproperties
```

Properties

[Table D-9](#) shows the properties in this mode:

Table D-9 *prepareIDStore mode=APM Properties*

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERNAMEATTRIBUTE	
IDSTORE_LOGINATTRIBUTE	
IDSTORE_USERSEARCHBASE	
IDSTORE_GROUPSEARCHBASE	
IDSTORE_SEARCHBASE	
POLICYSTORE_SHARES_IDSTORE	YES
IDSTORE_APMUSER	YES

Example properties File

Here is a sample properties file for this option:

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_APMUSER: opamadmin
```

See Also: [Table D-2](#) for details of the properties.

D.4.2.7 prepareIDStore mode=fusion

This mode:

- Creates a ReadOnly User
- Creates a ReadWrite User
- Creates a Super User
- Adds the readOnly user to the groups orclFAGroupReadPrivilegeGroup and orclFAUserWritePrefsPrivilegeGroup
- Adds the readWrite user to the groups orclFAUserWritePrivilegeGroup and orclFAGroupWritePrivilegeGroup

Syntax

```
idmConfigTool.sh -prepareIDStore mode=fusion
input_file=filename_with_Configproperties
```

Properties

Table D-10 lists the properties in this mode:

Table D-10 *prepareIDStore mode=fusion Properties*

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_READONLYUSER	
IDSTORE_READWRITEUSER	
IDSTORE_SUPERUSER	
IDSTORE_SYSTEMIDBASE	
POLICYSTORE_SHARES_IDSTORE	
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).) This property is required to connect to and configure OUD configuration structures: <ul style="list-style-type: none"> ■ creation of global ACIs ■ creation of indexes

Table D–10 (Cont.) prepareIDStore mode=fusion Properties

Parameter	Required?
IDSTORE_KEYSTORE_FILE	YES, if target identity store is OUD. Use the format: <i>OID-instance-path</i> /OUD/config/admin-keystore where <i>OID-instance-path</i> is the path to the OUD instance. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.

Example properties File

Here is a sample properties file for this option, which creates IDSTORE_SUPERUSER:

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 4389
IDSTORE_ADMIN_PORT: 1111
IDSTORE_BINDDN: cn=directory manager
IDSTORE_READONLYUSER: IDROUser
IDSTORE_READWRITEUSER: IDRWUser
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycomapny,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=us,dc=example,dc=com
IDSTORE_SUPERUSER: weblogic_fa
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_SSL_ENABLED: false
```

See Also: [Table D–2](#) for details of the properties.

D.4.2.8 prepareIDStore mode=all

The mode performs all the tasks that are performed in the modes OAM, OIM, WLS, WAS, OAAM, and FUSION.

Syntax

```
idmConfigTool.sh -prepareIDStore mode=all
input_file=filename_with_Configproperties
```

Properties

[Table D–11](#) lists the properties in this mode:

Table D–11 prepareIDStore mode=all Properties

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERSEARCHBASE	YES

Table D–11 (Cont.) prepareIDStore mode=all Properties

Parameter	Required?
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_LOGINATTRIBUTE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_SYSTEMIDBASE	
IDSTORE_READONLYUSER	YES
IDSTORE_READWRITEUSER	YES
IDSTORE_SUPERUSER	YES
IDSTORE_OAMSOFTWAREUSER	YES
IDSTORE_OAMADMINUSER	YES
IDSTORE_OIMADMINUSER	YES
IDSTORE_OIMADMINGROUP	YES
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_OAADMINUSER	YES
IDSTORE_WLSADMINUSER	YES
IDSTORE_WLSADMINGROUP	YES
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).) This property is required to connect to and configure OUD configuration structures: <ul style="list-style-type: none"> ■ creation of global ACIs ■ creation of indexes
IDSTORE_KEYSTORE_FILE	YES, if target identity store is OUD. Use the format: <i>OUD-instance-path</i> /OUD/config/admin-keystore where <i>OUD-instance-path</i> is the path to the OUD instance. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	
POLICYSTORE_SHARES_IDSTORE	
OIM_DB_URL	Required on IBM WebSphere
OIM_DB_SCHEMA_USERNAME	Required on IBM WebSphere
OIM_WAS_CELL_CONFIG_DIR	Required on IBM WebSphere
IDSTORE_WASADMINUSER	Required on IBM WebSphere

Example properties File

Here is a sample properties file for this option:

```

IDSTORE_HOST: node01.example.com
IDSTORE_PORT: 2345
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_READONLYUSER: IDROUser
IDSTORE_READWRITEUSER: IDRWUser
IDSTORE_SUPERUSER: weblogic_fa
IDSTORE_OAMSOFTWAREUSER: oamSoftwareUser
IDSTORE_OAMADMINUSER: oamAdminUser
IDSTORE_OIMADMINUSER: oimadminuser
POLICYSTORE_SHARES_IDSTORE: true
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
IDSTORE_OIMADMINGROUP: OIMAdministrators
IDSTORE_WLSADMINUSER: weblogic_idm
IDSTORE_WLSADMINGROUP: wlsadmingroup
IDSTORE_OAAMADMINUSER: oaamAdminUser
OIM_DB_URL: jdbc:oracle:thin:@xyz5678.us.example.com:5522:wasdb1
OIM_DB_SCHEMA_USERNAME: dev_oim
OIM_WAS_CELL_CONFIG_DIR:
/wassh/WebSphere/AppServer/profiles/Dmgr04/config/cells/xyz5678Cell104/fmwconfig
IDSTORE_WASADMINUSER: websphere_idm
    
```

See Also: [Table D-2](#) for details of the properties.

D.4.3 configPolicyStore Command

Syntax

```
idmConfigTool.sh -configPolicyStore input_file=input_properties
```

Properties

[Table D-12](#) lists the command properties.

Table D-12 *Properties for ConfigPolicyStore*

Property	Required?
POLICYSTORE_HOST	YES
POLICYSTORE_PORT	YES
POLICYSTORE_BINDDN	YES
POLICYSTORE_SEARCHBASE	YES
POLICYSTORE_SYSTEMIDBASE	
POLICYSTORE_READONLYUSER	YES
POLICYSTORE_READWRITEUSER	YES
POLICYSTORE_CONTAINER	YES

Example properties File

Here is a sample properties file for this option, which creates readonly user and writeonly user in the policy store:

```
POLICYSTORE_HOST: mynode.us.example.com
POLICYSTORE_PORT: 3060
POLICYSTORE_BINDDN: cn=orcladmin
POLICYSTORE_READONLYUSER: PolicyROUser
POLICYSTORE_READWRITEUSER: PolicyRWUser
POLICYSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_CONTAINER: cn=jpsroot
```

See Also: [Table D-2](#) for details of the properties.

D.4.4 configOAM Command**Prerequisite**

Ensure that the administration server for the domain hosting Oracle Access Manager is running before you execute this command.

Restart all servers on the OIM domain after running `configOIM`.

Syntax

On Linux, the command syntax is:

```
idmConfigTool.sh -configOAM input_file=input_properties
```

On Windows, the command syntax is:

```
idmConfigTool.bat -configOAM input_file=input_properties
```

For example:

```
idmConfigTool.sh -configOAM input_file=OAMconfigPropertyFile
```

Properties

[Table D-13](#) lists the command properties.

Table D-13 *Properties of configOAM*

Property	Required?
WLSHOST	YES WLSHOST and WLSPORT are, respectively, the host and port of your administration server, this will be the virtual name.
WLSPORT	YES
WLSADMIN	YES
IDSTORE_BINDDN	YES

Table D–13 (Cont.) Properties of configOAM

Property	Required?
IDSTORE_HOST	YES IDSTORE_HOST and IDSTORE_PORT are, respectively, the host and port of your Identity Store directory. If using a directory server other than Oracle Internet Directory or Oracle Unified Directory, specify the Oracle Virtual Directory host and port.
IDSTORE_PORT	YES
IDSTORE_DIRECTORYTYPE	YES
IDSTORE_BINDDN	YES IDSTORE_BINDDN is an administrative user in Oracle Internet Directory or Oracle Unified Directory. If using a directory server other than Oracle Internet Directory or Oracle Unified Directory, specify an Oracle Virtual Directory administrative user.
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	YES
IDSTORE_USERSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_OAMSOFTWAREUSER	YES
IDSTORE_OAMADMINUSER	YES
IDSTORE_SYSTEMIDBASE	YES
PRIMARY_OAM_SERVERS	YES
WEBGATE_TYPE	YES Default is ohsWebgate11g WEBGATE_TYPE is the type of WebGate agent you want to create. Valid values are ohsWebgate11g if WebGate version 11 is used, or ohsWebgate10g if WebGate version 10 is used.
ACCESS_GATE_ID	YES ACCESS_GATE_ID is the name you want to assign to the WebGate. Do <i>not</i> change the property value shown in the example.

Table D-13 (Cont.) Properties of configOAM

Property	Required?
OAM_TRANSFER_MODE	YES Default is OPEN OAM_TRANSFER_MODE is the security model in which the access servers function.
COOKIE_DOMAIN	YES
COOKIE_EXPIRY_INTERVAL	YES
OAM11G_WG_DENY_ON_NOT_PROTECTED	YES
OAM11G_IDM_DOMAIN_OHS_HOST	YES
OAM11G_IDM_DOMAIN_OHS_PORT	YES
OAM11G_IDM_DOMAIN_OHS_PROTOCOL	YES default is http OAM11G_IDM_DOMAIN_OHS_PROTOCOL is the protocol to use when directing requests to the load balancer.
OAM11G_OAM_SERVER_TRANSFER_MODE	YES OAM11G_OAM_SERVER_TRANSFER_MODE is the security model for the Access Manager servers. Access Manager must be configured for SIMPLE as the mode of communication.
OAM11G_IDM_DOMAIN_LOGOUT_URLS	
OAM11G_OIM_WEBGATE_PASSWD	YES
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	YES

Table D–13 (Cont.) Properties of configOAM

Property	Required?
OAM11G_SSO_ONLY_FLAG	<p>YES</p> <p>Default is TRUE</p> <p>OAM11G_SSO_ONLY_FLAG configures Access Manager 11g as authentication only mode or normal mode, which supports authentication and authorization. Default value is true.</p> <p>If OAM11G_SSO_ONLY_FLAG is true, the Access Manager 11g server operates in authentication only mode, where all authorizations return true by default without any policy validations. In this mode, the server does not have the overhead of authorization handling. This is recommended for applications which do not depend on authorization policies and need only the authentication feature of the Access Manager server.</p> <p>If the value is false, the server runs in default mode, where each authentication is followed by one or more authorization requests to the Access Manager server. WebGate allows the access to the requested resources or not, based on the responses from the Access Manager server.</p>
OAM11G_OIM_INTEGRATION_REQ	YES
OAM11G_IMPERSONATION_FLAG	<p>YES</p> <p>OAM11G_IMPERSONATION_FLAG enables or disables the impersonation feature in the OAM Server. Valid values are true (enable) and false (disable). The default is false. If you are using impersonalization, you must manually set this value to true.</p>
OAM11G_SERVER_LBR_HOST	YES
OAM11G_SERVER_LBR_PORT	YES
OAM11G_SERVER_LBR_PROTOCOL	<p>YES</p> <p>Default is http</p> <p>OAM11G_SERVER_LBR_PROTOCOL is the URL prefix to use.</p>
OAM11G_SERVER_LOGIN_ATTRIBUTE	YES
OAM11G_IDSTORE_NAME	YES
POLICYSTORE_SHARES_IDSTORE	YES

Table D-13 (Cont.) Properties of configOAM

Property	Required?
OAM11G_OIM_OHS_URL	http://sso.example.com:443/ OAM11G_OIM_OHS_URL is the URL of the load balancer or OHS fronting the OIM server.
SPLIT_DOMAIN	Set to true for cross-domain deployment. Omit for single-domain deployment. SPLIT_DOMAIN set to true is required to suppress the double authentication of Oracle Access Management administration console in a split domain scenario.

Example properties File

Here is a sample properties file for this option, which creates an entry for webgate in Access Manager:

```

WLSHOST: adminvhn.example.com
WLSPORT: 7001
WLSADMIN: weblogic
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_OAMSOFTWAREUSER: oamLDAP
IDSTORE_OAMADMINUSER: oamadmin
PRIMARY_OAM_SERVERS: oamhost1.example.com:5575,oamhost2.example.com:5575
WEBGATE_TYPE: ohsWebgate11g
ACCESS_GATE_ID: Webgate_IDM
OAM11G_IDM_DOMAIN_OHS_HOST:sso.example.com
OAM11G_IDM_DOMAIN_OHS_PORT:443
OAM11G_IDM_DOMAIN_OHS_PROTOCOL:https
OAM11G_OAM_SERVER_TRANSFER_MODE:simple
OAM11G_IDM_DOMAIN_LOGOUT_URLS:
/console/jsp/common/logout.jsp,/em/targetauth/emaslogout.jsp
OAM11G_WG_DENY_ON_NOT_PROTECTED: false
OAM11G_SERVER_LOGIN_ATTRIBUTE: uid
OAM_TRANSFER_MODE: simple
COOKIE_DOMAIN: .example.com
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
OAM11G_SSO_ONLY_FLAG: false
OAM11G_OIM_INTEGRATION_REQ: true or false
OAM11G_IMPERSONATION_FLAG:true
OAM11G_SERVER_LBR_HOST:sso.example.com
OAM11G_SERVER_LBR_PORT:443
OAM11G_SERVER_LBR_PROTOCOL:https
COOKIE_EXPIRY_INTERVAL: -1
OAM11G_OIM_OHS_URL:https://sso.example.com:443/
SPLIT_DOMAIN: true
OAM11G_IDSTORE_NAME: OAMIDStore
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com

```

Usage Notes

When you execute this command, the tool prompts you for:

- Password of the identity store account to which you are connecting
- Access Manager administrator password
- Access Manager software user password

In the IBM WebSphere environment:

- Run `idmconfigtool` from the Oracle Access Manager WebSphere cell.
- Provide details of the IBM WebSphere server by specifying the following in the properties file:
 - `WLSHOST` - The WebSphere Application Server host
 - `WLSPORT` - The WebSphere Application Server bootstrap port
 - `WLSADMIN` - Login ID for the Oracle Access Manager Admin console.

See Also: [Table D-2](#) for details of the properties.

D.4.5 configOIM Command

As of 11g Release 2 (11.1.2), `configOIM` supports 11g webgate by default. See the `WEBGATE_TYPE` option for details.

As indicated in the table, certain properties are required when Oracle Identity Manager and Access Manager are configured on different weblogic domains.

Prerequisites

Prior to running `configOIM`:

- `configOAM` must run successfully
- the admin server hosting OAM has to be restarted
- the admin server(s) hosting OIM and OAM must be running
- if using the `OIM_MSM_REST_SERVER_URL` property, in addition to the above, ensure that the URL is seeded in credential `msmLoginConfig`, and the system property 'OMSS Enabled' is set to `true`.

Syntax

On Linux, the command syntax is:

```
idmConfigTool.sh -configOIM input_file=configfile
```

On Windows, the command syntax is:

```
idmConfigTool.bat -configOIM input_file=configfile
```

For example:

```
idmConfigTool.sh -configOIM input_file=OIMconfigPropertyFile
```

Properties

[Table D-14](#) lists the command properties.

Table D–14 Properties for configOIM

Property	Required?
LOGINURI	Required by Oracle Platform Security Services (OPSS).
LOGOUTURI	Required by OPSS.
AUTOLOGINURI	Required by OPSS.
ACCESS_SERVER_HOST	YES
ACCESS_GATE_ID	YES ACCESS_GATE_ID must be the same as the ACCESS_GATE_ID value that you provided in the properties file for the configOAM command. (See Section D.4.4 , which covers configuring the Identity Store using the idmConfigTool with the -configOAM command.)
ACCESS_SERVER_PORT	YES
COOKIE_DOMAIN	YES
COOKIE_EXPIRY_INTERVAL	YES
WEBGATE_TYPE	YES
OAM_TRANSFER_MODE	YES OAM_TRANSFER_MODE must be the same as the OAM_TRANSFER_MODE value that you provided in the properties file for the configOAM command. (See Section D.4.4 , which covers configuring the Identity Store using the idmConfigTool with the -configOAM command.)
SSO_ENABLED_FLAG	YES
IDSTORE_HOST	YES Set IDSTORE_HOST to your Oracle Unified Directory or Oracle Internet Directory host or load balancer name if you are using Oracle Unified Directory or Oracle Internet Directory as your Identity Store. If not, set it to your Oracle Virtual Directory host or load balancer name.
IDSTORE_PORT	YES Set IDSTORE_PORT to your Oracle Unified Directory or Oracle Internet Directory port if you are using Oracle Unified Directory or Oracle Internet Directory as your Identity Store. If not, set it to your Oracle Virtual Directory port.
IDSTORE_BINDDN	
IDSTORE_DIRECTORYTYPE	YES Set IDSTORE_DIRECTORYTYPE to OVD if you are using Oracle Virtual Directory server to connect to either a non-OID directory, Oracle Internet Directory or Oracle Unified Directory. Set it to OID if your Identity Store is in Oracle Internet Directory and you are accessing it directly rather than through Oracle Virtual Directory. Set this value to OUD, if your identity store is in Oracle Unified Directory and you are accessing it directly rather than through OVD.
IDSTORE_LOGINATTRIBUTE	YES
IDSTORE_ADMIN_USER	YES Set IDSTORE_ADMIN_USER to the complete LDAP DN of the administrator of the identity store directory. This should be the same user specified for IDSTORE_OAMSOFTWAREUSER (if specified).

Table D-14 (Cont.) Properties for configOIM

Property	Required?
IDSTORE_SEARCHBASE	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_WLSADMINUSER	YES. Default is weblogic_idm IDSTORE_WLSADMINUSER is the value of the user which must be the same value as provided while running prepareIdStore mode=wls command.
IDSTORE_WLSADMINUSER_PWD	
MDS_DB_URL	YES
MDS_DB_SCHEMA_USERNAME	YES
WLSHOST	YES WLSHOST, WLSPORT, WLSADMIN are all properties related to Oracle Identity Manager and also for Access Manager only in-case of single domain configuration. In the split domain case where Oracle Identity Manager and Access Manager are in different domains, WLSHOST, WLSPORT, WLSADMIN are related to Oracle Identity Manager.
WLSPORT	YES
WLSADMIN	YES
DOMAIN_NAME	YES
DOMAIN_LOCATION	YES
OIM_MANAGED_SERVER_NAME	YES
OIM_WEB_SERVER_HOST	
OIM_WEB_SERVER_PORT	
OAM_SERVER_VERSION	Required only when Access Manager server does not support 11g webgate in Oracle Identity Manager-Access Manager integration. In that case, provide the value '10g'.
OAM11G_WLS_ADMIN_HOST	Required if Access Manager and Oracle Identity Manager servers are configured on different Weblogic domains (cross-domain setup)
OAM11G_WLS_ADMIN_PORT	Required if Access Manager and Oracle Identity Manager servers are configured on different Weblogic domains (cross-domain setup)
OAM11G_WLS_ADMIN_USER	Required if Access Manager and Oracle Identity Manager servers are configured on different Weblogic domains (cross-domain setup)
WLSPASSWD	Required for OMSM-OIM.
OAM11G_WLS_ADMIN_PASSWD	Required on IBM WebSphere.

Table D-14 (Cont.) Properties for configOIM

Property	Required?
OAM_ADMIN_WAS_DEFAULT_PORT	Required on IBM WebSphere, must be OAM node's OracleAdminServer default port number. To find this port number: <ol style="list-style-type: none"> 1. Navigate to the WebSphere admin console for OAM. 2. Go to Servers -> Server Types -> WebSphere application servers. 3. click on 'OracleAdminServer'. 4. Under 'Communications', expand 'Ports'. 5. 'WC_defaulthost' port is the OAM Node's OracleAdminServer default port number.
OIM_MSM_REST_SERVER_URL	Set OIM_MSM_REST_SERVER_URL: https://host:port. Set the property so the MSM URL is seeded in Oracle Identity Manager and sets the system property OMSS_Enabled. OIM_MSM_REST_SERVER_URL enables the Mobile Security Manager task flows in the Oracle Identity Manager console. If not set, configOIM will continue the configuration without configuring the Mobile Security Manager. The prerequisite for OMSS_Enabled is that the Oracle Identity Manager server should be up.

Note: If Access Manager and Oracle Identity Manager are on separate WebLogic domains, set OAM11G_WLS_ADMIN_HOST, OAM11G_WLS_ADMIN_PORT, and OAM11G_WLS_ADMIN_USER. OAM11G_WLS_ADMIN_HOST, OAM11G_WLS_ADMIN_PORT, and OAM11G_WLS_ADMIN_USER properties are related to Access Manager. For information about split domain integration topology, see Chapter 1.

Example properties File

Here is a sample properties file for this option, which seeds the SSOAccessKey, SSOKeystoreKey, SSOGlobalPP keys in the credential store framework (CSF):

```

LOGINURI: /${app.context}/adfAuthentication
LOGOUTURI: /oamssso/logout.html
AUTOLOGINURI: None
ACCESS_SERVER_HOST: OAMHOST1.example.com
ACCESS_SERVER_PORT: 5575
ACCESS_GATE_ID: Webgate_IDM
COOKIE_DOMAIN: .example.com
COOKIE_EXPIRY_INTERVAL: -1
OAM_TRANSFER_MODE: simple
WEBGATE_TYPE: ohsWebgate11g
SSO_ENABLED_FLAG: true
IDSTORE_PORT: 389
IDSTORE_HOST: idstore.example.com
IDSTORE_DIRECTORYTYPE: OVD
IDSTORE_ADMIN_USER: cn=oamLDAP,cn=systemids,dc=example,dc=com
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
MDS_DB_URL: jdbc:oracle:thin:DB Hostname:DB portno.:SID
MDS_DB_SCHEMA_USERNAME: edg_mds
WLSHOST: adminvhn.example.com
WLSPORT: 7001
WLSADMIN: weblogic
DOMAIN_NAME: IDMDomain

```

```
OIM_MANAGED_SERVER_NAME: WLS_OIM1
DOMAIN_LOCATION: ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_SEARCHBASE: dc=us,dc=example,dc=com
IDSTORE_WLSADMINUSER: weblogic_idm
OIM_WEB_SERVER_HOST: tx401alu.us.example.com
OIM_WEB_SERVER_PORT: 7777
OAM11G_WLS_ADMIN_HOST: abc1234.us.example.com
OAM11G_WLS_ADMIN_PORT: 9810
OAM11G_WLS_ADMIN_USER: wasadmin
OAM_ADMIN_WAS_DEFAULT_PORT: 7443
```

Usage Notes

When integrating Oracle Mobile Security Suite (MSM) with OIM, you may see the error:

```
SEVERE: System property OMSS Enabled could not be changed null
```

To work around this issue, provide the value of `WLSPASSWD` in the property file to seed the MSM URL.

In the IBM WebSphere environment:

- If Oracle Identity Manager (OIM) and Access Manager (OAM) are configured in two different WebSphere cells, you must specify the following properties:
 - `OAM11G_WLS_ADMIN_HOST` (OAM host on the Websphere application server)
 - `OAM11G_WLS_ADMIN_PORT` (Websphere Deployment Manager bootstrap port for the OAM cell)
 - `OAM11G_WLS_ADMIN_USER` (primary administrative user name for OAM Websphere cell (For example, wasadmin))
- If OIM and OAM are part of the same WebSphere cell, you do not have to specify the above properties.
- The following `configOIM` command properties are specific to WebSphere:
 - `IDSTORE_SEARCHBASE` - The identity store search base
 - `OIM_WEB_SERVER_HOST` - The IBM HTTP Server (IHS) host or Oracle HTTP Server (OHS) host
 - `OIM_WEB_SERVER_PORT` - The IBM HTTP Server (IHS) port or OHS port.
 - `OAM_ADMIN_WAS_DEFAULT_PORT` - The OAM node's OracleAdminServer default port number. To determine the port number:
 - * Navigate to OAM admin console of WebSphere.
 - * Go to Servers -> Server Types -> WebSphere application servers
 - * click on 'OracleAdminServer'
 - * Under 'Communications', expand 'Ports'.
 - * 'WC_defaulthost' port is the OAM Node's OracleAdminServer default port number.

See Also: [Table D-2](#) for details of the properties.

D.4.6 configOMSS Command

Syntax

```
idmConfigTool.sh -configOMSS input_file=input_file_with_path
```

If a log for running the script is required, you can alternatively run the command as follows:

```
idmConfigTool.sh -configOMSS input_file=input_file_with_path log_level=FINEST log_file=log_file_with_path
```

Properties

[Table D-15](#) lists the command properties.

Table D-15 Properties for configOMSS

Property	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_PASSWD	YES
IDSTORE_USERNAMEATTRIBUTE	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_LOGINATTRIBUTE	YES
IDSTORE_SSL_ENABLED	
IDSTORE_DIRECTORYTYPE	YES
OMSS_OMSM_IDSTORE_PROFILENAME	YES
APPLE_CACERT_FILE	YES (for iOS)
WLSHOST	YES
WLSPORT	YES
WLSADMIN	YES
WLSPASSWD	YES
MSM_SCHEMA_USER	YES
OMSS_MSAS_SERVER_HOST	YES
OMSS_MSAS_SERVER_PORT	YES
PROXY_SERVER_HOST	
PROXY_SERVER_PORT	
USE_PROXY	
PROXY_USER	
PROXY_PASSWD	
OMSS_DOMAIN_LOCATION	YES
JDBC_URL	YES

Table D-15 (Cont.) Properties for configOMSS

Property	Required?
DB_PASSWD	YES
GCM_API_KEY	
GCM_SENDER_ID	
APNS_FILE	
APNS_KEYSTORE_PASSWD	
TOPIC	YES
SMTP_HOST	
SMTP_PORT	
EMAIL_ADMIN_USER	
EMAIL_ADMIN_PASSWD	
EXCHANGE_DOMAIN_NAME	
EXCHANGE_SERVER_URL	
EXCHANGE_LISTENER_URL	
EXCHANGE_SERVER_VERSION	
EXCHANGE_ADMIN_USER	
EXCHANGE_ADMIN_PASSWD	
SCEP_DYNAMIC_CHALLENGE_USER	
SCEP_DYNAMIC_CHALLENGE_PASSWD	
OMSS_KEYSTORE_PASSWORD	YES
OISM_IDSTORE_ROLE_SECURITY_ADMIN	
OISM_IDSTORE_ROLE_SECURITY_HELPDESK	
MSM_SERVER_KEY_LENGTH	
MSM_SERVER_NAME	
OAM_POLICY_MGR_SERVER_NAME	

Note: It is recommended that you not specify passwords within properties files. Upon execution, the command will prompt you for passwords.

Example properties File

Here is a sample properties file for this option:

```
# LDAP
IDSTORE_SSL_ENABLED: false
IDSTORE_DIRECTORYTYPE: AD
IDSTORE_HOST: qadc2.domain2.testqa1.com
IDSTORE_PASSWD:
IDSTORE_PORT: 389
IDSTORE_BINDDN: CN=Administrator,CN=Users,DC=domain2,DC=testqa1,DC=com
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_USERSEARCHBASE: OU=Users,OU=msm,DC=domain2,DC=testqa1,DC=com
IDSTORE_GROUPSEARCHBASE: OU=Roles,OU=msm,DC=domain2,DC=testqa1,DC=com
```



```

IDSTORE_SEARCHBASE: OU=msm,DC=domain2,DC=testqa1,DC=com
IDSTORE_SYSTEMIDBASE: OU=SystemIDS,OU=msm,DC=domain2,DC=testqa1,DC=com
IDSTORE_LOGINATTRIBUTE: cn
OMSS_OMSM_IDSTORE_PROFILENAME: idsprofile_test2
# Weblogic
WLSHOST: wlshost01.us.example.com
WLSPORT: 7001
WLSADMIN: weblogic
WLSPASSWD:
OMSS_DOMAIN_LOCATION: /scratch/domains/base_domain
# Keystore related config
OMSS_KEYSTORE_PASSWORD:
SCEP_DYNAMIC_CHALLENGE_USER: adminuser
SCEP_DYNAMIC_CHALLENGE_PASSWD:
OMSM_IDSTORE_ROLE_SECURITY_ADMIN: MSMAdmin
# MSAS and PROXY
OMSS_MSAS_SERVER_HOST:host02.us.example.com
OMSS_MSAS_SERVER_PORT:14181
PROXY_SERVER_HOST:www-proxy.us.example.com
PROXY_SERVER_PORT:80
#PROXY_USER:
#PROXY_PASSWD:
USE_PROXY:true
# DB
JDBC_URL:jdbc:oracle:thin:@host02.us.example.com:5521:msmdb
MSM_SCHEMA_USER: DEV_OMSM
DB_PASSWD:
# APNS/GCM
APNS_FILE: /scratch/APNS.p12
APNS_KEYSTORE_PASSWORD:
GCM_API_KEY:AIzaSyCh_JALj5YBAIy7Ekyw9LzovHqJ2YMGk2c
GCM_SENDER_ID:610046050155
#TOPIC:com.apple.mgmt.External.2544264e-aa8a-4654-bfff-9d897ed39a87
#Exchange & Email settings
EXCHANGE_SERVER_URL:http://testuri.com
EXCHANGE_LISTENER_URL:http://testuri.com
EXCHANGE_DOMAIN_NAME:test.com
EXCHANGE_ADMIN_USER: serviceuser
EXCHANGE_SERVER_VERSION:2.0
EXCHANGE_ADMIN_PASSWD:
EMAIL_ADMIN_USER: admin@acme.com
EMAIL_ADMIN_PASSWD:
SMTP_HOST:exchangeurl.us.example.com
SMTP_PORT:80

```

See Also: [Table D-2](#) for details of the properties.

D.4.7 postProvConfig Command

Syntax

```
idmConfigTool.sh -postProvConfig input_file=postProvConfig.props
```

Properties

The properties for this command are the same as for the preConfigIDStore command.

Example properties File

Here is a sample properties file for this option:

```
IDSTORE_HOST: host01.example.com
IDSTORE_PORT: 3060
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_USERSEARCHBASE: cn=systemids,dc=example,dc=com
POLICYSTORE_CONTAINER: cn=FAPolicies
POLICYSTORE_HOST: host01.ca.example.com
POLICYSTORE_PORT: 3060
POLICYSTORE_BINDDN: cn=orcladmin
POLICYSTORE_READWRITEUSER: cn=PolicyRWUser,cn=systemids,dc=example,dc=com
ovd.host: host01.ca.example.com
ovd.port: 6501
ovd.binddn: cn=orcladmin
OIM_T3_URL: t3://host02.ca.example.com:14000
OIM_SYSTEM_ADMIN: abcdef
```

See Also: [Table D-2](#) for details of the properties.

D.4.8 upgradeLDAPUsersForSSO Command**Syntax**

```
idmConfigTool.sh -upgradeLDAPUsersForSSO input_file=input_Properties
```

Properties

[Table D-16](#) lists the command properties.

Table D-16 *Properties for upgradeLDAPUsersForSSO*

Property	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_ADMIN_USER	YES
IDSTORE_DIRECTORYTYPE	YES
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
PASSWORD_EXPIRY_PERIOD	
IDSTORE_LOGINATTRIBUTE	YES

Example properties File

Here is a sample properties file for this option:

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_ADMIN_USER: cn=orcladmin
IDSTORE_DIRECTORYTYPE:OVD
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
PASSWORD_EXPIRY_PERIOD: 7300
```

```
IDSTORE_LOGINATTRIBUTE: uid
```

See Also: [Table D-2](#) for details of the properties.

D.4.9 validate IDStore Command

Syntax

```
idmConfigTool.sh -validate component=IDSTORE input_file=input_Properties
```

Properties

[Table D-17](#) lists the command properties.

Table D-17 *Properties for validate IDStore*

Property	Required?
IDSTORE_TYPE	
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_SSLPORT	YES
IDSTORE_SSL_ENABLED	YES
IDSTORE_SUPER_USER	YES
IDSTORE_READWRITEUSER	YES
IDSTORE_READONLYUSER	YES
IDSTORE_USER_BASE	YES
IDSTORE_GROUP_BASE	YES
IDSTORE_SEEDING	
IDSTORE_POST_VALIDATION	
IDSTORE_ADMIN_GROUP	YES
IDSTORE_ADMIN_GROUP_EXISTS	

Example properties File

Here is a sample properties file for this option:

```
idstore.type: OID
idstore.host: acb21005.us.example.com
idstore.port: 3030
idstore.sslport: 4140
idstore.ssl.enabled: false
idstore.super.user: cn=weblogic_fa,cn=systemids,dc=example,dc=com
idstore.readwrite.username: cn=IDRWUser,cn=systemids,dc=example,dc=com
idstore.readonly.username: cn=IDROUser,cn=systemids,dc=example,dc=com
idstore.user.base: cn=Users,dc=example,dc=com
idstore.group.base: cn=Groups,dc=example,dc=com
idstore.seeding: true
idstore.post.validation: false
idstore.admin.group: cn=IDM Administrators,cn=Groups,dc=example,dc=com
idstore.admin.group.exists: true
```

See Also: [Table D-2](#) for details of the properties.

D.4.10 validate PolicyStore Command

Syntax

```
idmConfigTool.sh -validate component=POLICYSTORE input_file=input_Properties
```

Properties

Table D-18 lists the command properties.

Table D-18 Properties for validate polycystore

Property	Required?
POLICYSTORE_HOST	YES
POLICYSTORE_PORT	YES
POLICYSTORE_SECURE_PORT	YES
POLICYSTORE_IS_SSL_ENABLED	
POLICYSTORE_READ_WRITE_USERNAME	
POLICYSTORE_SEEDING	
POLICYSTORE_JPS_ROOT_NODE	
POLICYSTORE_DOMAIN_NAME	YES
POLICYSTORE_CREATED_BY_CUSTOMER	
POLICYSTORE_JPS_CONFIG_DIR	
POLICYSTORE_CRED_MAPPING_FILE_LOCATION	
POLICYSTORE_ADF_CRED_FILE_LOCATION	
POLICYSTORE_STRIPE_FSCM	
POLICYSTORE_STRIPE_CRM	
POLICYSTORE_STRIPE_HCM	
POLICYSTORE_STRIPE_SOA_INFRA	
POLICYSTORE_STRIPE_APM	
POLICYSTORE_STRIPE_ESSAPP	
POLICYSTORE_STRIPE_B2BUI	
POLICYSTORE_STRIPE_OBI	
POLICYSTORE_STRIPE_WEBCENTER	
POLICYSTORE_STRIPE_IDCCS	
POLICYSTORE_CRED_STORE	
IDM_KEYSTORE_FILE	

Example properties File

Here is a sample properties file for this option:

```
POLICYSTORE_HOST: node0316.example.com
POLICYSTORE_PORT: 3067
POLICYSTORE_SECURE_PORT: 3110
POLICYSTORE_IS_SSL_ENABLED: FALSE
POLICYSTORE_READ_WRITE_USERNAME: cn=PolicyRWUser,cn=systemids,dc=example,dc=com
POLICYSTORE_SEEDING: true
```

```
POLICYSTORE_JPS_ROOT_NODE: cn=jpsroot
POLICYSTORE_DOMAIN_NAME: dc=example,dc=com
```

See Also: [Table D-2](#) for details of the properties.

D.4.11 validate OAM Command (11g)

Prerequisite

Ensure that the administration server and managed servers hosting Oracle Access Manager components are running before you execute this command.

Syntax

```
idmConfigTool.sh -validate component=OAM11g input_file=input_Properties
```

Note: The tool prompts for the WebLogic administration server user password upon execution.

Properties

[Table D-19](#) lists the command properties.

Table D-19 *Properties for validate component=OAM11g*

Property	Required?
ADMIN_SERVER_HOST	YES
ADMIN_SERVER_PORT	YES
ADMIN_SERVER_USER	YES
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_IS_SSL_ENABLED	
OAM11G_ACCESS_SERVER_HOST	YES
OAM11G_ACCESS_SERVER_PORT	YES
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	
OAM11G_OIM_INTEGRATION_REQ	
OAM11G_OAM_ADMIN_USER	
OAM11G_SSO_ONLY_FLAG	

Example properties File

Here is a sample properties file for this option, which validates the Access Manager server:

```
admin_server_host: abc5411405.ca.example.com
admin_server_port: 17001
admin_server_user: weblogic
IDSTORE_HOST:abc5411405.ca.example.com
IDSTORE_PORT:3060
IDSTORE_IS_SSL_ENABLED:false
OAM11G_ACCESS_SERVER_HOST:abc5411405.ca.example.com
OAM11G_ACCESS_SERVER_PORT:5575
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN:OAMAdministrators
```

```
OAM11G_OIM_OHS_URL: http://abc5411405.ca.example.com:7779/  
OAM11G_OIM_INTEGRATION_REQ: true  
OAM11G_OAM_ADMIN_USER:oamadminuser  
OAM11G_SSO_ONLY_FLAG: false  
OAM11G_OAM_ADMIN_USER_PASSWD:
```

See Also: [Table D-2](#) for details of the properties.

D.4.12 validate OAM Command (10g)

Syntax

```
idmConfigTool.sh -validate component=OAM10g input_file=input_Properties
```

Properties

[Table D-20](#) lists the command properties.

Table D-20 Properties for validate component=OAM10g

Property	Required?
OAM10g_MODE	
OAM10g_NOPROMPT	
OAM10g_POLICY_HOST	
OAM10g_POLICY_PORT	
OAM10g_POLICY_USERDN	
OAM10g_POLICY_USERPWD	
OAM10g_AAA_MODE	
OAM10g_AAA_PASSPHRASE	
OAM10g_PRIMARY_SERVERS	
OAM10g_SECONDARY_SERVERS	
OAM10g_RUNTIME_USER	

See Also: [Table D-2](#) for details of the properties.

D.4.13 validate OIM command

Prerequisite

Ensure that the administration server and managed servers hosting Oracle Access Manager components are running before you execute this command.

Syntax

```
idmConfigTool.sh -validate component=OIM11g input_file=input_Properties
```

Note: The tool prompts for the WebLogic administration server user password upon execution.

Properties

[Table D-21](#) lists the command properties.

Table D–21 Properties for validate component=OIM11g

Property	Required?
ADMIN_SERVER_HOST	YES
ADMIN_SERVER_PORT	YES
ADMIN_SERVER_USER	YES
OAM_HOST	
OAM_NAP_PORT	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
OIM_IS_SSL_ENABLED	
OIM_FRONT_END_URL	YES
OIM_T3_URL	YES

Example properties File

Here is a sample properties file for this option:

```
admin_server_host: node06.example.com
admin_server_port: 17111
admin_server_user: weblogic
oam_host: node06.example.com
oam_nap_port: 5575
idm.keystore.file: idm.keystore.file
idstore.user.base: cn=Users,dc=example,dc=com
idstore.group.base: cn=Groups,dc=example,dc=com
oim_is_ssl_enabled: false
OIM_FRONT_END_URL: http://node06.example.com:14000
OIM_T3_URL: t3://node06.example.com:14000
```

See Also: [Table D–2](#) for details of the properties.

D.4.14 configOVD Command**Syntax**

```
idmConfigTool.sh -configOVD input_file=input_Properties
```

Properties

[Table D–22](#) lists the command properties (in ldapn properties, n=1,2..).

Table D–22 configOVD properties

Property	Required?
ovd.host	YES
ovd.port	YES
ovd.binddn	YES
ovd.ssl	
ldapn.type	
ldapn.host	YES

Table D-22 (Cont.) configOVD properties

Property	Required?
ldapn.port	YES
ldapn.binddn	YES
ldapn.ssl	
ldapn.base	YES
ldapn.ovd.base	YES
usecase.type	YES
ovd.oamenabled	

Example Properties Files

The content of the properties file for the configOVD command depends on the Oracle Virtual Directory configuration. This section provides some sample files.

Here is an example of the file named single.txt for a single-server configuration:

```
ovd.host:myhost.us.example.com
ovd.port:7000
ovd.binddn:cn=orcladmin
ovd.ssl:true
ldap1.type:OID
ldap1.host:myhost.us.example.com
ldap1.port:7000
ldap1.binddn:cn=oimadmin,cn=systemids,dc=example,dc=com
ldap1.ssl:false
ldap1.base:dc=example,dc=com
ldap1.ovd.base:dc=example,dc=com
usecase.type: single
```

The user referenced in the ldap1.binddn: parameter is the proxy user for Oracle Identity Manager, created when you pre-configure the identity store.

When using this file, the command is invoked as:

```
idmConfigTool -configOVD input_file=path/single.txt
```

```
Enter OVD password: password
Enter LDAP password: password
```

Here is an example of the file named split.txt for a split-profile server configuration:

```
ovd.host:myhost.us.example.com
ovd.port:7000
ovd.binddn:cn=orcladmin
ovd.ssl:true
ldap1.type:AD
ldap1.host:10.0.0.0
ldap1.port:7000
ldap1.binddn:administrator@idmqa.com
ldap1.ssl:true
ldap1.base:dc=idmqa,dc=com
ldap1.ovd.base:dc=idmqa,dc=com
usecase.type: split
ldap2.type:OID
ldap2.host:myhost.us.example.com
ldap2.port:7000
ldap2.binddn:cn=oimadmin,cn=systemids,dc=example,dc=com
```



```
ldap2.ssl:false
ldap2.base:dc=example,dc=com
ldap2.ovd.base:dc=example,dc=com
```

When using this file, the command is thus invoked as:

```
idmConfigTool -configOVD input_file=path/split.txt
```

```
Enter OVD password: password
Enter LDAP1 password: password
Enter LDAP2 password: password
```

See Also: [Table D-2](#) for details of the properties.

D.4.15 ovdConfigUpgrade Command

Syntax

```
idmConfigTool.sh -ovdConfigUpgrade input_file=input_Properties
```

Properties

[Table D-23](#) lists the command properties.

Table D-23 *ovdConfigUpgrade Properties*

Property	Required?
ovd.host	
ovd.port	
ovd.binddn	
ovd.ssl	
ldapn.binddn	
ldapn.ssl	

Example properties File

Here is a sample properties file for this option which upgrades the existing adapters:

```
ovd.host:abk005sjc.us.myhost.com
ovd.port:8801
ovd.binddn:cn=orcladmin
ovd.ssl:true
```

See Also: [Table D-2](#) for details of the properties.

D.4.16 disableOVDAccessConfig Command

Syntax

```
idmConfigTool.sh -disableOVDAccessConfig input_file=input_Properties
```

Properties

[Table D-24](#) lists the command properties.

Table D–24 *disableOVDAccessConfig Properties*

Property	Required?
ovd.host	
ovd.port	
ovd.binddn	
ovd.ssl	
ldapn.binddn	
ldapn.ssl	

Example properties File

Here is a sample properties file for this option which disables the anonymous access in Oracle Virtual Directory:

```
ovd.host:abc00def.ca.example.com
ovd.port:8501
ovd.binddn:cn=orcladmin
ovd.ssl:true
```

See Also: [Table D–2](#) for details of the properties.

D.4.17 upgradeOIMTo11gWebgate**Syntax**

```
idmConfigTool.sh -upgradeOIMTo11gWebgate input_file=input_Properties
```

Properties

This command uses the same properties that are required for the `configOIM` command, so the same properties file can work for both. See [Table D–14](#).

As indicated in the table, certain properties are required when Oracle Identity Manager and Access Manager are configured on different weblogic domains.

See Also: [Table D–2](#) for details of the properties.

D.5 Additional Tasks for OUD Identity Store in an HA Environment

This section explains additional tasks you may need to perform when using `idmConfigTool` for a target Oracle Unified Directory (OUD) identity store in a high-availability environment. Topics include:

- [Creating the Global ACI for Oracle Unified Directory](#)
- [Creating Indexes on Oracle Unified Directory Replicas](#)

D.5.1 Creating the Global ACI for Oracle Unified Directory

Global ACI and indexes are not replicated when you use `idmConfigTool` for an Oracle Unified Directory (OUD) identity store in a high availability (HA) environment that contains replicas. Global ACI and indexes are created **ONLY** in the instance(s) specified in the property file. You must manually re-create (remove then create) them on all other OUD instances of the replication domain.

Consequently you must first grant access to the change log, and then create the ACIs. Take these steps:

1. Create a file called `mypassword` which contains the password you use to connect to OUD.
2. Remove the existing change log on one of the replicated OUD hosts. The command syntax is:

```

OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--remove \
global-aci:"(target=\"ldap:///cn=changelog\") (targetattr=\"*\") (version 3.0;
acl \"External changelog access\"; deny (all) userdn=\"ldap:///anyone\");\"
--hostname OUD Host \
--port OUD Admin Port \
--trustAll ORACLE_INSTANCE/config/admin-truststore \
--bindDN cn=oudadmin \
--bindPasswordFile mypassword \
--no-prompt

```

For example:

```

OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--remove
global-aci:"(target=\"ldap:///cn=changelog\") (targetattr=\"*\") (version 3.0;
acl \"External changelog access\"; deny (all) userdn=\"ldap:///anyone\");\"
--hostname OUDHOST1.example.com \
--port 4444 \
--trustAll /u01/app/oracle/admin/oud1/OU/D/config/admin-truststore \
--bindDN cn=oudadmin \
--bindPasswordFile mypassword \
--no-prompt

```

3. Add the new ACI for the changelog:

```

OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add global-aci:"(target=\"ldap:///cn=changelog\") (targetattr=\"*\") (version
3.0; acl \"External changelog access\"; allow
(read,search,compare,add,write,delete,export)
groupdn=\"ldap:///cn=oimAdminGroup,cn=groups,dc=example,dc=com\");\" \
--hostname OUD Host \
--port OUD Admin Port \
--trustAll \
--bindDN cn=oudadmin \
--bindPasswordFile password
--no-prompt

```

For example:

```

OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add
--add global-aci:"(target=\"ldap:///cn=changelog\") (targetattr=\"*\") (version
3.0; acl \"External changelog access\"; allow
(read,search,compare,add,write,delete,export)
groupdn=\"ldap:///cn=oimAdminGroup,cn=groups,dc=example,dc=com\");\" \
--hostname OUDHOST1 \
--port 4444 \
--trustAll \
--bindDN cn=oudadmin \
--bindPasswordFile password
--no-prompt

```

4. Then add the ACI:

```

OULD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add global-aci:"(targetcontrol=\\"1.3.6.1.4.1.26027.1.5.4 ||
1.3.6.1.4.1.26027.2.3.4\\")(version 3.0; acl \\"OIMAdministrators control
access\\"; allow(read)
groupdn=\\"<ldap:///cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com\\;" ) \" \
--hostname OULD_HOST \
--port OULD_ADMIN_PORT \
--trustAll \
--bindDN cn=oudadmin \
--bindPasswordFile passwordfile \
--no-prompt

```

For example:

```

OULD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add global-aci:"(targetcontrol=\\"1.3.6.1.4.1.26027.1.5.4 ||
1.3.6.1.4.1.26027.2.3.4\\")(version 3.0; acl \\"OIMAdministrators control
access\\"; allow(read)
groupdn=\\"ldap:///cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com\\;" ) \" \
--hostname IDMHOST1.mycompany.com \
--port 4444 \
--trustAll \
--bindDN cn=oudadmin \
--bindPasswordFile mypasswordfile \
--no-prompt

```

5. Finally add the ACI:

```

OULD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add
global-aci:"(target=\\"ldap:///\\")(targetscope=\\"base\\")(targetattr=\\"lastExtern
alChangelogCookie\\")(version 3.0; acl \\"User-Visible lastExternalChangelog\\";
allow (read,search,compare)
groupdn=\\"ldap:///cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com\\;" ) \" \
--hostname OULD_HOST \
--port OULD_ADMIN_PORT \
--trustAll \
--bindDN cn=oudadmin \
--bindPasswordFile passwordfile \
--no-prompt

```

For example:

```

OULD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add
global-aci:"(target=\\"ldap:///\\")(targetscope=\\"base\\")(targetattr=\\"lastExtern
alChangelogCookie\\")(version 3.0; acl \\"User-Visible lastExternalChangelog\\";
allow (read,search,compare)
groupdn=\\"ldap:///cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com\\;" ) \" \
--hostname IDMHOST1.mycompany.com \
--port 4444 \
--trustAll \
--bindDN cn=oudadmin \
--bindPasswordFile mypasswordfile \
--no-prompt

```

6. Repeat Steps 1 through 5 for each OUD instance.

D.5.2 Creating Indexes on Oracle Unified Directory Replicas

When `idmConfigTool` prepares the identity store, it creates a number of indexes on the data. However in a high availability (HA) environment that contains replicas, global ACI and indexes are created only in the instance(s) specified in the property file; the replicas are not updated with the indexes which need to be added manually.

The steps are as follows (with `LDAPHOST1.example.com` representing the first OUD server, `LDAPHOST2.example.com` the second server, and so on):

1. Create a file called `mypassword` which contains the password you use to connect to OUD.
2. Configure the indexes on the second OUD server:

```
ORACLE_INSTANCE/OU/binary/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444
-a -D "cn=oudadmin" -j mypassword -c -f
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/ldif/ojd/schema/ojd_user_
index_generic.ldif
```

and

```
ORACLE_INSTANCE/OU/binary/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444
-a -D "cn=oudadmin" -j mypassword -c -f
/u01/app/oracle/product/fmw/iam/idmtools/templates/oud/oud_indexes_extn.ldif
```

Notes:

- Repeat both commands for all OUD servers for which `idmConfigTool` was not run.
 - Execute the commands on one OUD instance at a time; that instance must be shut down while the commands are running.
-
-

3. Rebuild the indexes on all the servers:

```
ORACLE_INSTANCE/OU/binary/bin/rebuild-index -h localhost -p 4444 -X -D
"cn=oudadmin" -j mypassword --rebuildAll -b "dc=example,dc=com"
```

Note: You must run this command on all OUD servers, including the first server (`LDAPHOST1.example.com`) for which `idmConfigTool` was run.

Enabling LDAP Synchronization in Oracle Identity Manager

This appendix explains how to manually configure LDAP synchronization of Oracle Identity Manager with the LDAP identity store post-installation.

Note: LDAP synchronization is required only if you are using Oracle Identity Manager in database mode, and Oracle Identity Manager is integrated with Access Manager (OAM). If your installation does not require OAM, then LDAP synchronization is not required and you can skip this appendix.

If you plan to use LDAP synchronization, there are prerequisite steps that must be taken to configure the LDAP directories. These prerequisites are described in subsequent sections in this document.

For an overview of the integration between LDAP identity store and Oracle Identity Manager, see [Section 1.1.3, "About LDAP Synchronization in Oracle Identity Manager"](#).

This appendix contains the following topics:

- [Configuring LDAP Synchronization](#)
- [Managing LDAP Synchronization](#)

E.1 Configuring LDAP Synchronization

Perform the following steps to configure LDAP synchronization:

1. Ensure that all prerequisites are performed in the identity store. See [Section E.1.1, "Completing the Prerequisites for Enabling LDAP Synchronization"](#) for more information.
2. Create the OVD adapters.

In LDAP synchronization, Oracle Identity Manager uses the virtualization functionality of OVD. This can be used in any one of the following ways:

- Install a standalone instance of OVD: When you use a standalone instance of OVD, you must create OVD adapters.
- Use Identity Virtualization Library (libOVD): With libOVD, a runtime library is used by Oracle Identity Manager as part of its own process, which simplifies installation and maintenance.

For detailed information, see [Section E.1.3, "Creating OVD Adapters"](#).

3. Enable LDAP synchronization. See [Section E.1.4, "Enabling LDAP Synchronization"](#) for information.
4. Perform post-configuration steps of LDAP synchronization. See [Section E.2.1, "Running the LDAP Post-Configuration Utility"](#) for information.
5. Verify LDAP synchronization. See [Section E.2.2, "Verifying the LDAP Synchronization"](#) for details.

E.1.1 Completing the Prerequisites for Enabling LDAP Synchronization

LDAP directory servers must be configured with default containers (including changelog), administrators, and Access Control Lists (ACIs). The exact procedure is determined by the choice of LDAP server.

- **Preconfiguring OID, OUD, and standalone OVD:** Preconfigure OID, OUD, and OVD by running the `idmConfigTool` utility. This adds user, group, and reserve containers and the appropriate ACIs. The required preconfiguration step is performed by the following command:

```
idmConfigTool -preConfigIDStore
```

The `idmConfigTool` is in the `IAM_ORACLE_HOME/idmtools/bin/` directory. The `preConfigIDStore` option extends the schema in OUD or OID, adding object classes required by the integration. It also creates a number of users and groups. Based on the information you provide in the configuration file, this command will act on the appropriate identity store. For example:

```
./idmConfigTool.sh -preConfigIDStore input_file=/scratch/fwadmin/ldap_scripts/prepareIDStore.properties
```

Note: On a replicated OUD instance, `cn=changelog` is available by default depending on the condition that this instance contains both directory server and replication server components, which is the default. The changelog has no additional cost since the replication is already up.

On a non replicated OUD instance, `cn=changelog` is not available by default because there is a cost in disk and cpu that should not be paid if it is not useful. This can be easily enabled with the following command:

```
$ dsreplication enable-changelog -h localhost -p 4444 -D  
"cn=directory manager" \  
-j pwd-file -r 8989 -b dc=example,dc=com -X -n
```

In an Oracle Identity Manager deployment that is integrated with Access Manager, it is a requirement that the changelog is enabled for Oracle Identity Manager LDAP synchronization with OUD to work.

See [Section E.1.2, "Configuring Changelog in OUD"](#) for more information about enabling the external change log.

Here, `prepareIDStore.properties` file is the configuration file with the following input parameters with sample values:

```
- IDSTORE_HOST: HOST_NAME
```


- IDSTORE_PORT: *PORT*
- IDSTORE_BINDDN: cn=oudadmin
- IDSTORE_USERNAMEATTRIBUTE: cn
- IDSTORE_LOGINATTRIBUTE: uid
- IDSTORE_USERSEARCHBASE: cn=Users,dc=us,dc=example,dc=com
- IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=us,dc=example,dc=com
- IDSTORE_SEARCHBASE: dc=us,dc=example,dc=com
- IDSTORE_SYSTEMIDBASE: cn=Systemids,dc=us,dc=example,dc=com

If you are using OUD as the identity store, then the additional properties are:

- IDSTORE_ADMIN_PORT : 4444
- IDSTORE_KEYSTORE_FILE :
/u01/config/instances/oud1/OU/OU/config/admin-keystore
- IDSTORE_KEYSTORE_PASSWORD : Abcd1234

The value of the IDSTORE_KEYSTORE_PASSWORD parameter is the content of the /u01/config/instances/oud1/OU/OU/config/admin-keystore.pin file.

The idmConfigTool can then be run with the following command:

```
idmConfigTool.sh -prepareIDStore mode=OIM input_file=configfile
```

For OID and OUD, to perform additional schema extensions and create additional users and groups, the following is a sample property file:

```
IDSTORE_HOST : idstore.example.com
IDSTORE_PORT : 389
IDSTORE_BINDDN : cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE:cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_OIMADMINUSER: oimadmin
IDSTORE_OIMADMINGROUP:OIMAdministrators
```

If you are using OUD as the identity store, then the additional properties are:

```
IDSTORE_ADMIN_PORT : 4444
IDSTORE_KEYSTORE_FILE : /u01/config/instances/oud1/OU/OU/config/admin-keystore
IDSTORE_KEYSTORE_PASSWORD : Abcd1234
```

See [Appendix D, "Using the idmConfigTool Command"](#) for more information about using the idmConfigTool utility.

Note: For information about errors that might occur when synchronizing with OUD and workaround steps, see [Section E.2.14, "Fixing Permission Errors with OUD ACIs"](#).

- **Preconfiguring ODSEE and AD:** If Oracle Directory Server (ODSEE) or Active Directory (AD) is used, then do not use the idmConfigTool utility. Instead, manual steps must be followed, as described in subsequent sections in this document.

The following sections describe how to preconfigure the Identity Store for Active Directory and ODSEE:

- [Preconfiguring Active Directory](#)
- [Preconfiguring ODSEE](#)

E.1.1.1 Preconfiguring Active Directory

Before you can use your LDAP directory as an identity store, you must preconfigure it. The procedure in this section enables you to preconfigure Microsoft Active Directory for using it as your LDAP identity store.

Note: The data used in the examples provided below is sample data. Follow the examples and replace them with appropriate data according to your LDAP server configuration.

To preconfigure the identity store:

1. Create User, Group, and Reserve Container, as shown:

```
dn:cn=Reserve,dc=example,dc=com
cn:Reserve
objectclass:top
```

```
dn:cn=Groups,dc=example,dc=com
cn:Groups
objectclass:top
```

```
dn:cn:Users,dc=example,dc=com
cn:Users
objectclass:top
```

2. In Active Directory, create a container outside the search base to be used for Oracle Identity Manager reconciliation. This will avoid administrative users being reconciled into Oracle Identity Manager. For example:

```
dn:cn=systemids,dc=example,dc=com
cn:systemids
objectClass:top
```

3. Create the administrative user for Oracle Identity Manager inside this container:

```
dn:cn=oimadmin,cn=systmids,dc=example,dc=com
cn:oimadmin
objectclass:user
```

4. In the Users container created in step 1, create the system administrator user, with uid: `SYSTEM_ADMINISTRATOR` and an appropriate password.
5. In the Groups container created in step 1, create a group Oim Administrators, and then assign the users `oimadmin` and `SYSTEM_ADMINISTRATOR` to this group.
6. In the container created in step 2, create a user `oamadmin` with a password, such as `welcome11gR2`.
7. In the Groups container created in step 1, create a group `OAM Administrators` and assign the `oamadmin` user to the group.
8. In the Users container created in step 1, create a user for WebLogic administration with ID as `WLAdmin` and password as `welcome11gR2`.

9. In the Groups container created in step 1, create a group `WLSAdmins`, and assign the `WLSAdmin` user to that group.

10. Add ACLs that need to be setup:

OIM Administrators group - complete read/write privileges to all the user and group entities in the directory. This group needs read/write privileges for the Reserve container also.

11. Extend the OAM schema, as follows:

Navigate to the `IAM_ORACLE_HOME/oam/server/oim-intg/ldif/ad/schema` directory, and locate the following files:

- `ADUserSchema.ldif`
- `AD_oam_pwd_schema_add.ldif`

In the above LDIF files, replace the domain-dn with the appropriate domain-dn value.

Use `ldapadd` from the command line to load the two LDIF files, as follows:

a. Navigate to the following directory:

```
cd IAM_ORACLE_HOME/oam/server/oim-intg/ldif/ad/schema/
```

b. Run the `ldapadd` command.

```
ldapadd -h <activedirectoryhostname> -p <activedirectoryportnumber> -D <AD_
administrator> -q -c -f ADUserSchema.ldif
```

```
ldapadd -h <activedirectoryhostname> -p <activedirectoryportnumber> -D <AD_
administrator> -q -c -f AD_oam_pwd_schema.ldif
```

Here, `AD_administrator` is the user with schema extension privileges to the directory. For example:

```
ldapadd -h activedirectoryhost.mycompany.com -p 389 -D adminuser -q -c -f
ADUserSchema.ldif
```

12. Extend the OIM Schema for Active Directory by using the `extendadschema` script.

The `extendadschema` script and the OIM Schema for Active Directory is located at:

```
MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/oimtemplates
```

This directory contains the following files used by `extendadschema` for extending Active Directory:

- `adOAMDisable.ldif`
- `adOAMEnable.ldif`
- `adOIMLanguageSubtype.ldif`
- `adOIMSchema.ldif`

Run the following command to extend Active Directory schema:

On Windows:

```
extendadschema.bat -h AD_host -p AD_port -D <administrator@mydomain.com> -AD
<dc=mydomain,dc=com> -OAM <true/false>
```

On UNIX:

```
extendadschema.sh -h AD_host -p AD_port -D <administrator@mydomain.com> -AD
```

```
<dc=mydomain,dc=com> -OAM <true/false>
```

Specify the value of `-OAM` parameter as `true`.

Note: The `extendadschema` script is certified only on Active Directory 2003, 2008, 2008R2, and 2012.

13. Set Active Directory password policy. To do so:

- a. Verify that the value of the `pwdMaxFailure` configuration parameter for the `libOVD` adapter in the `DOMAIN_HOME/config/fmwconfig/ovd/oim/adapters.os_xml` file is set to 10.
- b. Set the `lockoutThreshold` value to 10 in Active Directory. For information about `lockoutThreshold`, refer to the following URL:

<https://technet.microsoft.com/en-us/library/cc775412%28v=ws.10%29.aspx>

E.1.1.2 Preconfiguring ODSEE

Before you can use your LDAP directory as an Identity store, you must preconfigure it. The procedure in this section enables you to preconfigure Oracle Directory Server Enterprise Edition (ODSEE) for using Oracle Directory Server Enterprise Edition (ODSEE) as your LDAP Identity store if you are integrating with OAM, and therefore, configuring LDAP Synchronization.

Note:

- If your LDAP identity store (OIM) has been configured for the containers and `oimadminuser` with the schema extension, then you need not follow the configuration steps described in this section.
 - `cn=oracleAccounts` is sample data. Follow the examples and replace them with appropriate data as per your LDAP server configuration.
 - `cn=oracleAccounts` is sample data suggesting a name for a directory container meant for containing information to be synchronized with OIM. It is not mandatory to use this data when you preconfigure the identity store.
-
-

To preconfigure the identity store:

1. Create a new file `iPlanetContainers.ldif`. Add the following entries and save the file.

```
dn:cn=oracleAccounts,dc=mycompany,dc=com
cn:oracleAccounts
objectClass:nsContainer
```

```
dn:cn=Users,cn=oracleAccounts,dc=mycompany,dc=com
cn:Users
objectClass:nsContainer
```

```
dn:cn=Groups,cn=oracleAccounts,dc=mycompany,dc=com
cn:Groups
```

```
objectClass:nsContainer

dn:cn=Reserve,cn=oracleAccounts,dc=mycompany,dc=com
cn:Reserve
objectClass:nsContainer
```

2. Import the containers into iPlanet Directory Server with `ldapadd` command. This will create the user, group and reserve containers.

```
ldapadd -h <ODSEE Server> -p <ODSEE port> -D <ODSEE Admin ID> -w <ODSEE Admin password> -c -f ./iPlanetContainers.ldif
```

For example:

```
ldapadd -h localhost -p 1389 -D "cn=Directory Manager" -w "welcome1" -c -f ./iPlanetContainers.ldif
```

If the above gives authentication error, try the command with '-x' option with simple bind option.

```
ldapadd -h localhost -p 1389 -x -D "cn=Directory Manager" -w "welcome1" -c -f ./iPlanetContainers.ldif
```

3. Enable the `moddn` property for the rename of entries to happen between nodes.

```
..dsee7/bin/dsconf set-server-prop -h <ODSEE Server> -p <ODSEE port>
moddn-enabled:on
```

For example:

```
..dsee7/bin/dsconf set-server-prop -h localhost -p 1389 moddn-enabled:on
```

4. Enable `changelog`.

```
..dsee7/bin/dsconf set-server-prop -h <ODSEE Server> -p <ODSEE port>
retro-cl-enabled:on
```

For example:

```
..dsee7/bin/dsconf set-server-prop -h localhost -p 1389 retro-cl-enabled:on
```

5. Check the status, as shown:

```
..dsee7/bin/dsccsetup status
```

6. Stop and Start the ODSEE server instance.

```
..dsee7/bin/dsadm stop <ODSEE instance>
..dsee7/bin/dsadm start <ODSEE instance>
```

For example:

```
..dsee7/bin/dsadm stop /scratch/<userid>/iPlanet/dsinst1/
..dsee7/bin/dsadm start /scratch/<userid>/iPlanet/dsinst1/
```

7. Extend the Sun schema to include OIM-specific Object Classes and Attribute Types.

```
cd to $MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/oimtemplates
```

Run the following command to load the ldif file, `sunOneSchema.ldif`.

```
ldapmodify -h <ODSEE Server> -p <ODSEE port> -D <ODSEE Admin ID> -w <ODSEE Admin password> -f sunOneSchema.ldif
```

For example:

```
./ldapmodify -h localhost -p 1389 -D "cn=directory manager" -w welcome1 -c -f
sunOneSchema.ldif
```

8. If you want to enable OAM-OIM integration, then extend the following OAM schema:

For ODSEE/iPlanet, to extend OAM Schema for ODSEE, locate the following files:

Note: If you are not sure about the which index-root you should use, instead of iPlanet7_user_index_add.ldif, use iPlanet7_user_index_generic.ldif file, which also has step by step instructions on finding index-root.

Use ldapmodify from the command line to load the four LDIF files:

```
cd $IAM_HOME/oam/server/oim-intg/ldif/iplanet/schema/
ldapadd -h <ODSEE_server> -p <ODSEE_port> -D <ODSEE_admin_ID> -w <ODSEE_admin_
password> -f iPlanet7_user_index_add.ldif
```

Or:

```
ldapadd -h <ODSEE_Server> -p <ODSEE_port> -D <ODSEE_admin_ID> -w <ODSEE_admin_
password> -f iPlanet7_user_index_generic.ldif
ldapmodify -h <ODSEE_server> -p <ODSEE_port> -D <ODSEE_admin_ID> -w <ODSEE_
admin_password> -f iPlanet_oam_pwd_schema_add.ldif
ldapmodify -h <ODSEE_server> -p <ODSEE_port> -D <ODSEE_admin_ID> -w <ODSEE_
admin_password> -f iPlanet_user_schema_add.ldif
ldapadd -h <ODSEE_server> -p <ODSEE_port> -D <ODSEE_admin_ID> -w <ODSEE_admin_
password> -f iPlanet_user_index_add.ldif
```

9. Enable Referential Integrity for OIM's Common Name Generation feature.

Anytime the DN or RDN is being modified, then the Referential Integrity needs to be enabled in OIM and OID/Active Directory/ODSEE.

If Referential Integrity is enabled in the Directory Server, then customers need to set the OIM property `XL.IsReferentialIntegrityEnabledInLDAP` to TRUE as by default it is set to FALSE. To set `XL.IsReferentialIntegrityEnabledInLDAP` to TRUE, log into OIM and go to **Advanced, System Management, System Configuration**. Search for System Properties (`XL.IsReferentialIntegrityEnabled`), and set the property value to TRUE.

- a. Use the following command to see the value of the referential integrity property.

```
..dsee7/bin/dsconf get-server-prop -h <ODSEE server> -p <ODSEE port>
ref-integrity-enabled
Enter "cn=Directory Manager" password:
ref-integrity-enabled : off
```

- b. Use the following commands to enable the referential integrity property.

```
./dsconf set-server-prop -h <ODSEE server> -p <ODSEE port>
ref-integrity-enabled:on
Enter "cn=Directory Manager" password:
```

Directory Server must be restarted for changes to take effect. Restart ODSEE/iPlanet Server after enabling referential integrity property.

```
..dsee7/bin/dsadm stop <ODSEE instance>
..dsee7/bin/dsadm start <ODSEE instance>
```

For example:

```
..dsee7/bin/dsadm stop /scratch/<userid>/iPlanet/dsinst1/
..dsee7/bin/dsadm start /scratch/<userid>/iPlanet/dsinst1/
```

- c.** Now query to see if the value has been set correctly.

```
..dsee7/bin/dsconf get-server-prop -h <ODSEE server> -p <ODSEE port>
ref-integrity-enabled
Enter "cn=Directory Manager" password:
ref-integrity-enabled : on
```

- 10.** Create the OIM Admin User, Group and the ACIs. Open a new file `oimadminuser.ldif`. This `oimadminuser` will be used as a proxy user for OIM.

The root suffix is given as `dc=mycompany,dc=com`. This must be replaced with the appropriate root suffix of the ODSEE server.

- a.** Add the following LDAP entries and save the file `oimadminuser.ldif`. Run the following command to load the ldif file, `oimadminuser.ldif`.

```
ldapmodify -h <ODSEE Server> -p <ODSEE port> -D <ODSEE Admin ID> -w <ODSEE
Admin password> -f oimadminuser.ldif
```

```
dn: cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: nsContainer
objectclass: top
cn: systemids
```

```
dn: cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
mail: oimAdminUser
givenname: oimAdminUser
sn: oimAdminUser
cn: oimAdminUser
uid: oimAdminUser
userPassword: welcome1
```

```
dn: cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: groupOfUniqueNames
objectclass: top
cn: oimAdminGroup
description: OIM administrator role
uniquemember: cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com
```

```
dn: cn=users,cn=oracleAccounts,dc=mycompany,dc=com
changetype: modify
add: aci
aci: (target =
"ldap:///cn=users,cn=oracleAccounts,dc=mycompany,dc=com") (targetattr =
"*)(version 3.0; acl "Allow OIMAdminGroup add, read and write access to
all attributes"; allow (add, read, search, compare,write, delete, import)
(groupdn = "ldap:///cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com");)
```

```

dn: cn=Groups,cn=oracleAccounts,dc=mycompany,dc=com
changetype: modify
add: aci
aci: (target =
"ldap:///cn=Groups,cn=oracleAccounts,dc=mycompany,dc=com")(targetattr =
"*)(version 3.0; acl "Allow OIM AdminGroup to read and write access";
allow (read, search, compare, add, write,delete) (groupdn =
"ldap:///cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com");)

dn: cn=reserve,cn=oracleAccounts,dc=mycompany,dc=com
changetype: modify
add: aci
aci: (target =
"ldap:///cn=reserve,cn=oracleAccounts,dc=mycompany,dc=com")(targetattr =
"*)(version 3.0; acl "Allow OIM AdminGroup to read and write access";
allow (read, search, compare, add, write,delete,export) (groupdn =
"ldap:///cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com");)

dn: cn=changelog
changetype: modify
add: aci
aci: (target = "ldap:///cn=changelog")(targetattr = "*)(version 3.0; acl
"Allow OIM AdminGroup to read and write access"; allow (read, search,
compare, add, write,delete,export) (groupdn =
"ldap:///cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com");)

```

b. Use the following commands to check for the entries and ACI in the LDAP:

```

ldapsearch -h <ODSEE Server> -p <ODSEE Port> -x -D "cn=Directory Manager"
-w <ODSEE Admin Password> -b "cn=changelog" -s sub "objectclass=*" aci

ldapsearch -h <ODSEE Server> -p <ODSEE Port> -x -D "cn=Directory Manager"
-w <ODSEE Admin Password> -b
"cn=users,cn=oracleAccounts,dc=mycompany,dc=com" -s sub
"objectclass=*" aci

ldapsearch -h <ODSEE Server> -p <ODSEE Port> -x -D "cn=Directory Manager"
-w <ODSEE Admin Password> -b
"cn=groups,cn=oracleAccounts,dc=mycompany,dc=com" -s sub
"objectclass=*" aci

ldapsearch -h <ODSEE Server> -p <ODSEE Port> -x -D "cn=Directory Manager"
-w <ODSEE Admin Password> -b
"cn=reserve,cn=oracleAccounts,dc=mycompany,dc=com" -s sub
"objectclass=*" aci

```

E.1.2 Configuring Changelog in OUD

LDAP synchronization requires the creation in LDAP of a proxy user and group, different from the LDAP administrative user. This is done to permit Oracle Identity Manager to update LDAP's directory store. Without those updates being reconciled back to Oracle Identity Manager, the changes are made as the proxy user, and changes made by the proxy user are filtered out by Oracle Identity Manager during reconciliation.

Using LDAP synchronization with OUD has some additional requirements. OUD's External Changelog (ECL) must be enabled, and the proxy user must be given permissions to query it. To do so:

Note: The examples in this section assume an OUD instance on localhost, and a simple bind password stored in a secure file (PASSWORD_FILE). Modify the commands as required for your local environment.

1. After OUD has been installed, modify its configuration file to change the global ACIs for the proxy user and group for changelog access. To do so, in the *MIDDLEWARE_HOME/Oracle_OUD1/asinst_1/OUd/config/config.ldif* file, replace the default:

```
ds-cfg-global-aci: (target="ldap:///cn=changelog") (targetattr="*") (version 3.0;
acl "External changelog access"; deny (all) userdn="ldap:///anyone");
```

With the following:

```
ds-cfg-global-aci: (target="ldap:///cn=changelog") (targetattr="*") (version 3.0;
acl "External changelog access"; deny (all)
userdn!="ldap:///cn=oimAdminUser,cn=systemids,dc=us,dc=mydomain,dc=com");)
```

```
ds-cfg-global-aci: (target="ldap:///cn=changelog") (targetattr="*") (version 3.0;
acl "External changelog access"; allow
(read,search,compare,add,write,delete,export)
groupdn="ldap:///cn=oimAdminGroup,cn=systemids,dc=us,dc=mydomain,dc=com");)
```

Note:

- The proxy user and group do not have to be created at this point.
 - OUD must be restarted for these changes to take effect. Use the `stop-ds` and `start-ds` commands in the OUD bin directory.
-
-

2. From the OUD bin directory, create the proxy user and group by using the `oudadmin.ldif` file:

```
./ldapmodify -h localhost -p PORT -D cn=orcladmin -j PASSWORD_FILE -c -f FILE_
LOCATION/oudadmin.ldif
```

3. Create the replication server and domain. Set the replication port number and the base-dn (for example, `dc=com`) appropriately for your installation, as shown:

```
./dsconfig -h localhost -p ADMIN_PORT -D cn=orcladmin -j PASSWORD_FILE -X -n
create-replication-server --provider-name 'Multimaster Synchronization' --set
replication-port:PORT --set replication-server-id:1 --type generic
```

```
./dsconfig -h localhost -p ADMIN_PORT -D cn=orcladmin -j PASSWORD_FILE -X -n
create-replication-domain --provider-name 'Multimaster Synchronization' --set
base-dn:dc=com --set replication-server:localhost:PORT --set server-id:1 --type
generic --domain-name dc=com
```

4. Provide access to the ECL control, as shown:

```
./dsconfig -h localhost -p ADMIN_PORT -D cn=orcladmin -X -j PASSWORD_FILE -n
set-access-control-handler-prop --add
global-aci:\(targetcontrol="\1.3.6.1.4.1.26027.2.3.4"\)\(version\ 3.0\;\ acl\
\"Authenticated\ users\ control\ access\";\ allow\ (read)\
userdn="ldap:///all\";\)
```

5. Confirm that the proxy user has access to the changelog, both at the command line and by a manual test within Oracle Identity Manager, as follows:

- **Command line test:** Ensure that the results of the following commands are identical:

```
ldapsearch -h localhost -p PORT -D OIM_PROXY_USER -j PASSWORD_FILE -b "cn=changelog" -s one
```

```
ldapsearch -h localhost -p PORT -D OUD_ADMIN_USER -j PASSWORD_FILE -b "cn=changelog" -s one
```

Here, *OIM_PROXY_USER* is the proxy user created previously (for example, *cn=oimAdminUser,cn=systemids,...*), and *OUD_ADMIN_USER* is the administrator created when installing OUD (for example, *cn=orcladmin*).

- **OIM test:** It is necessary to obtain the last changelog number from OUD in order to run incremental reconciliation. To do so:
 - a. Create a user and/or role in Oracle Identity Manager.
 - b. Verify that the user and/or role has been successfully synced to LDAP.
 - c. Modify a harmless attribute, such as the display name, for the user and/or role in LDAP.
 - d. Making sure that the last changelog is correctly initialized in the incremental recon scheduled task UI, run incremental user (or role) create/modify, and verify that the entity changes are reflected in Oracle Identity Manager.

The global ACIs can be investigated directly from OUD by the following:

```
./dsconfig -h localhost -p ADMIN_PORT -D cn=orcladmin -X -j PASSWORD_FILE -n get-access-control-handler-prop --property global-aci
```

6. Get the last changelog from OUD.

OUD uses the external changelog (ECL) for its changelog numbers. This is not numeric, but instead in a format beginning with the base name. The command to get the ECL is:

```
ldapsearch -h localhost -p PORT -D "cn=orclAdmin" -j PASSWORD_FILE -b "" -s base "objectclass=*" lastExternalChangelogCookie
```

An example command and sample ECL follows. Copy your changelog string beginning with the basename. Usually the string has a space and/or carriage return before the end. Be sure to copy the entire string, but eliminating the string and CR.

```
ldapsearch -h localhost -p PORT -D "cn=orclAdmin" -j PASSWORD_FILE -b "" -s base "objectclass=*" lastExternalChangelogCookie
```

```
dn:
lastExternalChangelogCookie: dc=com:00000154c04613df0001000000
1b;
```

In order to use this in Oracle Identity Manager, remove the <CR>/space, if it exists, such as:

```
dc=com:00000154c04613df00010000001b
```

For test purposes, you may need to set the changelog back a few entries to get changes made before obtaining the ECL:

```
dc=us,dc=mydomain,dc=com:00000154c04613df000100000010
```

E.1.3 Creating OVD Adapters

Enabling LDAP synchronization at install time also configures the libOVD or OVD adapters required for integration. In the event that LDAP synchronization is enabled after the initial Oracle Identity Manager installation, it you must manually configure the libOVD or OVD adapters.

To enable LDAP synchronization with libOVD, see [Section E.1.3.2, "Creating Identity Virtualization Library \(libOVD\) Adapters and Integrating With Oracle Identity Manager"](#) and [Section E.2.10, "Managing Identity Virtualization Library \(libOVD\) Adapters"](#).

Alternately, if you have configured a standalone OVD server, then the IT Resource page for the Directory Server IT resource type must be configured with the OVD server details. See [Section E.1.4.2, "Modifying the IT Resource"](#). In addition, you must create the OVD adapters for various LDAP servers. For details, see "Creating Adapters in Oracle Virtual Directory" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

If you are configuring OVD for integration with Oracle Identity Manager, then refer to the following topics:

- [Section E.1.3.1, "Creating Oracle Virtual Directory Adapters for Oracle Internet Directory and Active Directory"](#)
- [Section E.1.3.2, "Creating Identity Virtualization Library \(libOVD\) Adapters and Integrating With Oracle Identity Manager"](#)

E.1.3.1 Creating Oracle Virtual Directory Adapters for Oracle Internet Directory and Active Directory

You can use the UserManagement plug-in to create the Oracle Virtual Directory User and Changelog adapters for Oracle Internet Directory and Active Directory. Oracle Identity Manager requires adapters. It is highly recommended, though not mandatory, that you use Oracle Virtual Directory to connect to Oracle Internet Directory.

To do this, perform the following tasks:

1. Ensure you have set all of the necessary environment variables as described in [Section D.2, "Set Up Environment Variables"](#).
2. Create a properties file for the Oracle Internet Directory adapter called `ovd1.props` as follows:

Note: The `usecase.type:single` parameter is not supported for Active Directory via the `configOVD` option.

```
ovd.host:ovdhost1.mycompany.com
ovd.port:8899
ovd.binddn:cn=orcladmin
ovd.password:ovdpassword
ovd.oamenabled:true
ovd.ssl:true
ldap1.type:OID
```

```

ldap1.host:oididstore.myhost.mycompany.com
ldap1.port:3060
ldap1.binddn:cn=orcladmin,cn=systemids,dc=mycompany,dc=com
ldap1.password:oidpassword
ldap1.ssl:false
ldap1.base:dc=mycompany,dc=com
ldap1.ovd.base:dc=mycompany,dc=com
usecase.type: single
    
```

The following table describes the parameters used in the properties file.

Parameter	Description
ovd.host	Host name of a server running Oracle Virtual Directory.
ovd.port	The https port used to access Oracle Virtual Directory.
ovd.binddn	User DN used to connect to Oracle Virtual Directory.
ovd.password	Password for the DN used to connect to Oracle Virtual Directory.
ovd.oamenabled	Always true in <ul style="list-style-type: none"> ■ Fusion Applications deployments. ■ Deployments that involve integration between Oracle Identity Manager and Oracle Access Manager. For example, when the underlying Directory server is also used by Oracle Access Manager for authentication purposes.
ovd.ssl	Set to true, as you are using an https port.
ldap1.type	Set to OID for the Oracle Internet Directory back end directory or set to AD for the Active Directory back end directory.
ldap1.host	Host on which back end directory is located. Use the load balancer name.
ldap1.port	Port used to communicate with the back end directory.
ldap1.binddn	Bind DN of the oimLDAP user.
ldap1.password	Password of the oimLDAP user.
ldap1.ssl	Set to true if you are using the back end's SSL connection, and otherwise set to false. Always set this parameter to true when creating an adapter for AD.
ldap1.base	Base location in the directory tree.
ldap1.ovd.base	Mapped location in Oracle Virtual Directory.
usecase.type	Set to Single when using a single directory type.

3. Configure the adapter by using the `idmConfigTool` command, which is located at:

```
IAM_ORACLE_HOME/idmtools/bin
```

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

```
IAM_ORACLE_HOME/idmtools/bin
```

The syntax of the command on Linux is:

```
idmConfigTool.sh -configOVD input_file=configfile [log_file=logfile]
```

The syntax on Windows is:

```
idmConfigTool.bat -configOVD input_file=configfile [log_file=logfile]
```

For example:

```
idmConfigTool.sh -configOVD input_file=ovd1.props
```

The command requires no input. The output looks like this:

```
The tool has completed its operation. Details have been logged to logfile
```

Run this command for each Oracle Virtual Directory instance in your topology, with the appropriate value for `ovd.host` in the property file.

E.1.3.2 Creating Identity Virtualization Library (libOVD) Adapters and Integrating With Oracle Identity Manager

You can configure Identity Virtualization Library (libOVD) adapters by using script and template files related to libOVD. [Table E-1](#) lists the files used for Identity Virtualization Library (libOVD) adapter configuration.

Table E-1 Identity Virtualization Library (libOVD) Adapter Configuration Files

File	Description
Files in the <code>\$MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/</code> directory	Files related to Identity Virtualization Library (libOVD)
Files in the <code>\$MW_HOME/oracle_common/bin/</code> directory: <code>libovdadapterconfig.sh</code> <code>libovdconfig.sh</code> <code>libovdadapterconfig.bat</code> <code>libovdconfig.bat</code>	Script files to configure Identity Virtualization Library (libOVD)
Files in the <code>\$MW_HOME/Oracle_IDM/libovd/</code> directory: <code>adapter_template_oim_ldap.xml</code> <code>adapter_template_oim.xml</code>	Template files to configure Identity Virtualization Library (libOVD)
Files in the <code>\$MW_HOME/user_projects/domains/DOMAIN_NAME/config/fmwconfig/ovd/ADAPTER_NAME/</code> directory: <code>adapters.os_xml</code> By default, the value of <code>ADAPTER_NAME</code> is <code>oim</code> .	Configuration file after Identity Virtualization Library (libOVD) has been configured

To configure Identity Virtualization Library (libOVD) adapters and integrate with Oracle Identity Manager:

- Before running the scripts to configure Identity Virtualization Library (libOVD), set the following environment variables:
 - set `MW_HOME` to the appropriate Middleware home directory
 - set `ORACLE_HOME` to `$MW_HOME/oracle_common`

- set WL_HOME to \$MW_HOME/wlserver_10.3
 - set JAVA_HOME to the appropriate jdk path
2. To configure Identity Virtualization Library (libOVD):

Note: Substitute the appropriate information of your host computer and directory path in the commands to run the scripts for configuring Identity Virtualization Library (libOVD).

- a. To create libOVD configuration files and lay out the directory structure, run the following command:

```
sh $MW_HOME/oracle_common/bin/libovdconfig.sh -domainPath FULL_PATH_OF_
DOMAIN -contextName oim -host ADMIN_SERVER_HOST -port ADMIN_SERVER_PORT
-userName ADMIN_SERVER_USERNAME
```

For example:

```
sh $MW_HOME/oracle_common/bin/libovdconfig.sh -domainPath $MW_HOME/user_
projects/domains/base_domain -contextName oim -host myhost.mycompany.com
-port 7001 -userName weblogic
```

This command creates the directory structure containing the OVD configuration files for Oracle Identity Manager and copies the configuration file templates. In the example, the contextName is assumed to be oim, and therefore, the OVD configuration files are created in the *DOMAIN_HOME/config/fmwconfig/ovd/oim/* directory. Here, *DOMAIN_HOME* is the directory that you are using as the home directory for your domain.

Note: Because Identity Virtualization Library (libOVD) is included in Oracle Identity Manager, both are deployed on the same web container. Therefore, the Admin Server host and Admin Server port must be of the same computer on which Oracle Identity Manager is installed, and not of the computer on which LDAP is installed.

Running the command displays the following. Enter the password when prompted.

```
Enter AdminServer Password:
Successfully created OVD config files
CSF Credential creation successful
Permission Grant successful
Successfully configured OVD MBeans
```

- b. To create user and changelog adapters, run the following command:

```
sh $MW_HOME/oracle_common/bin/libovdadapterconfig.sh -domainPath FULL_PATH_
OF_DOMAIN -contextName oim -host ADMIN_SERVER_HOST -port ADMIN_SERVER_PORT
-userName ADMIN_SERVER_USERNAME -adapterName ADAPTER_NAME -adapterTemplate
$MW_HOME/Oracle_IDM1/libovd/adapter_template_oim.xml -bindDN LDAP_BIND_DN
-createChangelogAdapter -dataStore LDAP_DIRECTORY_TYPE -ldapHost LDAP_HOST
-ldapPort LDAP_PORT -remoteBase REMOTE_BASE -root VIRTUAL_BASE
```

Here, template is oim template. This creates the adapters with the information you provide when running this script, based on the Oracle Identity Manager template. In the command examples shown in this step, contextName is

assumed to be oim. In addition, the `bindDN` parameter must contain the same DN of the Oracle Identity Manager administrator account created during the LDAP preconfiguration step. In other words, if during LDAP preconfiguration, the `cn=oimAdminUser, cn=systemids, dc=mycompany, dc=com` account has been created, then the `bindDN` must be set to `cn=oimAdminUser, cn=systemids, dc=mycompany, dc=com`.

Note:

- Because Identity Virtualization Library (libOVD) is included in Oracle Identity Manager, both are deployed on the same web container. Therefore, the Admin Server host and Admin Server port must be on the same computer on which Oracle Identity Manager is installed, and not of the computer on which LDAP server is installed.
 - In the parameters that you pass while running the tool, value for the `-dataStore` argument must be the backend directory type. Valid values for this parameter, when using the `adapter_template_oim.xml`, are `OID`, `ACTIVE_DIRECTORY`, `IPLANET`, and `ODU`.
-
-

If the backend LDAP server port is configured over SSL, then Oracle Identity Manager user must use `keytool` to import the trusted certificate from the LDAP server into Identity Virtualization Library (libOVD) keystore. To do so, refer to ["Enabling SSL Between Identity Virtualization Library \(libOVD\) and the Directory Server"](#) on page E-38.

Example with non-SSL LDAP server port:

```
sh $MW_HOME/oracle_common/bin/libovdadapterconfig.sh -domainPath $MW_HOME/user_projects/domains/base_domain -contextName oim -host myadminserver.mycompany.com -port 7001 -userName weblogic -adapterName LDAP1 -adapterTemplate adapter_template_oim.xml -bindDN "cn=orcladmin" -createChangelogAdapter -dataStore OID -ldapHost myldaphost.mycompany.com -ldapPort 3060 -remoteBase "dc=us,dc=oracle,dc=com" -root "dc=us,dc=oracle,dc=com"
```

Enter AdminServer Password:

Enter LDAP Server Password:

Example with LDAP server port configured over SSL:

Note: If you are using SSL port for the LDAP port, then provide the `-enableSSL` parameter in the `libovdadapterconfig.sh` or `libovdadapterconfig.bat` command.

```
sh $MW_HOME/oracle_common/bin/libovdadapterconfig.sh -domainPath $MW_HOME/user_projects/domains/base_domain -contextName oim -host myadminserver.mycompany.com -port 7001 -userName weblogic -adapterName LDAP1 -adapterTemplate adapter_template_oim.xml -bindDN "cn=orcladmin" -createChangelogAdapter -dataStore OID -ldapHost myldaphost.mycompany.com -ldapPort 3161 -enableSSL -remoteBase "dc=us,dc=oracle,dc=com" -root "dc=us,dc=oracle,dc=com"
```

Enter AdminServer Password:

Enter LDAP Server Password:

3. Restart the web container and Oracle Identity Manager by running the following commands:

```
cd $MW_HOME/user_projects/domains/DOMAIN_NAME/bin/
```

```
./stopManagedWebLogic.sh oim_server1
```

```
./stopWebLogic.sh
```

```
./startWebLogic.sh
```

```
./startManagedWebLogic.sh oim_server1
```

4. To integrate Oracle Identity Manager to Oracle Identity Virtualization (libOVD):
 - a. Login to Oracle Identity System Administration.
 - b. Under Configuration on the left pane, click **IT Resource**. The Manage IT Resource page is displayed in a separate window.
 - c. From the IT Resource Type list, select **Directory Server**, and then click **Search**.
 - d. For the Directory Server IT resource, click **Edit**. The Edit IT Resource Details and Parameters page is displayed.
 - e. In the Search Base field, enter a value, for example, `dc=oracle,dc=com`.
 - f. In the User Reservation Container field, enter a value, for example, `cn=reserve,dc=us,dc=oracle,dc=com`.
 - g. Restart the WebLogic server on which Oracle Identity Manager is deployed.
 - h. Try accessing the server and manage users and roles through the Oracle Identity System Administration.
 - i. Connect directly to the LDAP server by using the `ldapclient` tool to verify that the data is managed in the LDAP server you chose with the `-dataStore` option to the `libovdadapterconfig.sh` command.

E.1.4 Enabling LDAP Synchronization

Enabling LDAP synchronization involves the following:

- [Section E.1.4.1, "Modifying the MDS"](#)
- [Section E.1.4.2, "Modifying the IT Resource"](#)
- [Section E.1.4.3, "Seeding Reconciliation Jobs"](#)
- [Section E.1.4.4, "Reverting from OVD to libOVD in LDAPSvc"](#)

E.1.4.1 Modifying the MDS

By default, MDS does not contain files required for enabling LDAP synchronization. Therefore, several configuration files must be imported into MDS. Initially, the files are not present in MDS, but template versions can be found in the Oracle Identity Manager distribution. In some case, these files need to be edited before import to reflect your own customizations.

- The template versions of these files can be found in `$IAM_ORACLE_HOME/server/metadata/` directory.

- The User, Role, Role Hierarchy, and Role Membership files must be imported into MDS. If you are modifying these entities and relationships, for example, by adding UDFs, then you must create a backup of the original files before modification and import.
- In most new installations, you can import the event handlers to MDS without modifying them. Occasionally, you might modify the event handlers to customize OIM response to lifecycle events.
- The LDAPContainerRules must always be edited to allow synchronization in your environment.
- After customizations have been applied in your environment, you must first export the files from MDS in order to obtain the active versions, as the original template versions on the file system might be outdated.

To modify and import MDS files:

1. Set the `OIM_ORACLE_HOME` environment variable to the directory on which Oracle Identity Manager is deployed. The exact location depends on your installation. An example of this can be `/u01/Oracle/Middleware/IAM`.
2. Copy the following files from the MDS to a temporary staging directory, such as `/tmp`:

Note:

- The files must not be copied to the root directory (`/tmp`). Instead, maintain the structure listed in this step, for example, `/tmp/db/LDAPUser`. If the files are copied to the `/tmp` directory and imported to MDS, then Oracle Identity Manager will fail to run the reconciliation scheduled jobs.
- It is mandatory to create a separate staging directory. The `$OIM_ORACLE_HOME/server/metadata` directory cannot be used as the staging directory because it contains some other files. If these files are imported inadvertently, then it might corrupt the Oracle Identity Manager instance.

Here, `OIM_ORACLE_HOME` represents an environment variable that identifies the directory on which Oracle Identity Manager is installed. This variable is used for various Oracle Identity Manager scripts.

- The following metadata files used for configuring reconciliation profile and reconciliation horizontal table entity definition for LDAP user, role, role hierarchy, and role membership reconciliation:

`/db/LDAPUser`

`/db/LDAPRole`

`/db/LDAPRoleHierarchy`

`/db/LDAPRoleMembership`

`/db/LDAPContainerRules.xml`

`/db/RA_LDAPROLE.xml`

`/db/RA_LDAPROLEHIERARCHY.xml`

/db/RA_LDAPROLEMEMBERSHIP.xml
 /db/RA_LDAPUSER.xml
 /db/RA_MLS_LDAPROLE.xml
 /db/RA_MLS_LDAPUSER.xml

These files must be copied to a temporary location before importing, or you might corrupt your instance because oim-config.xml is also present in the same location.

- The LDAP event handlers. The predefined event handlers are in the /db/ldapMetadata/EventHandlers.xml file.
- The LDAPContainerRules.xml consisting of the container information for users and roles to be created.

Note: The LdapContainerRules.xml file can contain rules by using only those attributes that are mapped to the directory. A rule cannot be written by using attributes from foreign objects or attributes that are not part of the entity. This is true for both user and role entities. For example, Role Email cannot be used for rules for roles, and user's Organization Name cannot be used for user entity.

3. Edit the LDAPContainerRules.xml. To do so, open LDAPContainerRules.xml, and replace \$DefaultUserContainer\$ and \$DefaultRoleContainer\$ with appropriate user and role container values. For example, replace:
 - \$DefaultUserContainer\$ with a value reflecting your desired container structure, such as cn=Users, dc=us, dc=sample, dc=com
 - \$DefaultRoleContainer\$ with a value reflecting your desired container structure, such as cn=SomeSubContainer, cn=Groups, dc=us, dc=sample, dc=com
4. Perform the import by using Oracle Enterprise Manager. For information about importing metadata files from MDS, see "Migrating User Modifiable Metadata Files" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Note: Ensure that EventHandlers.xml is in the \$STAGING_DIR/db/ldapMetadata/ directory when importing into MDS.

After performing your customizations and imports, it is recommended to export the files from MDS to confirm the files are in the correct MDS location with the desired changes. The MDS documentation provides instructions for MDS export.

E.1.4.2 Modifying the IT Resource

Edit IT Resource configuration in Oracle Identity Manager. To do so:

1. Login to the Oracle Identity System Administration as the system administrator by navigating to the following URL:
 http://HOST_NAME:PORT/sysadmin
2. In the left navigation pane, under Configuration, click **IT Resource**. The Manage IT Resource page is displayed.
3. Search for the Directory Server IT resource.

4. Update the IT resource with Search base and Reservation container values.

The suggested value for Search base is the root suffix or the BaseDN, for example, `dc=us,dc=example,dc=com`.

5. If you want to configure Oracle Identity Manager with OVD server, then enter the values for ServerURL with the OVD server host and port details.

If you want to configure Oracle Identity Manager with Identity Virtualization Library (libOVD), then do not enter the values for ServerURL. It must be empty.

6. Enter the values for the bind credentials used for LDAP server. This is the same as used as the `IDSTORE_BINDDN` in the `idmConfigTool`.

Admin Login: `cn=oimadmin`

Admin Password: `1111111111`

7. Make sure that the value for the Reservation Container is `cn=reserve,VALUE_OF_THE_ROOT_SUFFIX`. For example:

Reservation Container: `cn=reserve,dc=us,dc=example,dc=com`

E.1.4.3 Seeding Reconciliation Jobs

For reconciliation jobs, seed the LDAP reconciliation scheduled jobs into Quartz tables, which are part of Oracle Identity Manager schema. As a prerequisite to do so, set the `OIM_ORACLE_HOME` environment variable. For example:

For Microsoft Windows, set the `OIM_ORACLE_HOME` environment variable to the `C:\Oracle\Middleware\Oracle_IDM1` directory by running the following command:

```
set OIM_ORACLE_HOME=C:\Oracle\Middleware\Oracle_IDM
```

For UNIX, run the following command:

```
setenv OIM_ORACLE_HOME /u01/mwhome/Oracle_IDM
```

Seeding the LDAP reconciliation scheduled jobs can be performed in any one of the following ways:

- **Seeding LDAP reconciliation scheduled jobs with parameters:**
 - a. Go to the `$OIM_ORACLE_HOME/server/setup/deploy-files` directory.
 - b. Set ant home. The following are sample commands to set ant home:

For UNIX:

```
setenv ANT_HOME /u01/mwhome/modules/org.apache.ant_1.7.1
```

For Microsoft Windows:

```
set ANT_HOME=/u01/mwhome/modules/org.apache.ant_1.7.1
```

Note: If ANT is not installed, then download ANT from Oracle Technology Network (OTN) web site by navigating to the following URL:

<http://www.oracle.com/technetwork/index.html>

Install ANT and set the `ANT_HOME`. Make sure that ant executable file exists in the `$ANT_HOME/bin/ant/` directory.

- c. Run the following ant command with parameters:

```
$ANT_HOME/bin/ant -f setup.xml seed-ldap-recon-jobs
-DoperationsDB.driver=oracle.jdbc.OracleDriver -DoperationsDB.user=SCHEMA_
OWNER_USERNAME -DOIM.DBPassword=SCHEMA_OWNER_PASSWORD
-DoperationsDB.host=SCHEMA_HOST_ADDRESS -DoperationsDB.port=SCHEMA_PORT_
NUMBER -DoperationsDB.serviceName=SCHEMA_SERVICE_NAME -Dssi.provisioning=ON
-Dweblogic.server.dir=WEBLOGIC_SERVER_LOCATION -Djdbc.location=OJDBC_
LOCATION -Dwork.dir=seed_logs
```

For example:

```
$ANT_HOME/bin/ant -f setup.xml seed-ldap-recon-jobs
-DoperationsDB.driver=oracle.jdbc.OracleDriver
-DoperationsDB.user=schemaowner1_OIM -DOIM.DBPassword=SCHEMA_OWNER_PASSWORD
-DoperationsDB.host=myhost.mycompany.com -DoperationsDB.port=1521
-DoperationsDB.serviceName=oimdb.regress.rdbms.mycompany.com
-Dssi.provisioning=ON -Dweblogic.server.dir=$MW_HOME/wlserver_10.3
-Djdbc.location=$MW_HOME/wlserver_10.3/server/lib/ojdbc6.jar
-Dwork.dir=seed_logs
```

- **Seeding LDAP reconciliation scheduled jobs with the profile file:**

- a. Set the ANT_HOME environment variable to the directory on which ANT is installed.

Note: If ANT is not installed, then download and ANT from Oracle Technology Network (OTN) web site by navigating to the following URL:

<http://www.oracle.com/technetwork/index.html>

Install ANT and set the ANT_HOME. Make sure that ant executable file exists in the \$ANT_HOME/bin/ant/ directory.

- b. Go to the \$OIM_ORACLE_HOME/server/bin/ directory.
- c. Create a property file with the properties listed in [Table E-2](#).

Note: You can also use the appserver.profile file instead of creating a new property file. Make sure that the properties listed in this step are present with the values.

Table E-2 Parameters of the Property File

Parameter	Description
operationsDB.user	Oracle Identity Manager database schema owner.
operationsDB.driver	Constant value of oracle.jdbc.OracleDriver.
operationsDB.host	Oracle Identity Manager database schema host address.
OIM.DBPassword	Oracle Identity Manager database schema owner's password.
operationsDB.serviceName	Oracle Identity Manager database schema service name, for example, oimdb.regress.rdbms.mycompany.com
operationsDB.port	Oracle Identity Manager database schema port number
ssi.provisioning	Value must be ON

Table E–2 (Cont.) Parameters of the Property File

Parameter	Description
weblogic.server.dir	Directory on which Oracle WebLogic Server is installed, for example, <i>MW_HOME/wlserver_10.3</i>
ojdbc.location	Directory on which JDBC is installed, for example, <i>MW_HOME/wlserver_10.3/server/lib/ojdbc6.jar</i>
work.dir	Any preferred directory on which log files will be created After successful completion of target, you can check logs at the <i>\$WORK_DIR/seed_logs/ldap/SeedSchedulerData.log</i> file.
appserver.type	Application server; the value is <i>wls</i> for WebLogic
appserver.dir	Absolute path to the WebLogic Server directory

- d. Go to the *\$OIM_ORACLE_HOME/server/setup/deploy-files/* directory.
- e. Run the following command:

```
$ANT_HOME/bin/ant -f setup.xml seed-ldap-recon-jobs -propertyfile $OIM_ORACLE_HOME/server/bin/PROPERTY_FILE_NAME
```

E.1.4.4 Reverting from OVD to libOVD in LDAPSyc

Either OVD or libOVD can be the front-end to all supported directory servers. However, it is recommended that libOVD, and not stand-alone OVD, is used as the front end to OUD. If you already have a OVD-OUD-OIM topology and wish to convert to libOVD-OUD-OIM, then run the following steps:

1. Disable the incremental role and user reconciliation scheduled jobs.
2. Record the last changelog entry of the directory server by running the following command:

```
ldapsearch -h HOST -p PORT -D "cn=orcladmin" -w PASSWORD -b "" -s base "objectclass=*" lastchangenumber
```

Before re-enabling the scheduled reconciliation jobs, ensure that this changelog number is placed in the IT Resource for the directory server.

3. Create the libOVD adapters. See [Section E.1.3.2, "Creating Identity Virtualization Library \(libOVD\) Adapters and Integrating With Oracle Identity Manager"](#) for details.
4. Edit Oracle Identity Manager IT resource. See [Section E.1.4.2, "Modifying the IT Resource"](#) for details.
5. Re-enable the incremental role and user reconciliation jobs disabled in step 1.

E.2 Managing LDAP Synchronization

Managing LDAP synchronization is described in the following sections:

- [Running the LDAP Post-Configuration Utility](#)
- [Verifying the LDAP Synchronization](#)
- [Customizing and Filtering Users](#)
- [Configuring LDAP Sync Using Plug-ins](#)
- [Troubleshooting and Debugging OVD](#)

- [Filtering Data in Incremental Reconciliation](#)
- [Enabling SSL Between Identity Virtualization Library \(libOVD\) and the Directory Server](#)
- [Provisioning Users and Roles Created Before Enabling LDAP Synchronization to LDAP](#)
- [Disabling LDAP Synchronization](#)
- [Managing Identity Virtualization Library \(libOVD\) Adapters](#)
- [Enabling Access Logging for Identity Virtualization Library \(libOVD\)](#)
- [Configuring LDAP Authentication When LDAP Synchronization is Enabled](#)
- [Verifying the Value of pwdLockout in the Directory Password Policy](#)
- [Fixing Permission Errors with OUD ACIs](#)
- [Disabling the LDAPAddMissingObjectClasses for Users and Roles](#)
- [Setting Up LDAP Synchronization With HA Multi-Master Replication \(MMR\)](#)

Note:

- Before enabling incremental reconciliation through post configuration, as described in this section, always run LDAP full reconciliation first if there is a pre-existing population of users and roles on the directory server. Make sure that incremental reconciliation is disabled until full reconciliation completes. This approach is discussed in "Approach Used for Reconciliation" in *Administering Oracle Identity Manager*.

Oracle recommends using the LDAP Consolidated Full Reconciliation scheduled job, as discussed in "Managing the Scheduler" at the following URL:

http://docs.oracle.com/cd/E37115_01/admin.1112/e27149/scheduler.htm#OMADM2773

- When using AD as the LDAP directory, disable the LDAPAddMissingObjectClasses handler before running full reconciliation, as described in [Section E.2.15, "Disabling the LDAPAddMissingObjectClasses for Users and Roles"](#).
-
-

E.2.1 Running the LDAP Post-Configuration Utility

The LDAP configuration post-setup script enables all the LDAP Sync-related incremental Reconciliation Scheduler jobs, which are disabled by default. In addition, it retrieves the last change number from the Directory Server and updates all the LDAPSvc Incremental Reconciliation jobs and updates all the LDAP synchronization incremental reconciliation jobs with the last change number.

Note:

- This procedure is applicable to all the Directory Server options.
- The LDAP post-setup script and the properties files are located in the *server/LDAP_CONFIG_UTIL* directory under your *IAM_HOME*, which is the Oracle Identity and Access Management home directory for Oracle Identity Manager, Oracle Access Management, Oracle Adaptive Access Manager, Oracle Entitlements Server, Oracle Identity Navigator, Oracle Privileged Account Manager, and Oracle Access Management Mobile and Social.
- The *wlfullclient.jar* file is required to run LDAP configuration post-setup. Generate this file as described in "Post-Configuration Steps" in *Installation Guide for Oracle Identity and Access Management*. In this section, the step to copy the *wlfullclient.jar* file to the *IAM_HOME\designconsole\ext* directory on the machine where Design Console is configured is required only if the Design Console is required for some other purpose than enabling LDAP synchronization. Configuring the Design Console is not required for the purpose of LDAP synchronization.

To run the LDAP post-configuration utility:

1. Before you run the LDAP post-configuration utility, ensure that the following environment variables are set:
 - *APP_SERVER* is set to the application server on which Oracle Identity Manager is running. Set *APP_SERVER* to *weblogic*.
 - *JAVA_HOME* is set to the directory on which JDK is installed on your machine.
 - *MW_HOME* is set to the Middleware home path provided during Oracle Identity Manager installation.
 - *OIM_ORACLE_HOME* is set to the directory on which Oracle Identity Manager is deployed. For example:
 - On UNIX, it is the *MW_HOME/IAM_HOME* directory.
 - On Windows, it is the *MW_HOME\IAM_HOME* directory.
 - *WL_HOME* is set to the *wlserver_10.3* directory under your Middleware home directory. For example:
 - On UNIX, it is the *MW_HOME/wlserver_10.3* directory.
 - On Windows, it is the *MW_HOME\wlserver_10.3* directory.
 - *DOMAIN_HOME* is set to the domain of the WebLogic Server. For example:
 - On UNIX, it is the *MW_HOME/user_projects/domains/base_domain* directory.
 - On Windows, it is the *MW_HOME\user_projects\domains\base_domain* directory.
2. Open the *ldapconfig.props* file in a text editor. This file is located in the *server/ldap_config_util* directory under *IAM_HOME* for Oracle Identity and Access Management.

- In the `ldapconfig.props` file, set values for the parameters listed in [Table E-3](#).

Table E-3 Parameters of the `ldapconfig.props` File

Parameter	Description
OIMServerType	<p>Specify the application server on which Oracle Identity Manager is deployed. For example:</p> <pre>OIMServerType=WLS</pre>
OIMProviderURL	<p>Specify the URL for the Oracle Identity Manager provider. If the OIMServerType is WLS, then specify the URL in the following format:</p> <pre>OIMProviderURL=t3://localhost:MANAGED_SERVER_PORT</pre>
LDAPURL	<p>Specify the URL for the OVD instance.</p> <p>If OVD server is selected during Oracle Identity Manager installation, then provide value for LDAPURL. If OVD server is not selected during Oracle Identity Manager installation, then leave the value of LDAPURL as blank.</p> <p>Specify the URL in the following format:</p> <pre>LDAPURL=ldap://OVD_SERVER:OVD_PORT</pre> <p>For example:</p> <pre>LDAPURL=ldap://OVDserver.examplehost.exampledomain.com:6501</pre> <p>Note: If you have selected Active Directory, OID, ODSEE or OUD as the directory server, then do not specify a value for the LDAPURL parameter. If you are using OVD as the directory server, then enter OVD server and OVD port number and specify the URL as value only.</p>
LDAPAdminUsername	<p>Specify the user name for the OVD Administrator.</p> <p>If OVD server is selected during Oracle Identity Manager installation, then provide the Admin user name to connect to LDAP/OVD Server. For example:</p> <pre>LDAPAdminUsername=cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com</pre> <p>Note: LDAPAdminUsername is the name of the user used to connect to the Identity Store, for example, <code>cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com</code>.</p> <p>This LDAPAdminUsername must not be located in the user container where customer's user accounts exist. For example, do not use <code>cn=Users,cn=mycompanyAccounts,dc=mycompany,dc=com</code>. This user must be outside the search scope to avoid reconciliation of this user into Oracle Identity Manager.</p> <p>Note: If you have selected Active Directory, OID, ODSEE, or OUD as the directory, then do not specify a value of the LDAPAdminUsername parameter after enabling LDAP synchronization. Enter the OVD user admin name as the value only if you are using OVD as the directory server.</p>

Table E-3 (Cont.) Parameters of the `ldapconfig.props` File

Parameter	Description
LIBOVD_PATH_PARAM	<p>Specify the configuration directory path of libOVD. Provide the following value for this parameter:</p> <pre>LIBOVD_PATH_PARAM=MW_HOME/user_projects/domains/base_domain/config/fmwconfig/ovd/oim</pre> <p>Note: If you specify the value for the LIBOVD_PATH_PARAM parameter on Microsoft Windows, then the value must start with the forward slash (/) character. In addition, use forward slash as the path separator, for example:</p> <pre>LIBOVD_PATH_PARAM=/C:/MW_HOME/user_projects/domains/base_domain/config/fmwconfig/ovd/oim</pre> <p>Note: If you have selected Active Directory or ODSEE or OUD as the directory server, then specify the value of this property similar to the example given above.</p> <p>Note: If you have selected OVD server as the directory server, then do not specify a value of this parameter.</p>
ChangeLogNumber	Leave the value of this parameter as blank.

4. Ensure that the required environment variables are set, as described in step 1.
5. Start the Oracle Identity Manager Managed Server. See "Starting the Servers" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
6. On the command line, run the LDAP configuration post-setup script as follows:

On UNIX, run:

```
LDAPConfigPostSetup.sh LOCATION_OF_THE_DIRECTORY_CONTAINING_THE_ldapconfig.props_FILE
```

For example:

```
LDAPConfigPostSetup.sh MW_HOME/IAM_HOME/server/ldap_config_util
```

The scripts run against IPv4 stack by default. If the LDAP is setup on a host configured only with IPv6, then `ipv6` must be passed explicitly as the final argument with the `LDAPConfigPostSetup.sh` script, as shown:

```
LDAPConfigPostSetup.sh LOCATION_OF_THE_DIRECTORY_CONTAINING_THE_ldapconfig.props_FILE ipv6
```

On Windows, run:

```
LDAPConfigPostSetup.bat LOCATION_OF_THE_DIRECTORY_CONTAINING_THE_ldapconfig.props_FILE
```

For example:

```
LDAPConfigPostSetup.bat c:\Oracle\Middleware\IAM_HOME\server\ldap_config_util
```

7. When prompted, enter the Oracle Identity Manager system administrator password and the LDAP administrator password as applicable.

If you are using Active Directory or ODSEE or OUD as the Directory Server, then you are prompted only for the Oracle Identity Manager system administrator password.

If you are using OVD as the Directory Server, then you are prompted for both Oracle Identity Manager system administrator password and LDAP Administrator password.

E.2.2 Verifying the LDAP Synchronization

To verify the configuration of LDAP with Oracle Identity Manager:

1. Ensure that the WebLogic Administration Server and Oracle Identity Manager Managed Server are running.
2. Login to Oracle Identity System Administration.
3. Under Provisioning Configuration, click **IT Resource**. The Manage IT Resource page is displayed. Click **Search**.

Verify the parameter values of Search Base, Reservation Container, URL, and bind DN.

See "Managing IT Resources" in *Administering Oracle Identity Manager*.

4. Login to Oracle Identity Self Service, and create a user.
5. Verify that the same user is created in the chosen LDAP store or OVD by using any LDAP client.

Note: Ensure that the chosen Directory Server or OVD and Oracle Identity Manager are running.

E.2.3 Customizing and Filtering Users

Customizing and filtering user creation can be done in the following ways:

- [Customizing User Creation Through Oracle Identity Manager With Different Custom Object Classes](#)
- [Creating Users in Oracle Identity Manager and Not in LDAP When LDAP Synchronization is Enabled](#)

E.2.3.1 Customizing User Creation Through Oracle Identity Manager With Different Custom Object Classes

You can add custom object classes and custom attributes while creating a new user by adding the custom attributes as user-defined fields (UDFs) in Oracle Identity Manager as well as to the LDAPUser.xml in MDS. As a prerequisite, the custom object class with one or more attributes must be created and loaded into OID.

To add custom attributes as UDFs in Oracle Identity Manager and LDAPUser.xml in MDS:

1. Add the custom attributes to the user attributes in Oracle Identity Manager, as described in "Creating a Custom Attribute" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.
2. Export the /metadata/iam-features-ldap-sync/LDAPUser.xml metadata file from the repository, as described in "Migrating User Modifiable Metadata Files" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

3. Update the LDAPUser.xml file to add the custom attribute1 custom attribute and customObjectClass custom object class.
4. To add additional object classes on 'create', edit LDAPUser.xml and add additional <value> entries to the <parameter name="objectclass"> node. For example:

```
<parameter name="objectclass">
<value>orclIDXPerson</value>
<value>customObjectClass</value>
</parameter>
```

5. Add your custom attributes to the three sections of the LDAPUser.xml file. To do so:
 - a. Add the attribute entry to the end of the <entity-attributes> tag, for example:

```
<entity-attributes>
.....
.....
<attribute name="custom attribute1">
<type>string</type>
<required>>false</required>
<attribute-group>Basic</attribute-group>
<searchable>>true</searchable>
</attribute>
</entity-attributes>
```

Note: If you are using an OUD LDAP directory, then the custom attribute name must not contain a space. OUD does not allow creating a custom attribute with space in the attribute name.

- b. Add the attribute entry to the end of the <target-fields> tag, for example:

```
<target-fields>
.....
.....
<field name="customattr1">
<type>string</type>
<required>>false</required>
</field>
</target-fields>
```

- c. Add the attribute entry to the end of the <attribute-maps> tag, for example:

```
<attribute-maps>
.....
.....
<attribute-map>
<entity-attribute>custom attribute1</entity-attribute>
<target-field>customattr1</target-field>
</attribute-map>
</attribute-maps>
```

- d. Save and close the LDAPUser.xml file.
6. Import the /metadata/iam-features-ldap-sync/LDAPUser.xml metadata file into the repository, as described in "Migrating User Modifiable Metadata Files" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

7. (Optional) If you want to change the RDN attribute from 'cn' to another attribute, then update the <parameter name="rdnattribute"> tag to the new directory attribute name, and then reimport the /metadata/iam-features-ldap-sync/LDAPUser.xml metadata file into the repository. For example:

```
<parameter name="rdnattribute">
<value>companyid</value>
</parameter>
```

8. Test the configuration by creating the new user through Oracle Identity Manager.

E.2.3.2 Creating Users in Oracle Identity Manager and Not in LDAP When LDAP Synchronization is Enabled

When LDAP synchronization is enabled, you can configure the filter parameter 'excludeEntityFilter' in the LDAPUser.xml file to filter out user entries to be created in LDAP, but that can only reside in Oracle Identity Manager. Based on any Oracle Identity Manager attribute and its value, users can be created in Oracle Identity Manager without pushing to LDAP server although LDAP synchronization is in enabled mode.

Note: This feature is supported only for the user entity.

For example, if you want Oracle Identity Manager accounts with act_key=2 not to be created in LDAP, then perform the following steps:

1. Import the LDAPUser.xml file from MDS.
2. Add the following filter to LDAPUser.xml:

```
<parameter name="excludeEntityFilter">
<value>act_key=2</value>
</parameter>
<parameter name="excludeEntityActions">
<value>ALL</value>
</parameter>
```

3. Export the LDAPUser.xml file to MDS.
4. Create a user in Oracle Identity Manager with organization act_key as 2. The same user will not be created in LDAP. Note that users created in Oracle Identity Manager that are assigned to organization with act_key other than 2 are successfully created in LDAP.

Another example is to create users only in Oracle Identity Manager but not in LDAP server in LDAP synchronization enabled mode if the user's role matches 'Full-Time'. To do so, use the filter parameter as shown:

```
<parameter name="excludeEntityFilter">
<value>Role=Full-Time</value>
</parameter>
<parameter name="excludeEntityActions">
<value>ALL</value>
</parameter>
```

In the examples, certain Oracle Identity Manager users are not allowed in LDAP based on the filter and actions. By default, ALL is set for disabling the operations, and no CRUD operation is possible on these users. This is as shown:

```
<parameter name="excludeEntityActions">
<value>ALL</value>
</parameter>
```

The filter that you provide in the LDAPUser.xml file is evaluated and a boolean value is returned to determine whether or not to proceed to LDAP synchronization handlers.

Schema file is available in the product for these parameters. If you want to customize it, then configuration has to be done in the LDAPUser.xml file, which must be exported back to MDS.

E.2.4 Configuring LDAP Sync Using Plug-ins

For an integration scenario with a standalone instance of OVD, configuring LDAP synchronization using plug-ins:

Note: This section only applies to integration with a standalone instance of Oracle Virtual Directory.

- [Using the UserManagement Plug-In](#)
- [Using the Changelog Plug-In](#)

E.2.4.1 Using the UserManagement Plug-In

This topic describes the plug-ins designed for use when Oracle Virtual Directory is a connector target for Oracle Identity Manager integrations.

The UserManagement plug-in provides data mapping for Oracle Identity Manager attributes to LDAP directory servers.

E.2.4.1.1 Configuration Parameters The UserManagement plug-in has the following configuration parameters:

filterObjectclass

Comma-separated list of objectclasses that need to be removed on an add/modify request.

removeAttribute

Comma-separated list of attributes that will be virtually removed from entries before they are returned to the client.

exclusionMapping

Defines the exclusion of a specific attribute mapping on a specific objectclass. For example, specifying a parameter with the value `inetorgperson,uid=samaccountname` excludes mapping a `uid` to `samaccountname` on entries of objectclass `inetorgperson`. Using multiple instances of this option allows for multiple exclusions on mappings.

oimLanguages

Comma-separated list of language codes to be used in attribute language subtypes. This parameter is functional only when the `directoryType` parameter is set to `ActiveDirectory`.

oamEnabled

True or False: Indicates whether Oracle Access Management Access Manager (Access Manager) is deployed with Oracle Identity Manager. By default, Access Manager is not deployed, therefore the default setting for this parameter is false.

Note: The `oamEnabled` parameter for the UserManagement plug-in and the changelog plug-in must have identical values.

directoryType

Identifies the type of source LDAP directory server. Supported values are `OID`, `ActiveDirectory`, and `SunOne`. The default value is `OID`.

Note: The `directoryType` parameter for the UserManagement plug-in and the changelog plug-in must have identical values.

ssladapter

The `ssladapter` parameter, which is operational only when the `directoryType` parameter is set to `ActiveDirectory`, identifies the name of the adapter to which the UserManagement plug-in routes requests when `userPassword` or `unicodePwd` is contained in requests. If `unicodePwd` is contained in the request, the request must also contain the `useraccountControl` attribute with a proper value.

The adapter identified by the `ssladapter` parameter *must* have:

- The same local base as the adapter the UserManagement plug-in is configured on
- Its Routing Visibility set to **Internal**

If no value is set for `ssladapter`, the current adapter is used by default.

mapAttribute

Defines the attribute translation in the form of *OVD-attribute=OIM-attribute*, for example: `orclGUID=objectGuid`. You can set the `mapAttribute` configuration parameter multiple times to define translations for multiple attributes.

mapPassword

True or False. When the `directoryType` configuration parameter is set to `ActiveDirectory`, the `mapPassword` parameter controls whether to convert the user password to the `unicodePwd` attribute. The default value is `false`.

mapRDNAttribute

Defines the RDN attribute translation in the form of *OVD-RDNattribute=OIM-RDNattribute*, for example: `uid=cn`.

pwdMaxFailure

Identifies the maximum number of failed logins the source LDAP directory server requires to lock an account (as defined by the password policy effective on the user entries being exposed through the adapter on which this plug-in is deployed).

Note: Parameter values for `XL.MaxLoginAttempts`, `pwdMaxFailure`, and `lockout count` must be the same in LDAP-enabled setups. In LDAP-enabled environments, the values specified for these attributes must be consistent for lock/unlock to work consistently. For example, in LDAP-enabled environment with `libOVD` and `OUD`, the value of the `XL.MaxLoginAttempts` system property is set to 10, and `pwdMaxFailure` in `adapters.os_xml` is set to 10. However, the `OUD lockout-failure-count` is set to 25. For lock/unlock to work consistently, the attribute values in `OUD` and `adapters.os_xml` must be the same.

mapObjectclass

Defines the objectclass value translation in the form of *OVD-objectclass=OIM-objectclass*, for example: *inetorgperson=user*. You can set the `mapObjectclass` configuration parameter multiple times to define translations for multiple objectclasses.

Note: The `mapObjectclass` parameter for the UserManagement plug-in and the changelog plug-in must have identical values.

addAttribute

In the form of *attribute=value pairs*, this parameter identifies attributes to be added before returning the get operation result. You can prefix the attribute name with *objectclass*, to add the attribute and value to a specific objectclass. You can also surround a value with % to reference other attributes. For example, specifying the value *user,samaccountname=%cn%* assigns the value of `cn` to `samaccountname` when the entry `objectclass=user`. Specifying the value *samaccountname=jdoe* adds attribute `samaccountname` with value `jdoe` to all the entries.

E.2.4.2 Using the Changelog Plug-In

Note: Prior to release 11.1.1.4.0, Oracle Virtual Directory had three changelog plug-ins:

- `oidchangelog` for use with Oracle Internet Directory
- `sunonechangelog` for use with Oracle Directory Server Enterprise Edition
- `adchangelog` for use with Microsoft Active Directory

These three plug-ins were deprecated in release 11.1.1.4.0 and a new, single Changelog plug-in is now available. You can use this plug-in with Oracle Internet Directory, Oracle Directory Server Enterprise Edition, and Microsoft Active Directory.

E.2.4.2.1 Deploying the Release 11.1.1.4.0 Changelog Plug-In When deploying the single Changelog plug-in, you must:

- Set the adapter's Remote Base to an empty value; that is blank, nothing.
- Set the adapter's Mapped Namespace to: `cn=changelog`.
- If the back-end is Oracle Directory Server Enterprise Edition, be sure to enable change logging on Oracle Directory Server Enterprise Edition.

E.2.4.2.2 Deploying Changelog Plug-Ins from Prior Releases If you are using a version of Oracle Virtual Directory that was released *prior to 11.1.1.4.0*, you must use the following changelog plug-ins to standardize changelog information from source directories into a suitable format for Oracle Identity Manager.

Note: These plug-ins *will not* work with Oracle Virtual Directory release 11.1.1.4.0.

For Oracle Internet Directory

Use the oidchangelog plug-in with Oracle Internet Directory.

When deploying the oidchangelog plug-in, you must set the adapter's Remote Base to an empty value; that is, blank, nothing.

For Oracle Directory Server Enterprise Edition

Use the sunonechangelog plug-in with Oracle Directory Server Enterprise Edition.

When deploying the sunonechangelog plug-in, you must:

- Set the adapter's Remote Base to an empty value; that is, blank, nothing.
- Ensure change logging is enabled on the Oracle Directory Server Enterprise Edition.
- Set the adapter's Mapped Namespace to: `cn=changelog`

For Microsoft Active Directory

Use the adchangelog plug-in with Microsoft Active Directory.

When deploying the adchangelog plug-in, you must:

- Set the adapter's Remote Base to an empty value; that is, blank, nothing.
- Set the adapter's Mapped Namespace to: `cn=changelog`

E.2.4.2.3 Configuration Parameters Each of the changelog plug-ins have the following configuration parameters:

removeAttribute

Comma-separated list of attributes that are virtually removed from entries before they are returned to the client.

oimLanguages

Comma-separated list of languages to be used in attribute language subtypes.

skipErrorChangelog

True or False. If set to false and the plug-in encounters a corrupted changelog entry, the plug-in throws a `DirectoryException` and stops further processing changelog entries. If set to true, the plug-in logs an error without throwing an exception, skips this changelog, and continues processing the next changelogs. The default value is false.

oamEnabled

True or False: Indicates whether Access Manager is deployed with Oracle Identity Manager. By default, Access Manager is not deployed, therefore the default setting for this parameter is false.

Note: The `oamEnabled` parameter for the `UserManagement` plug-in and the changelog plug-in must have identical values.

directoryType

Identifies the type of source LDAP directory server. Supported values are `OID`, `ActiveDirectory`, and `SunOne`. The default value is `OID`.

Note: The `directoryType` parameter for the `UserManagement` plug-in and the `changelog` plug-in must have identical values.

mapObjectclass

Defines the `objectclass` value translation in the form of *OIM-objectclass=Source-Directory-objectclass*, for example: `inetorgperson=user`. You can set the `mapObjectclass` configuration parameter multiple times to define translations for multiple objectclasses.

In the Oracle Identity Manager use case, the following parameters are configured out-of-the-box:

- **For Active Directory:** `inetorgperson=user`, `orclidperson=user`, and `groupOfUniqueNames=group`
- **For Oracle Directory Server Enterprise Edition:** `container=nsContainer` and `changelog=changelogentry`
- **For Oracle Internet Directory:** `container=orclContainer`

Note: The `mapObjectclass` parameter for the `UserManagement` plug-in and the `changelog` plug-in must have identical values.

sizeLimit

Identifies the maximum number of `changelog` entries to be returned.

A zero (0) or a negative value means no size restriction.

If the incoming search request specifies a size constraint, then the smaller value is used. For example, if you specify the plug-in's `sizeLimit` as 100, and the search request's count limit is 200, then the actual size limit of the request is reset to 100.

mapAttribute

Defines the attribute translation in the form of *Source-Directory-attribute=OIM-attribute*, for example: `orclGUID=objectGuid`. You can set the `mapAttribute` configuration parameter multiple times to define translations for multiple attributes.

targetDNFilter

Identifies the container to retrieve changes from. This parameter can be set multiple times to identify multiple containers to retrieve changes from. If set multiple times, the `targetDN` filter should look similar to the following example, and this `targetDN` filter is "ANDed" to the incoming filter:

```
" ( | (targetDN=*cn=users,dc=mycom1) (targetDN=*,cn=groups,dc=mycom2) ) "
```

Sample values include:

- `*,cn=xxx,dc=yyy`
- `*cn=xxx,dc=yyy`
- `cn=xxx,dc=yyy` (must be a descendant of the local base of the adapter specified in `virtualDITAdapterName`)

All of these samples have the same meaning.

requiredAttribute

Comma-separated list of attributes to always be retrieved from the source LDAP directory server, regardless of the return attributes list specified for changelog queries to Oracle Virtual Directory.

addAttribute

Comma-separated list of attributes to be added to the normalized changelog entry. For example, orclContainerOC=1, changelogSupported=1, where =1 indicates the changes retrieved from the source directory which support changelog.

mapUserState

True or False. This parameter enables or disables the mapping of the directory specific account attributes to Oracle Virtual Directory virtual account attributes.

modifierDNFilter

Single-valued configuration parameter that defines an LDAP filter on modifiersName. This parameter is "ANDed" to the incoming filter. An example value can be "(modifiersName=cn=myadmin,cn=users,dc=mycom)".

Note: This configuration does not take effect if directoryType=ActiveDirectory.

virtualDITAdapterName

Identifies the corresponding user profile adapter name.

For example, in a single-directory deployment, you can set this parameter value to "A1," which is the user adapter name. In a split-user profile scenario, you can set this parameter to "J1;A2," where "J1" is the JoinView adapter name, and "A2" is the corresponding user adapter in the "J1".

This parameter can be multi-valued, which means there are multiple base entry adapters configured for the same back-end directory server as this changelog adapter.

If you set this parameter to "A1," the plug-in fetches the mapAttribute and mapObjectclass configuration in the UserManagementPlugin of adapter A1, so you do not have to duplicate those configurations.

E.2.5 Troubleshooting and Debugging OVD

This topic describes how to enable debugging in Oracle Virtual Directory, which can be useful if you need to troubleshoot your Oracle Identity Manager and Oracle Virtual Directory integration.

To enable debugging, perform the following steps:

1. Open a command window and go to the following location:

```
OVD ORACLE_INSTANCE/config/OVD/ovd1
```

2. Save a copy of the ovd-logging.xml file.
3. Edit the ovd-logging.xml file as follows:

- Change line #25 from:

```
<logger name='com.octetstring.vde' level='NOTIFICATION:1'  
useParentHandlers='false'>
```

```
to
```

```
<logger name='com.octetstring.vde' level='TRACE:32'
useParentHandlers='false'>
```

- Change line #28 from:

```
<logger name='com.octetstring.accesslog' level='ERROR:1'
useParentHandlers='false'>
```

to

```
<logger name='com.octetstring.accesslog' level='NOTIFICATION:1'
useParentHandlers='false'>
```

4. Restart Oracle Virtual Directory by typing the following:

```
cd OVD_INSTANCE/bin
./opmnctl stopall
./opmnctl startall
```

See Also: ["Using My Oracle Support for Additional Troubleshooting Information"](#) on page 1-31.

E.2.6 Filtering Data in Incremental Reconciliation

Changelog query returns incremental changes of user/role accounts or entries in the LDAP server to Oracle Identity Manager database during changelog reconciliation when LDAP synchronization incremental reconciliation jobs are run. However, you can choose not to return changes to Oracle Identity Manager database for some entries in LDAP based on a rule or filter during the changelog reconciliation when LDAP synchronization incremental reconciliation jobs are run. To do so, you can use the `includeEntriesFilter` filter tag or filter parameter in the `LDAPUser.xml` file to filter out the unwanted entries and bring in only the required entries based on the rule before sending the data to the reconciliation engine, so that those entries are not in Oracle Identity Manager database. In other words, support for attribute level filtering is provided.

The following example shows how you can specify the attribute-level filtering in the `LDAPUser.xml` file:

```
<parameter name="includeEntriesFilter">
  <value>employeeNumber=123456</value>
</parameter>
```

Here, the `<value>` tag contains the `employeeNumber` LDAP attribute and the corresponding value. This filters out all the changelog entries or user entries from the LDAP server that match the criteria "employeeNumber=123456", and sends them to the reconciliation engine for the users to be reconciled into Oracle Identity Manager database. Other changelog entries that do not match this filter are stopped from being sent to the reconciliation engine to be reconciled into Oracle Identity Manager database.

The following is a sample of the `includeEntriesFilter` filter parameter:

```
(!(LDAP_attribute=val1) (LDAP_attribute=val2) (LDAP_attribute=val3) ...)
```

If the values are variables, then the filter must be "ObjectClass=*". You must specify a variable value for `LDAP_attribute` as different users have different attribute values.

E.2.7 Enabling SSL Between Identity Virtualization Library (libOVD) and the Directory Server

For SSL, you must export the server side certificates from the directory server and import into Identity Virtualization Library (libOVD), as described in the following sections:

- [Enabling SSL Between Identity Virtualization Library \(libOVD\) and Microsoft Active Directory](#)
- [Enabling SSL Between Identity Virtualization Library \(libOVD\) and iPlanet](#)
- [Enabling SSL Between Identity Virtualization Library \(libOVD\) and OID](#)

E.2.7.1 Enabling SSL Between Identity Virtualization Library (libOVD) and Microsoft Active Directory

To export the server side certificates from Active Directory and import into Identity Virtualization Library (libOVD):

1. Export the certificate from the Active Directory server by referring to the instructions in the following Microsoft TechNet documents:

<http://technet.microsoft.com/en-us/library/cc732443%28WS.10%29.aspx>

<http://technet.microsoft.com/en-us/library/cc772898%28WS.10%29.aspx>

2. Retrieve the CA signing certificate and save it to a file. To do so:
 - a. Login to the Active Directory domain server as a domain administrator.
 - b. Click **Start, Control Panel, Administrative Tools, Certificate Authority** to open the CA Microsoft Management Console (MMC).
 - c. Right-click the CA computer, and select **CA Properties**.
 - d. From the General menu, select **View Certificate**.
 - e. Select the Details view, and click **Copy to File** on the lower-right corner of the window.
 - f. Use the Certificate Export wizard to save the CA certificate in a file by running the following command:

```
certutil -ca.cert OutCACertFile
```

Note: You can save the CA certificate in either DER Encoded Binary X-509 format or Based-64 Encoded X-509 format.

3. Import the Active Directory server certificate created in step 3f to the Identity Virtualization Library (libOVD) keystore as a trusted entry by running the following command:

```
$ORACLE_HOME/jdk/jre/bin/keytool -importcert -keystore $DOMAIN_
HOME/config/fmwconfig/ovd/CONTEXT/keystores/adapters.jks -storepass password
-alias alias -file OutCACertFile -noprompt
```

E.2.7.2 Enabling SSL Between Identity Virtualization Library (libOVD) and iPlanet

To export certificates from iPlanet (ODSEE) and import into Identity Virtualization Library (libOVD) for enabling SSL between Identity Virtualization Library (libOVD) and iPlanet (ODSEE):

1. To export certificate from iPlanet (ODSEE), run the following command:

```
dsadm export-cert -o OUTPUT_FILE INSTANCE_PATH CERT_ALIAS
```

For example:

```
./dsadm export-cert -o /tmp/server-cert /scratch/aim1/iPlanet/dsInst/defaultCert
```

Choose the PKCS#12 file password:

Confirm the PKCS#12 file password:

```
ls -lrt /tmp
```

```
-rw----- 1 aim1 svrtech 1684 Jan 20 00:39 server-cert
```

2. To import the iPlanet (ODSEE) certificate created in step 1 to the Identity Virtualization Library (libOVD) keystore as a trusted entry, run the following command:

```
ORACLE_HOME/jdk/jre/bin/keytool -importcert -keystore
$DOMAIN_HOME/config/fmwconfig/ovd/CONTEXT/keystores/adapters.jks -storepass
PASSWORD -alias ALIAS_VALUE_USED_FOR_EXPORT -file SERVER-CERT_FILENAME
-noprompt
```

Note: Provide the same certificate alias name, which you provided for exporting the certificate, for the '-alias' parameter while importing the certificate. For example:

```
ORACLE_HOME/jdk/jre/bin/keytool -importcert -keystore
$DOMAIN_HOME/config/fmwconfig/ovd/CONTEXT/keystores/adapters.jks
-storepass password -alias defaultCert -file server-cert -noprompt
```

In addition, export/import certificates as instructed in the ODSEE documentation in the following URL:

<http://docs.oracle.com/cd/E19656-01/821-1504/gcvhu/index.html>

E.2.7.3 Enabling SSL Between Identity Virtualization Library (libOVD) and OID

To export the server side certificates from OID and import into Identity Virtualization Library (libOVD):

1. Export the Oracle Internet Directory server certificate in Base64 format using the following command:

```
orapki wallet export -wallet LOCATION_OF_OID_WALLET -dn DN_FOR_OID_SERVER_
CERTIFICATE -cert ./b64certificate.txt
```

Note: If you use a certificate alias in the orapki command, then an error is generated if the alias is not in all lower case letters.

2. Import the Oracle Internet Directory server certificate created in step 2 to the Identity Virtualization Library (libOVD) keystore as a trusted entry using the following command:

```
$ORACLE_HOME/jdk/jre/bin/keytool -importcert -keystore $DOMAIN_
HOME/config/fmwconfig/ovd/CONTEXT/keystores/adapters.jks -storepass password
-alias alias -file OutCACertFile -noprompt
```

E.2.8 Provisioning Users and Roles Created Before Enabling LDAP Synchronization to LDAP

If you create users and roles in Oracle Identity Manager deployment without LDAP synchronization, and later decide to enable LDAP synchronization, then the users and roles created before LDAP synchronization enablement must be synced with LDAP after enablement. The provisioning of users, roles, role memberships, and role hierarchy to LDAP is achieved by the following predefined scheduled jobs for LDAP:

- LDAPSync Post Enable Provision Users to LDAP
- LDAPSync Post Enable Provision Roles to LDAP
- LDAPSync Post Enable Provision Role Memberships to LDAP
- LDAPSync Post Enable Provision Role Hierarchy to LDAP

For details about these scheduled jobs, see "Predefined Scheduled Tasks" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

E.2.9 Disabling LDAP Synchronization

To disable LDAP synchronization in Oracle Identity Manager deployment:

1. Remove the `/db/ldapMetadata/EventHandlers.xml` file from MDS by using Oracle Enterprise Manager. See "Migrating User Modifiable Metadata Files" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about deleting metadata files from MDS.
2. Login to Oracle Identity System Administration as the System Administrator.
3. Disable all scheduled jobs for LDAP sync reconciliation. These jobs are:
 - LDAP User Create and Update Reconciliation
 - LDAP Role Create and Update Reconciliation
 - LDAP Role Membership Reconciliation
 - LDAP Role Hierarchy Reconciliation

This list can also include LDAP User Delete Reconciliation and LDAP Role Delete Reconciliation scheduled jobs. For information about these scheduled jobs, go to the following URL:

http://docs.oracle.com/cd/E37115_01/admin.1112/e27149/scheduler.htm#OMADM2773

E.2.10 Managing Identity Virtualization Library (libOVD) Adapters

In an Oracle Identity Manager deployment with LDAP synchronization enabled and AD, iPlanet (ODSEE), or OID as the directory server, you can manage the Identity Virtualization Library (libOVD) adapters by using the WLST command.

See Also: Library Oracle Virtual Directory (LibOVD) Commands in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference* for information about the WLST commands to manage Library Oracle Virtual Directory (LibOVD) adapters

To manage the Identity Virtualization Library (libOVD):

1. Start the WLST console. To do so, run `$FMW_ROOT/Oracle_IDM1/common/bin/wlst.sh`. This path can be referenced as `$OIM_ORACLE_HOME/common/bin/wlst.sh`.

Here, `$FMW_ROOT` refers to your `$MW_HOME` directory. For example, for this binary location, it can be the `/u01/apps/mwhome/` directory.

`$OIM_ORACLE_HOME` refers to the directory in which Oracle Identity Manager is deployed. For example, `/u01/apps/mwhome/Oracle_IDM1/` must point to `OIM_ORACLE_HOME`.

2. In the WLST console, run the following command:

```
connect()
```

When prompted, provide the WLST username, password, and t3 URL.

3. Run the following command to display a list of Identity Virtualization Library (libOVD) WLST commands:

```
help('OracleLibOVDConfig')
```

This lists the commands for creating, deleting, and modifying Identity Virtualization Library (libOVD), LDAP, and join adapters. The following commands act on the Identity Virtualization Library (libOVD) configuration associated with a particular OPSS context, which is passed in as a parameter:

- **addJoinRule:** Adds a join rule to an existing Join adapter for the Identity Virtualization Library (libOVD) associated with the given OPSS context
- **addLDAPHost:** Adds a new remote host to an existing LDAP adapter

Note: The following is an example of adding multiple remote hosts for High Availability (HA) scenario:

```
addLDAPHost(adapterName='ldap1', host='myhost.example.domain.com',
port=389, contextName='myContext')
```

See *Oracle Fusion Middleware High Availability Guide* for detailed information about HA.

- **addPlugin:** Adds a plug-in to an existing adapter or at the global level

See Also: "Developing Plug-ins" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about developing plug-ins in Oracle Identity Manager

- **addPluginParam:** Add new parameter values to the existing adapter level plug-in or global plug-in
- **createJoinAdapter:** Creates a new Join adapter for the Identity Virtualization Library (libOVD) associated with the given OPSS context

- **createLDAPAdapter:** Creates a new LDAP adapter for the Identity Virtualization Library (libOVD) associated with the given OPSS context
 - **deleteAdapter:** Deletes an existing adapter for the Identity Virtualization Library (libOVD) associated with the given OPSS context
 - **getAdapterDetails:** Displays the details of an existing adapter that is configured for the Identity Virtualization Library (libOVD) associated with the given OPSS context
 - **istAdapters:** Lists the name and type of all adapters that are configured for this Identity Virtualization Library (libOVD) associated with the given OPSS Context
 - **modifyLDAPAdapter:** Modifies the existing LDAP adapter configuration
 - **removeJoinRule:** Removes a join rule from a Join adapter configured for this Identity Virtualization Library (libOVD) associated with the given OPSS Context
 - **removeLDAPHost:** Removes a remote host from an existing LDAP adapter configuration
 - **removePlugin:** Removes a plug-in from an existing adapter or at global level
 - **removePluginParam:** Removes an existing parameter from a configured adapter level plug-in or global plug-in
4. Run help on the individual commands to get usage, such as:

```
help('addPluginParam')
```

The following are examples for updating the AD User Management adapter for the oimLanguages attribute for Multi Language Support (MLS):

- **addPluginParam:**

You can use this command to add oimLanguage param to UserManagement plug-in in AD user adapter, as shown:

```
add PluginParam(adapterName='ldap1', pluginName='UserManagement',
paramKeys='oimLanguages', paramValues='fr,zh-CN', contextName='oim')
```

- **removePluginParam:**

You can use this command to remove oimLanguage param from UserManagement plug-in in AD user adapter, as shown:

```
removePluginParam(adapterName='ldap1', pluginName='UserManagement',
paramKey='oimLanguages', contextName='oim')
```

- **removePluginParam:**

You can use this command to remove modifierDNFilter param from Changelog plug-in, as shown:

```
removePluginParam(adapterName='CHANGELOG_ldap1', pluginName='Changelog',
paramKey='modifierDNFilter', contextName='oim')
```

See Also: "Creating Adapters in Oracle Virtual Directory" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* for detailed information about creating the OVD adapters for Oracle Identity Manager change log and user management

E.2.11 Enabling Access Logging for Identity Virtualization Library (libOVD)

Enabling access logging for Identity Virtualization Library (libOVD) allows you to capture all requests and responses flowing through Identity Virtualization Library (libOVD), which can be very useful if you are trying to triage performance issues.

To enable access logging for Identity Virtualization Library (libOVD):

1. Remove any Identity Virtualization Library (libOVD) loggers that were previously configured in Debug mode. You must remove these loggers to see real performance numbers. See "[Troubleshooting and Debugging OVD](#)" on page E-36 for information about how to enable debugging in OVD.
2. Create a WLS logger named `oracle.ods.virtualization.accesslog` in WLS with NOTIFICATION level.
3. Create a WLS loghandler, specifying a file name similar to `ovd-access.log` and associate that log handler to the logger you created in step 2.

This loghandler logs all Oracle Virtual Directory access log messages into a separate file.

4. Create a backup of the `DOMAIN_HOME/config/fmwconfig/ovd/default/provider.os_xml` file, and then add the following XML fragment (if it is not already present):

```
<providers ...>
...
<auditLogPublisher>
  <provider name="FMWAuditLogPublisher">
    ...
  </provider>
  <provider name="AccessLogPublisher">

<configClass>oracle.ods.virtualization.config.AccessLogPublisherConfig</configC
lass>
  <properties>
    <property name="enabled" value="true"/>
  </properties>
</provider>
</auditLogPublisher>
...
</providers>
```

5. Restart the WLS Admin and Managed servers.

Oracle Virtual Directory can now generate the access log in the `ovd-access.log` file.

E.2.12 Configuring LDAP Authentication When LDAP Synchronization is Enabled

Use the following procedure to be able to use LDAP for authentication when LDAP synchronization is enabled.

Note: This procedure does not enable the following functionality:

- Forced password changes, including first login, administrator password reset, and expired passwords
 - Forced setting of challenge responses
-
-

1. Configure the LDAP Authenticator in WLS. To do so:

- a. Log in to WebLogic Administrative Console.
- b. Go to Security Realms, myrealm, Providers.
- c. Click **New**. Give a name and choose OracleInternetDirectoryAuthenticator as type.
- d. Set the Control Flag to SUFFICIENT.
- e. Click the Provider Specific settings and configure the OID connection details.
- f. In Dynamic groups section, enter the following values:
 - Dynamic Group Name Attribute: cn
 - Dynamic Group Object Class: orcldynamicgroup
 - Dynamic Member URL Attribute: labeleduri
 - User Dynamic Group DN Attribute: GroupOfUniqueNames
- g. Click the **Providers** tab. Remove OIM Authenticator from the list of security providers. This is to ensure that the user is not locked in Oracle Identity Manager database.
- h. Configure the OIMSignatureAuthenticator security provider in the realm. To do so:
 - i) Login to the WebLogic Administrative Console.
 - ii) Navigate to **Security realm, myrealm, Security providers, Authentication, New**.
 - iii) Select **OIMSignatureAuthenticator** from the drop-down, and select provider name as OIMSignatureAuthenticator.
 - iv) Save the changes.
- i. Click **Reorder**. Reorder the security providers and set their Control Flags as listed in the following table:

Authentication Provider	Control Flag
Default Authenticator	SUFFICIENT
OIM Signature Authenticator	SUFFICIENT
LDAP Authenticator	SUFFICIENT
Default Identity Asserter	Not applicable

2. Restart all servers.
3. Validate role memberships.
 - a. Login to WebLogic Admin Console.
 - b. Go to Security Realms, myrealm, User and Groups.
 - c. Click **users** to display all the users in the LDAP user search base. If the LDAP users are not displayed, it means that there is an error with the LDAP connection, and the details are specified in OID Authenticator (provider specific settings).
 - d. Click on any user and then to the corresponding group entry. "Oimusers" should be one of the listed entries. If this validation fails, please go through the LDAP authenticator's provider-specific details.

E.2.13 Verifying the Value of pwdLockout in the Directory Password Policy

Correct notification is sent when a user is locked by an administrator if the `pwdLockout` attribute is set to `TRUE` by the password policy in the directory server.

A user locked by the administrator cannot be unlocked by the forgot password flow, but the notification sent to the user is misleading if the value of `pwdLockout` is set to `FALSE`.

Therefore, validate the password policy for the LDAP server and check the attributes of the entry `"cn=Password Policy,cn=config"`. Ensure that `pwdLockout` is set to `TRUE`.

E.2.14 Fixing Permission Errors with OUD ACIs

If the following type of errors occur when synchronizing with OUD, then it is necessary to update the ACIs for OUD:

```
<Jan 27, 2014 9:36:12 AM PST> <Warning>
<oracle.ods.virtualization.engine.backend.jndi.CHANGELOG_oud1> <LIBOVD-40066>
<Remote Server Failure:example.com:1234.
javax.naming.NoPermissionException: [LDAP: error code 50 - The request control
with Object Identifier (OID) "1.3.6.1.4.1.26027.1.5.4" cannot be used due to
insufficient access rights]; remaining name 'cn=Changelog'.
```

Note that the list of OIDs with insufficient access rights includes, but is not limited to:

```
1.3.6.1.4.1.26027.1.5.4
1.3.6.1.4.1.26027.2.3.4
1.2.840.113556.1.4.319
```

To remedy this problem:

1. Verify that the `ObjectIdentifier` is defined in the Global ACI in the OUD configuration file `OID_INSTANCE/config/config.ldif`.
2. If a particular `ObjectIdentifier` is not defined, then add the missing OID to OUD by using the `dsconfig` tool, as described in "Managing Global ACIs With `dsconfig`" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory*.

If the particular control is not defined, or if it is defined but granted to a `groupdn`, then the following command defines it and assigns it to a `userdn`:

```
$ dsconfig -h {Hostname} -p {Port} -D cn="Directory Manager" -j pwd-file -n \
  set-access-control-handler-prop \
  --add global-aci:\(targetcontrol="1.3.6.1.4.1.26027.1.5.4" \ (version 3.0;
  acl \"Authenticated users control
  access\"; allow\read\ userdn=\"ldap:///all\";\)
```

3. Double-check the configuration file and ensure that there are no duplicate lines.
4. Save the configuration file.
5. Restart OUD and Oracle Identity Manager servers.

E.2.14.1 Checking and Fixing ACIs With `lastExternalChangelogCookie` for OUD

The `LDAPConfigPostConfig` script normally fetches the LDAP `lastchangenumber` and updates incremental reconciliation jobs. For OUD, situations can arise where Oracle Identity Manager administrator cannot access the `lastExternalChangeLogCookie`, and the `lastchangenumber` cannot be updated, leading to incorrect results. This is because the ACIs are not granted successfully. To test if this is the issue, run:

```
ldapsearch -x -h OUD_HOST -p OUD_PORT -D OIM_ADMIN -w PASSWORD -s base -b ""
"objectclass=*" lastExternalChangelogCookie
```

This must return results. If not, then the problem can be fixed by performing the following steps:

1. Remove the ACI that denies access to cn=changelog.
2. Add an ACI allowing your user or group access to cn=changelog.
3. For reading in cookie mode only, add an ACI allowing usage of the OUD cookie control to your user or group.
4. For reading in cookie mode only, add an ACI allowing your user or group to read the lastExternalChangelogCookie from the root entry (-s base -b "").

Note: For detailed instructions on granting OUD change log access, see "Granting Oracle Unified Directory Change Log Access" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

All steps must be verified on the OUD instance targeted by the `idmConfigTool` and all other OUD instances.

E.2.14.2 Fixing External Changelog Cookie Expiration Issue When Performing Reconciliation with OUD

In some instances, reconciliation with OUD might fail with the following error:

```
Caused By: oracle.ods.virtualization.service.VirtualizationException:
oracle.ods.virtualization.engine.util.DirectoryException: LDAP Error 53 : [LDAP:
error code 53 - Full resync required. Reason: The provided cookie is older than
the start of historical in the server for the replicated domain :
dc=hsgbu,dc=oracle,dc=com]
```

This error is caused when Oracle Identity Manager does not find for a long time any changes on LDAP matching its search filters.

Eventually, the changelog-based query fails because OUD purges its changelogs, and Oracle Identity Manager searches for changelogs older than OUD history. As a result, OUD returns an error.

To troubleshoot this issue, ensure that OUD 11.1.2.2 has been patched with the fix for 18495042, which provides new request control to allow continuing with purged cookie. You can download the patch by navigating to the My Oracle Support web site at:

<https://support.oracle.com>

`libOVD Changelog Plugin` code must be modified to use this new request control, and must set the `supportCookieExceptions` boolean to `FALSE` to avoid error code 53 UNWILLING TO PERFORM.

E.2.15 Disabling the LDAPAddMissingObjectClasses for Users and Roles

In an AD environment, there are some default AD groups that do not have `orclIDXGroup` objectclass. As Oracle Identity Manager requires this objectclass in groups, whenever a full reconciliation is done, Oracle Identity Manager tries to update the LDAP group with the objectclass. AD schema does not allow objectclass modification, and therefore, part of the reconciliation fails, and none of the post handlers are executed. Even if one group does not have the `orclIDXGroup` objectclass,

the post handlers fail for every role in the batch as it is a bulk orchestration and it rolls back on failure. This prevents the handler that published the role to the Top organization from executing, and therefore, none of the roles are published resulting in authorization failures for users having these roles.

As a solution to this problem, disable the Oracle Identity Manager event handler named `LDAPAddMissingObjectClasses`, which tries to add objectclasses for both users and roles. This must be done right after AD is configured for LDAP synchronization and before any full reconciliation is run.

To disable the event handler:

1. Export the `/db/ldapMetadata/EventHandlers.xml` file from MDS, as described in "Migrating User Modifiable Metadata Files" in *Developing and Customizing Applications for Oracle Identity Manager*.
2. Comment out the following lines in the `EventHandlers.xml` file:


```
<action-handler
class="oracle.iam.ldapsync.impl.eventhandlers.LDAPAddMissingObjectClasses"
entity-type="User" operation="CREATE" name="LDAPAddMissingObjectClasses"
stage="postprocess" sync="TRUE" order="1140"/>

<action-handler
class="oracle.iam.ldapsync.impl.eventhandlers.LDAPAddMissingObjectClasses"
entity-type="Role" operation="CREATE" name="LDAPAddMissingObjectClasses"
stage="postprocess" sync="TRUE" order="1040"/>
```
3. Import the `EventHandler.xml` file back to MDS. Make sure that no other file (backup) exists in the import directory while importing the updated file.
4. Restart Oracle Identity Manager Managed Server.

E.2.16 Setting Up LDAP Synchronization With HA Multi-Master Replication (MMR)

When setting up LDAP synchronization, ensure that it is configured to connect with an OID node in the Multi-Master Replication (MMR) and not via Load Balancer (LBR). This is because of the limitation in OID that changenumber is local to the replica and is not global.

If LDAP synchronization needs to point to an alternate replica, then perform the following steps:

1. Stop the incremental reconciliation scheduled jobs.
2. Capture the current changenumber from the new replica.
3. Run full reconciliation from the new replica. Update the Directory Server IT resource to point to the new replica.

In addition, point `libOVD` to the new replica by referring to "[Managing Identity Virtualization Library \(libOVD\) Adapters](#)" on page E-40. You are required to run the `removeLDAPHost()` and then the `addLDAPHost()` WLST commands in order to point to the new replica.

4. Update the incremental reconciliation scheduled jobs with the change number captured in step 2.
5. Enable the incremental reconciliation scheduled jobs.

Configuring Oracle Virtual Directory for Integration with Oracle Access Management Access Manager

This appendix explains how to configure Oracle Virtual Directory for integration with Oracle Access Management Access Manager (Access Manager).

Note: Using Oracle Virtual Directory with Access Manager is *optional*, so the procedures described here are not required as part of the core integration process.

This appendix includes the following sections:

- [Creating and Configuring Oracle Virtual Directory Adapters](#)
- [Using the OAMPolicyControl Plug-In with Oracle Access Manager 10g](#)

Note: You can use Oracle Virtual Directory with most LDAP-enabled technologies. The information contained in this appendix highlights Oracle Virtual Directory features and capabilities that simplify common integrations.

For assistance with other Oracle Virtual Directory integrations, contact your Oracle support representative.

F.1 Creating and Configuring Oracle Virtual Directory Adapters

To configure Oracle Virtual Directory for integration with Access Manager, you use the Oracle Directory Services Manager's Setup for Oracle Access Manager Quick Config Wizard. This Wizard walks you through the steps to create the required Local Store Adapter and the appropriate adapter type (LDAP, Database, or Custom) for the data repository used by Access Manager.

1. Log in to Oracle Directory Services Manager.
2. Select **Advanced** from the task selection bar. The Advanced navigation tree appears.
3. Expand the **Quick Config Wizards** entry in the Advanced tree.
4. Click **Setup for Oracle Access Manager** in the tree. The Setup for Oracle Access Manager screen appears.

5. Enter the namespace for the Local Store Adapter in DN format in the Namespace used for creating Local Store Adapter (LSA) field and click **Apply**. The Adapters screen appears.
6. Create an adapter that is appropriate for the data repository that Access Manager uses. Refer to one of the following sections for instructions:
 - [Section F.1.1, "Creating and Configuring an LDAP Adapter"](#)
 - [Section F.1.2, "Creating and Configuring a Database Adapter"](#)
 - [Section F.1.3, "Creating and Configuring a Custom Adapter"](#)
7. Configure the adapter for the data repository that Access Manager uses by selecting **Adapter** from the Oracle Directory Services Manager task selection bar and then clicking the name of the adapter to configure in the Adapter tree.
 Refer to the following sections for information about configuring each type of adapter:
 - ["Creating and Configuring an LDAP Adapter"](#) on page F-2
 - ["Creating and Configuring a Database Adapter"](#) on page F-10
 - ["Creating and Configuring a Custom Adapter"](#) on page F-12

F.1.1 Creating and Configuring an LDAP Adapter

This section provides instructions for creating and configuring an LDAP Adapter for Access Manager.

F.1.1.1 Creating an LDAP Adapter

To create an LDAP Adapter for Access Manager, refer to "Creating LDAP Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

F.1.1.2 Configuring an LDAP Adapter

After you create the LDAP Adapter, you can configure that adapter by using the procedures described in the following sections:

- [Configuring LDAP Adapter General Settings](#)
- [Managing Certificate Authorities for LDAP Adapters Secured by SSL](#)

Note: For more information, about configuring LDAP adapters, refer to "Configuring LDAP Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*

F.1.1.2.1 Configuring LDAP Adapter General Settings You can configure the general settings for the adapter by clicking the adapter name in the Adapter tree, clicking the **General** tab, setting values for the following fields, and clicking **Apply**:

Root

This field defines the root DN that the adapter provides information for. The DN defined, and the child entries below it, comprise the adapter's namespace. The value you enter in this field should be the base DN value for the returned entries. For example, if you enter dc=mydomain,dc=com in the field, all entries end with dc=mydomain,dc=com.

Active

You can configure an adapter as active (enabled) or inactive (disabled). An adapter configured as inactive does not start during a server restart or an attempted adapter start. Use the inactive setting to keep old configurations available or in stand-by without having to delete them from the configuration. The default setting is active (enabled).

LDAP Server Details

Perform the following procedures to configure the proxy LDAP host information in the LDAP Servers table in the General tab. Each proxy LDAP host must provide equivalent content, that is, must be replicas.

Be careful when specifying only a single host for proxying. Without a failover host, the LDAP Adapter cannot automatically fail over to another host. A single host is suitable when Oracle Virtual Directory is connected to a logical LDAP service by using a load balancing system.

Note: The information in the LDAP Servers table is used only if you set the Use DNS for Auto Discovery parameter to **No**.

To add a proxy LDAP host to the adapter:

1. Click the **Add Host** button.
2. Enter the IP Address or DNS name of the LDAP host to proxy to in the Hosts field.

Note: Oracle Virtual Directory 11g Release 2 (11.1.2.3.0) supports IPv6. If your network supports IPv6 you can use a literal IPv6 address in the Hosts field to identify the proxied LDAP host.

3. Enter the port number the proxied LDAP host provides LDAP services on in the Port field.
4. Enter a number between 0 and 100 in the Percentage field to configure the load percentage to send to the host. If the combined percentages for all of the hosts configured for the adapter do not total 100, Oracle Virtual Directory automatically adjusts the load percentages by dividing the percentage you entered for a host by the total percentage of all hosts configured for the adapter. For example, if you have three hosts configured for the adapter at 20 percent, 30 percent, and 40 percent, Oracle Virtual Directory adjusts the 20 to 22 (20/90), the 30 to 33 (30/90), and the 40 to 44 (40/90).
5. Select the Read-only option to configure the LDAP Adapter to only perform search operations on the LDAP host. The LDAP Adapter automatically directs all modify traffic to read/write hosts in the list.

To delete a proxy LDAP host from the adapter:

1. Click anywhere in the row of the host you want to delete in the Remote Host table.
2. Click the **Delete** button. A confirmation dialog box appears.
3. Click Confirm to delete the proxy LDAP host from the adapter.

To validate a proxy LDAP host connection:

1. Click anywhere in the row of the Remote Host table for the host you want to validate the connection for.

2. Click the **Validate** button. The connection to the proxy LDAP host must be validated for the adapter to proxy the LDAP host.

Use SSL/TLS

Enabling this option secures the communication between the LDAP Adapter and the proxy LDAP hosts using SSL/TLS.

See: ["Managing Certificate Authorities for LDAP Adapters Secured by SSL"](#) on page F-9 for information on Certificate Authorities.

SSL Authentication Mode

If you select (enable) the **Use SSL/TLS** option, choose the SSL authentication mode to use for securing the adapter by selecting an option from the SSL Authentication Mode list. The SSL Authentication Mode setting is functional only when the Use SSL/TLS option is enabled.

Failover Mode

If set to **Sequential**, the first host specified in LDAP Servers table is used unless a failure occurs. If a failure occurs, the next host is tried. Sequential failover is often used for fail-over between geographies. In sequential failover, the LDAP Adapter attempts to use the designated host until it fails. At this point, it would fail-over to an equivalent host available in another data center or continent.

If set to **Distributed**, each new connection made is load balanced through the list defined by the LDAP Servers table. Distributed failover is most often used when proxying a set of LDAP hosts that are typically in the same data center or are equally available in terms of network performance.

Note: If a remote host's network fails, a delay of several minutes may occur in Oracle Virtual Directory because of platform specific TCP socket timeout settings. However, Oracle Virtual Directory failover is operating properly and no data is lost during the delay.

Extended Trying

Enable this option to force the Oracle Virtual Directory server to continue trying to connect to the last host listed in the LDAP Servers table for new incoming requests on the adapter even after it has been determined that the connection to the host failed. When enabled, the adapter's **Heartbeat Interval** setting is ignored regardless if a connection to the host has failed and the host will not be removed from the LDAP Servers table. Some environments with distributed directories may prefer to disable the **Extended Trying** option with the **Routing Critical** setting to quickly return partial results at that time. The default setting is enabled.

Heartbeat Interval

The LDAP Adapter periodically verifies the availability of each the hosts defined in the LDAP Servers table. Any currently disabled host can be resurrected or a currently active host that fails the TCP/IP connection test is labeled as **false** during this verification cycle. The Heartbeat Interval parameter specifies the number of seconds between verification passes. Setting a value too low can cause unnecessary connections to the remote directory. Setting a value too high can mean extended time for recovery detection when you have a failure. For production environments, Oracle suggests starting with a value of 60 seconds, then making adjustments as needed.

Operation Timeout

The amount of time in milliseconds the server waits for an LDAP request to be acknowledged by a remote host. If the operation fails, the LDAP Adapter automatically tries the next server in the Remote Host table. The minimum configurable value is 100. Settings that are too low can cause erroneous failures on busy servers. For production environments, Oracle suggests starting with a value of 5000, which is 5 seconds, then making adjustments as needed.

Max Pool Connections

A tuning parameter that enables you to control how many simultaneous connections can be made to a single server. For production environments, Oracle suggests starting with a value of 10 connections, then making adjustments as needed.

Max Pool Wait

The maximum amount a time in milliseconds that an LDAP operation waits to use an existing connection before causing the LDAP Adapter to generate a new connection. For production environments, Oracle suggests starting with a value of 1000, which is 1 second, then making adjustments as needed.

Max Pool Tries

Maximum number of times an operation waits for an LDAP connection before overriding the Max Pool Connections parameter to generate a new connection. Maximum time is a function of multiplying Max Pool Wait time by the number of tries. If pool wait is 1 second, and 10 is the maximum number of tries, then if after 10 seconds an LDAP connection is not available in the normal pool, the pool will be expanded to handle the extended load. To prevent pool expansion beyond Max Pool Connections, set the number of tries to a high number. For production environments, Oracle suggests starting with a value of 10, then making adjustments as needed.

Use Kerberos

If you enable the **Use Kerberos** option:

You must set the Pass Through option to **BindOnly** because the Kerberos authentication can only be used to validate credentials and not passed to the back-end server for any other operation.

The RDN value must be the same as the Kerberos principal name, for example, sAMAccountName in Active Directory. This may mean that the bind DN for a Kerberos bind is not the actual user DN. For example, if the user DN is cn=Jane Doe, cn=users, dc=mycompany, dc=com but the sAMAccountName is jdoe, the bind DN with the Use Kerberos option enabled is cn=jdoe, cn=users, dc=mycompany, dc=com.

You must create a krb5.conf file and place it in the Oracle Virtual Directory's configuration folder. The krb5.conf has the following properties:

Table F-1 Properties in the krb5.conf File

Property	Description
default_realm	The default domain used if not supplied by the mapping. For example, if a user binds as uid=jsmith, ou=people, dc=myorg, dc=com, this will be treated as jsmith@myorg.com. If the mapped namespace does not include a domain component (dc) based root, this value is substituted instead.
domain_realm	Defines a mapping between a domain and a realm definition. For example: .oracle.com = ORACLE.COM
realms	Defines one or more realms, for example: ORACLE.COM = { ... }

Table F-1 (Cont.) Properties in the krb5.conf File

Property	Description
kdc	The DNS name of the server running the Kerberos service for a particular realm definition.

Kerberos binds use the Kerberos libraries provided in the standard Java package. The Kerberos libraries use the krb5.conf file, which is not currently synchronized with Oracle Virtual Directory LDAP Adapter settings. The default libraries control Kerberos fail-over. Refer to Java documentation for more information on fail-over and advanced krb5.conf file configurations.

Note: If a Microsoft Active Directory server is in the process of shutting down (either stopping or rebooting) and Oracle Virtual Directory tries to connect to it, Active Directory may not validate the credential and may return a `Client not Found in Kerberos Database` error message instead of returning a Key Distribution Center (Domain Controller) connection error.

The end-user should attempt to login again and assuming that either the Active Directory server is available or Key Distribution Center fail-over is enabled, successful authentication should be returned.

Kerberos Retry

If you enable the **Use Kerberos** option, you can use the **Kerberos Retry** option to control whether Oracle Virtual Directory should retry logging in after failed authentication attempts. If you enable the **Kerberos Retry** option and authentication fails, Oracle Virtual Directory reloads the krb5.conf file and retries the log in.

Note: If you identified multiple Active Directory servers in a single Kerberos realm in the krb5.conf file, do not enable the **Kerberos Retry** option, as enabling the retry may disrupt fail-over functionality.

Use DNS For Auto Discovery

Instead of configuring specific proxy LDAP hosts in the LDAP Servers table, you can use this option to instruct Oracle Virtual Directory to use DNS to locate the appropriate LDAP servers for the remote base defined, also known as serverless bind mode. The LDAP Adapter supports the following modes of operation:

- **No:** Use the LDAP Servers table configuration—no serverless bind.
- **Standard:** Use standard DNS lookup for a non-Microsoft server. All servers are marked as read/write, so enabling the **Follow Referrals** setting is advised to allow for LDAP write support.
- **Microsoft:** The DNS server is a Microsoft dynamic DNS and also supports load-balancing configuration. If proxying to a Microsoft dynamic DNS server, this is preferred setting because of Oracle Virtual Directory's ability to auto-detect read/write servers compared to read-only servers.

Note: Remote base should have a domain component style name when using this setting, for example, dc=myorg,dc=com. This name enables Oracle Virtual Directory to locate the LDAP hosts within the DNS service by looking up myorg.com.

The following fields appear in the **Settings** section of the **General** tab:

Remote Base

The location in the remote server directory tree structure to which the local Oracle Virtual Directory root suffix corresponds. This is the location in the remote directory under which Oracle Virtual Directory executes all searches and operations for the current adapter. The LDAP Adapter applies an automatic mapping of all entries from the remote base to the adapter root base.

DN Attributes

List of attributes to be treated as DNs for which namespace translation is required, such as member, uniquemember, manager. For example, when reading a group entry from a proxied directory, Oracle Virtual Directory automatically converts the DN for the group entry itself and the uniquemember or member attributes if these attributes are in the DN Attributes list.

Note: Translate only those attributes you know must be used by the client application. Entering all possible DN attributes may not be necessary and can consume some a small amount of additional CPU time in the proxy.

To add attributes to the DN Attributes list:

1. Click **Add**. The Select DN Attribute dialog box appears.
2. Select the attribute you want to add.
3. Click **OK**.

Escape Slashes

When a / character is encountered in a directory, Oracle Virtual Directory can optionally escape the slashes with back-slashes \ character. Some directory server products accept un-escaped slashes, while others reject them. Selecting this setting enables escaping of slashes.

Follow Referrals

Enabling this setting causes the LDAP Adapter to follow (chase) referrals received from a source directory on the client's behalf. If disabled, the referral is blocked and not returned to the client.

The following list summarizes the LDAP Adapter's behavior with different settings in relation to the send managed DSA control in LDAP operations setting:

- If the LDAP Adapter's Follow Referrals is set to **Enabled (true)**, and Send Managed DSA Control in LDAP Operations is also set to **True**, Oracle Virtual Directory does not chase the referral entries, but it returns them back to the client.
- If the LDAP Adapter's Follow Referrals is set to **Enabled (true)**, but Send Managed DSA Control in LDAP Operations is set to **False**, Oracle Virtual Directory chases the referral entries.

- If the LDAP Adapter's Follow Referrals is set to **Disabled (false)**, but Send Managed DSA Control in LDAP Operations is set to **True**, Oracle Virtual Directory does not chase the referral entries, but it returns them back to the client.
- If the LDAP Adapter's Follow Referrals is set to **Disabled (false)**, and Send Managed DSA Control in LDAP Operations is also set to **False**, Oracle Virtual Directory does not chase the referral entries and does not return them back to client.

Proxied Page Size

If enabled, this setting allows the proxy to use the paged results control with a proxied directory. Enabling this setting is most often used when a directory limits the number of results in a query. This setting is used on behalf of and transparently to Oracle Virtual Directory's clients.

The following fields appear in the Credential Processing section of the General tab:

Proxy DN

The default DN that the LDAP Adapter binds with when accessing the proxied directory. Depending on the **Pass-through Mode** setting, this DN is used for all operations, or only for exceptional cases such as pass-through mode. The form of the distinguished name should be in the form of the remote directory. Empty values are treated as Anonymous.

Proxy Password

The authentication password to be used with the **Proxy DN** value. To set the password, enter a value in clear text. When loaded on the server, the value is automatically hashed with a reversible mask to provide additional security, for example, {OMASK}jN63CfzDP8XrnmauvsWs1g==.

Pass-through Mode

To pass user credentials presented to Oracle Virtual Directory to the proxied LDAP server for all operations, set to **Always**. To pass user credentials to the proxied LDAP server for bind only and use the default server credentials for all other operations, set to **Bind Only**. To use the Proxy DN credentials for all operations, set to **Never**.

Note: In some situations when pass-through mode is set to **Always**, the LDAP Adapter may still use the Proxy DN. This occurs when the user credential cannot be mapped, for example, from another adapter namespace, or is the root account.

If defining multiple adapters to different domain controllers within a Microsoft Active Directory forest, you can program the LDAP Adapter to proxy credentials from other adapters (that is, two or more adapters pointing to the same Active Directory forest) by using the **Routing Bind-Include** setting.

The following fields appear in the Ping Protocol Settings section of the General tab:

The Ping Protocol Settings provide options for how to determine when a source LDAP directory server that is not responding becomes available. If multiple source directory servers are configured, Oracle Virtual Directory identifies the non-responsive servers and performs subsequent operations against the next available server.

Ping Protocol

Select either **TCP** or **LDAP** as the protocol Oracle Virtual Directory should use to ping source directory servers. Select **LDAP** if the source directory server is using SSL.

Note: While the **TCP** protocol option is faster than the **LDAP** option, it may produce an inaccurate response from the source directory server if its network socket is available, but its LDAP server process is unavailable.

Ping Bind DN

If you select **LDAP** as the Ping Protocol, identify the DN to use for the LDAP bind.

Ping Bind Password

If you select **LDAP** as the Ping Protocol, identify the password for the DN specified in the Ping Bind DN setting.

F.1.1.2.2 Managing Certificate Authorities for LDAP Adapters Secured by SSL In some situations, SSL connections from Oracle Virtual Directory to the SSL port of an LDAP Adapter can fail and the following message may appear:

```
Oracle Virtual Directory could not load certificate chain
```

Two examples of situations when this may happen are when:

- you create a new LDAP Adapter secured by SSL and use an untrusted Certificate Authority
- a certificate for an existing LDAP Adapter secured by SSL expires and the new certificate is signed by an untrusted Certificate Authority

To resolve this issue, import the LDAP server certificate *and* the Root Certificate Authority certificate used to sign the LDAP server certificate, into the Oracle Virtual Directory server so it knows the certificates are trusted.

Use the following `keytool` command and an appropriate alias **all on one command line**:

```
ORACLE_HOME/jdk/jre/bin/keytool -import -trustcacerts
-alias "NEW_CA" -file PATH_TO_CA_CERTIFICATE
-keystore ORACLE_INSTANCE/config/OVD/ovd1/keystores/adapters.jks
```

Using LDAP Adapters with Microsoft Active Directory and Microsoft Certificate Services

By default, Microsoft Certificate Services automatically update expired Active Directory SSL certificates. However, client applications are not normally notified of this change. If this happens, the Oracle Virtual Directory LDAP Adapter connected to an updated Active Directory server stops functioning. If this occurs, use Oracle Directory Services Manager to configure the LDAP Adapter to import trusted certificates and the adapter should begin to function again.

Note: Active Directory servers only support SSL server authentication. For this reason, you are only required to load the root CA certificate of the Certification Authority that signed the Active Directory server certificate to the OVD keystore. If the Active Directory server certificate is also loaded, then based on the standard behavior of Sun JSSE, OVD does not execute an expiry check of the trusted certificate.

Consequently, if the certificate sent by the back-end LDAP server is stored as a trusted certificate in the OVD keystore, no expiry check is executed.

F.1.2 Creating and Configuring a Database Adapter

This section describes how to create and configure a Database adapter for Access Manager.

F.1.2.1 Creating a Database Adapter

To create a Database Adapter for Access Manager, refer to "Creating Database Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

F.1.2.2 Configuring a Database Adapter

After you create the Database Adapter, you can configure the general settings for that adapter by clicking the adapter name in the Adapter tree, clicking the **General** tab, setting values for the following fields, and clicking **Apply**:

Note: For more information, about configuring LDAP adapters, refer to "Configuring Database Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

Root

This field defines the root DN that the adapter provides information for. The DN defined, and the child entries below it, comprise the adapter's namespace. The value you enter in this field should be the base DN value for returned entries. For example, if you enter `dc=mydomain,dc=com` in the field, all entries end with `dc=mydomain,dc=com`.

Active

An adapter can be configured as active (enabled) or inactive (disabled). An adapter configured as inactive does not start during a server restart or an attempted adapter start. Use the inactive setting to keep old configurations available or in stand-by without having to delete them from the configuration. The default setting is active.

The following fields appear in the Connection Settings section of the General tab:

URL Type

Select an option from the following URL Type list. Some fields for Database Adapter connection settings differ depending on which option you choose. After selecting an option, continue configuring the Connection Settings by setting the fields listed for each option.

- **Use Custom URL:** Select this option to connect Oracle Virtual Directory a custom database.

Enter the JDBC driver class name for the database in the JDBC Driver Class field.

Enter the URL that Oracle Virtual Directory should use to access the database in the Database URL field.

Enter the user name that the Database Adapter should use to connect the database in the Database User field.

Enter the password for the user name you entered in the Database User field in the Password field. Oracle Virtual Directory replaces the value you enter in this field with a reversible masked value upon startup.

- **Use Predefined Database:** Select this option to connect to a predefined database. The predefined databases appear in the Database Type list after selecting Use Predefined Database from the URL Type list. If you are unsure if Oracle Virtual Directory has predefined your type of database, select Use Predefined Database from the URL Type list and verify if your database is listed in the Database Type list. If your database is listed in the Database Type list, continue with the following steps. If your database is not listed, select **Use Custom URL** from the URL Type list and perform the steps for using a custom URL.

Select the type of your database from the Database Type list. After selecting the database type, the JDBC Driver Class and Database URL fields are populated with the appropriate information for the database.

Enter the IP Address or DNS host name of the database in the Host field.

Enter the port number the database listens on in the Port field.

Enter the name of the database, for example, the Oracle SID, in the Database Name field.

Enter the user name that the Database Adapter should use to connect the database in the Database User field.

Enter the password for the user name you entered in the Database User field in the Password field. Oracle Virtual Directory replaces the value you enter in this field with a reversible masked value upon startup.

The following fields appear in the Settings section of the General tab:

Ignore Modify Objectclass

Since objectclasses in the database are logical objects and do not map directly to a table column in the mapping, modifications to the objectclass attribute can cause errors. If the **Ignore Modify Objectclasses** option is enabled, the Database Adapter removes any references to the objectclass attribute so that errors are *not* sent to the client application, that is, they are ignored. If the **Ignore Modify Objectclasses** option is not selected, error messages *are* sent to the client application.

Include Object Class Super Classes

This setting causes the Database Adapter to list objectclass parent classes along with the main objectclass in the objectclass attribute. Disable this setting when you want to emulate Microsoft Active Directory server schema. For most scenarios, it is useful to enable this setting so that objectclass=xxx queries can be executed against parent objectclass values.

Enable Case Insensitive Search

Enabling (selecting) the **Enable Case Insensitive Search** option makes the search case insensitive for case insensitive LDAP attributes, such as uid. Oracle Virtual Directory uses UPPER in the SQL query when **Enable Case Insensitive Search** is enabled. If the database cannot maintain functional indexes, such as for Oracle TimesTen or MySQL databases, then you should disable the **Enable Case Insensitive Search** option. When the **Enable Case Insensitive Search** is disabled, Oracle Virtual Directory performs case

sensitive searches and does not use UPPER in the SQL query. The default value for **Enable Case Insensitive Search** is Enable.

Maximum Connections

This setting defines the maximum connections the Database Adapter may make with the database.

Connection Wait Timeout

This setting determines how much time (in seconds) the Database Adapter should wait before timing-out when trying to establish a connection with the database.

The following fields appear in the DB/LDAP Mapping section of the General tab:

Used Database Tables

This field displays the database tables the Database Adapter is set to use. To add a database table, click the **Add** button, navigate to the table file, select it and click **OK**.

The following fields appear in the Object Classes section of the General tab:

Object Classes

This field displays object classes and their RDNs that map to the database tables. To add an Object Class Mapping, click the **Create** button, select the appropriate object class from the Object Class list, enter an RDN value for the object class in the RDN field, and click **OK**.

Note: For more information, about configuring Database adapters, refer to "Configuring Database Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

F.1.3 Creating and Configuring a Custom Adapter

This section describes how to create and configure a Custom adapter for Access Manager.

F.1.3.1 Creating a Custom Adapter

To create a Custom Adapter for Access Manager, refer to "Creating Custom Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

F.1.3.2 Configuring Custom Adapters

After you create the Custom Adapter you can configure the general settings for that adapter by clicking the adapter name in the Adapter tree, clicking the **General** tab, setting values for the following fields, and clicking **Apply**:

Note: For more information, about configuring LDAP adapters, refer to "Configuring Custom Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

Root

This field defines the root DN that the adapter provides information for. The DN defined, and the child entries below it, comprise the adapter's namespace. The value you enter in this field should be the base DN value for returned entries. For example, if you enter dc=mydomain,dc=com in the field, all entries end with dc=mydomain,dc=com.

Active

An adapter can be configured as active (enabled) or inactive (disabled). An adapter configured as inactive does not start during a server restart or an attempted adapter start. Use the inactive setting to keep old configurations available or in stand-by without having to delete them from the configuration. The default setting is active.

F.2 Using the OAMPolicyControl Plug-In with Oracle Access Manager 10g

Note: This section is only relevant to customers that are still running Oracle Access Manager 10g. The OAMPolicyControl plug-in does not work with Access Manager 11g.

Oracle Virtual Directory provides the OAMPolicyControl plug-in to simplify the Oracle Virtual Directory-Access Manager 10g integration for applications that use LDAP for authentication and want to use Access Manager policy controls, but cannot integrate with Access Manager.

Before deploying the OAMPolicyControl plug-in, you must:

- Set the Bind pass-through settings to Never for any LDAP Adapters that are using the Access Manager policy configuration.

The plug-in handles all authentications and uses proxy credentials to perform all operations.

- Configure different adapters for Access Manager.

These adapters should use the OAMPolicyControl plug-in to use Access Manager policies. If you deploy these adapters on the same Oracle Virtual Directory server, you must configure one of the following options:

- Use a different LDAP namespace for each adapter. An Access Manager adapter namespace must be independent from the namespaces used by general purpose LDAP clients.
- Use an Oracle Virtual Directory view, with accessibility criteria that distinguishes requests for different Access Manager adapters.

- Configure the Access Manager Access Server by:

- Creating a proxy resource that corresponds to Oracle Virtual Directory.
- Disabling the policy domains for Identity Server and Access Server because the plug-in does not cache the OBSSO Cookie.

- Configure the AccessSDK as follows:

- Configure an AccessSDK installation for the Access Manager Access Server by using AccessServerSDK\oblix\tools\configureAccessGate.
- Configure the opmn to start the Oracle Virtual Directory component by pointing the -Djava.library.path to the AccessSDK installation.

Edit the INSTANCE_HOME/config/OPMN/opmn/opmn.xml file as follows:

```
<ias-component id="ovd1">
  <process-type id="OVD" module-id="OVD">
    <module-data>
      <category id="start-options">
        <data id="java-bin" value="$ORACLE_HOME/jdk/bin/java"/>
        <data id="java-options" value="-server -Xms512m -Xmx512m
```

```

-Dvde.soTimeoutBackend=0
-Doracle.security.jps.config=$ORACLE_
INSTANCE/config/JPS/jps-config-jse.xml
-Djava.library.path=AccessSDK_install_
dir/AccessSDK/AccessServerSDK/oblix/lib/" />
  <data id="java-classpath" value="$ORACLE_
HOME/ovd/jlib/vde.jar$: $ORACLE_HOME/jdbc/lib/ojdbc6.jar" />
  </category>
</module-data>
<stop timeout="120" />
</process-type>
</ias-component>

```

- Copy the jobaccess.jar file from AccessSDK_install_dir/AccessServerSDK/oblix/lib to ORACLE_HOME/ovd/plugins/lib.

Note: Failure to successfully complete the preceding prerequisite configurations will cause the Oracle Virtual Director to generate a NoClassDefFound error.

F.2.1 Configuration Parameters

The OAMPolicyControl plug-in has the following configuration parameters:

Note: All of the following configuration parameters—except for useAccessAuthPolicy—are required to deploy the OAMPolicyControl plug-in.

resourceIdOVD

Identifies the proxy resource for Oracle Virtual Directory that the Access Manager server configures. For example: //host:port/ovd_proxy_resource.

identityproxyid

Used for authentication against the Identity Server, the identityproxyid parameter identifies the value of the administrator's usernameAttribute.

install_dir

Identifies the AccessSDK installation directory containing the required libraries. For example: AccessSDK_INSTALL_DIRECTORY/AccessServerSDK/.

OrclOVDEncryptedproxypasswd

Administrator password for authentication against Identity Server.

identityEndpointAddress

Identifies the URL corresponding to the listening endpoint of the Identity Server's um_modifyUser web service. For example:
http://host:port/identity/oblix/apps/userservcenter/bin/userservcenter.cgi

usernameAttribute

Identifies the attribute configured to be the Login attribute of the Identity Server. For example, uid or genUserId.

useAccessAuthPolicy

An optional and case-insensitive parameter, useAccessAuthPolicy determines usage of the Access Manager server's authorization policies while accessing the proxy resource. Supported values are True and False. The default setting is False.

A

Access Manager, F-1
 and Oracle Adaptive Access Manager, 3-1
 and Oracle Identity Manager, 3-1
 creating a custom adapter, F-12
 creating Database adapter, F-10
 creating LDAP adapter, F-2
Access Manager and OAAM TAP Integration, 3-8
Access Manager, OAAM, and OIM integration, 3-1
Access Manager-OAAM TAP Integration, C-8
Account Lock and Unlock, 1-27
 processing flow, 1-27
actions, 3-4, C-5
adapters
 creating custom, F-12
 creating Database, F-10
 creating LDAP, F-2
 custom settings, F-12
 Database settings, F-10
 LDAP certificates, F-9
 LDAP settings, F-2
advanced integration
 procedure, C-17
alerts, C-5

B

Basic Integration
 prerequisites, C-12

C

Challenge Reset, 1-29
 processing flow, 1-29
Challenge Setup, 1-28
 processing flow, 1-28
Changelog plug-in
 configuration parameters, E-34
 description, E-33
Changelog plug-ins, E-33
configuration parameters
 Changelog plug-in, E-34
 OAMPolicyControl plug-in, F-14
 UserManagement plug-in, E-31
configure

LDAP authentication, E-43
configureOAAM WLST command
 OAAM-OAAM integration, C-54
credentials
 using Pass-through mode, F-8
custom adapters
 for Access Manager, F-12

D

Deployment Options for Strong Authentication, 3-2
Domain Agents, 1-16

F

flow
 Account Lock and Unlock, 1-27
 Challenge Reset, 1-29
 Challenge Setup, 1-28
 Change Password, 1-24
 Forgot Password, 1-25
 password management, 1-22
 Self-Registration, 1-23
Forgot Password, 1-25
 processing flow, 1-25
fraud rules, 3-9, C-10

I

identity store, 1-2
 multiple directories, 7-8
 split, 7-2
IdM configuration tool, D-1
idmConfigTool, E-13
IDMDomain Agents
 and Webgates, 1-16
integration
 OAAM with Access Manager, C-1
 Oracle Identity Manager and LDAP, 1-2

J

Java component
 defined, 1-14

K

knowledge-based authentication (KBA), 3-7, C-7
krb5.conf, F-5

L

LDAP, 1-2
LDAP authentication
 configuring, E-43
LDAP identity store, 1-2
 provisioning, 1-4
 reconciliation, 1-5

N

native integration
 procedure, C-12

O

OAAM actions, 3-4
OAAM alerts, 3-4
OAAM integration with Access Manager, C-1
OAAM Server as a Partner Application, C-26
OAMAgent, 1-16
 default in OHS, 1-16
oam-config.xml file, C-15, C-59
OAM-OAAM integration
 configureOAAM WLST command, C-54
OAMPolicyControl plug-in
 configuration parameters, F-14
 description, F-13
Oracle Access Manager
 and Oracle Adaptive Access Manager, 1-16, 3-2
 and Oracle Identity Federation, 6-1
 and Oracle Identity Federation, 1-17
 and Oracle Identity Manager, 1-16, 2-2, 3-2, 5-1
 with Oracle Adaptive Access Manager and Oracle
 Identity Manager, 3-1
Oracle Adaptive Access Manager, 1-16
 properties for Oracle Identity Manager, 3-17
 resource protection, C-35, C-36
Oracle Adaptive Access Manager integration with
 Access Manager, C-1
Oracle Adaptive Access Manager Snapshot, C-22
Oracle Enterprise Manager
 defined, 1-14
Oracle Enterprise Manager Fusion Middleware
 Control
 See Oracle Enterprise Manager
Oracle Fusion Middleware farm
 defined, 1-14
Oracle Fusion Middleware home
 defined, 1-13
Oracle home
 defined, 1-13
Oracle HTTP Server
 and OAMAgent, 1-16
 and WebGate, 1-16
Oracle Identity Federation, 1-17, 6-1

SP Integration Engine, 6-1
Oracle Identity Manager, 1-16
 configuring properties for three-way
 integration, 3-16
 credentials in Credential Store Framework, 3-20
 integration with Oracle Adaptive Access
 Manager, 3-16
 LDAP integration, 1-2
 password administration, 3-1
 WebGate credentials, 3-20
Oracle instance
 defined, 1-13
OVD
 configuring for Access Manager, F-1

P

Password Change, 1-24
 processing flow, 1-24
password management, 3-3
 processing flow, 1-22
 three-way integration, 3-3
 with Oracle Identity Manager, 1-22
plug-ins
 Changelog, E-33
 Java
 UserManagement, E-31
 OAMPolicyControl, F-13
plug-ins, Java
 Changelog, E-33
provisioning
 Oracle Identity Manager to LDAP, 1-4

R

reconciliation
 LDAP to Oracle Identity Manager, 1-5

S

Self-Registration, 1-23
 processing flow, 1-23
SP Integration Engine
 for Oracle Identity Federation, 6-1
Step Up Authentication, 1-18, 3-10, C-10
strong authentication, C-17
system component
 defined, 1-14

T

three-way integration
 procedure, 3-14
Trusted Authentication Protocol (TAP), 3-14, C-26

U

UserManagement plug-in
 configuration parameters
 , E-31
 description, E-31

W

- Webgates, 1-16
 - and IDMDomain Agents, 1-16
- WebLogic
 - Administration Server, 1-14
 - Managed Server, 1-14
- WebLogic Server
 - home defined, 1-13
- WebLogic Server domain
 - defined, 1-14

