Oracle® Fusion Middleware

Integration Guide for Oracle Identity Management Suite

11*g* Release 2 (11.1.2)

E27123-03

November 2012

Describes how to integrate Oracle Identity Management components.

ORACLE®

Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite, 11*g* Release 2 (11.1.2)

E27123-03

Primary Authors: Debapriya Datta, Ellen Desmond, Gail Flanegin, KC Francis, Trish Fuzesy, Priscilla Lee, Vinaye Misra

Contributing Authors: Damien Carru, Pratima Gogineni, Ari Kermaier, Gopal Kumarappan, Maya Neelakandhan, Olaf Stullich, Dawn Tyler, Jingjing Wei, Ramana Turlapati, Catherine Wong

Contents

2 Using the idmConfigTool Command

5 Integrating Oracle Internet Directory with Access Manager

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

7 Integrating Access Manager and Oracle Identity Manager

8 Integrating Access Manager and Oracle Adaptive Access Manager

9 Integrating Access Manager, OAAM, and OIM

List of Figures

List of Tables

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 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:

- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*

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.

Convention	Meaning
italic	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 November 2012 Documentation Refresh for 11*g* 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 11*g* 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 11*g* Release 2 (11.1.2) with Oracle Identity Federation 11*g* Release 1 (11.1.1). See Section 10.2.

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

11*g* 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 11*g* Release 2 (11.1.2)

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

Part I

IdM Integration Topology and Tools

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

This part contains the following chapters:

1 Introduction

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

The chapter contains these topics:

- Section 1.1, "Prerequisites to Integration"
- Section 1.2, "Integration Topologies"
- Section 1.3, "About Oracle Identity Management Components"
- Section 1.4, "Integration Quick Links"
- Section 1.5, "Common Integration Scenarios"
- Section 1.6, "System Requirements and Certification"
- Section 1.7, "Using My Oracle Support for Additional Troubleshooting Information"

Before proceeding with the topics in this chapter, refer to the following documents for background information about Oracle Identity Management:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Administrator's Guide*

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.

For details about installing Oracle Identity Management components, see:

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

Installation Roadmap

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

Deployment Topologies

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

To learn more about the range of topologies supported in this document, see Section 1.2.

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 topologies

  This topology supports integration between suite components, in an environment where each component runs on at most one node.

- Enterprise integration topologies

  This topology is meant for configuring integration between suite components in an enterprise environment. Each component may run on one or more nodes.

Topologies Described in this Document

This book is dedicated to single-node integration topologies. Use the procedures described in this book when deploying Oracle Identity Management in an environment where each component runs on a single 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 Topologies

This section describes the component topologies that form the basis of this document. It also explains the tiers that make up each topology.

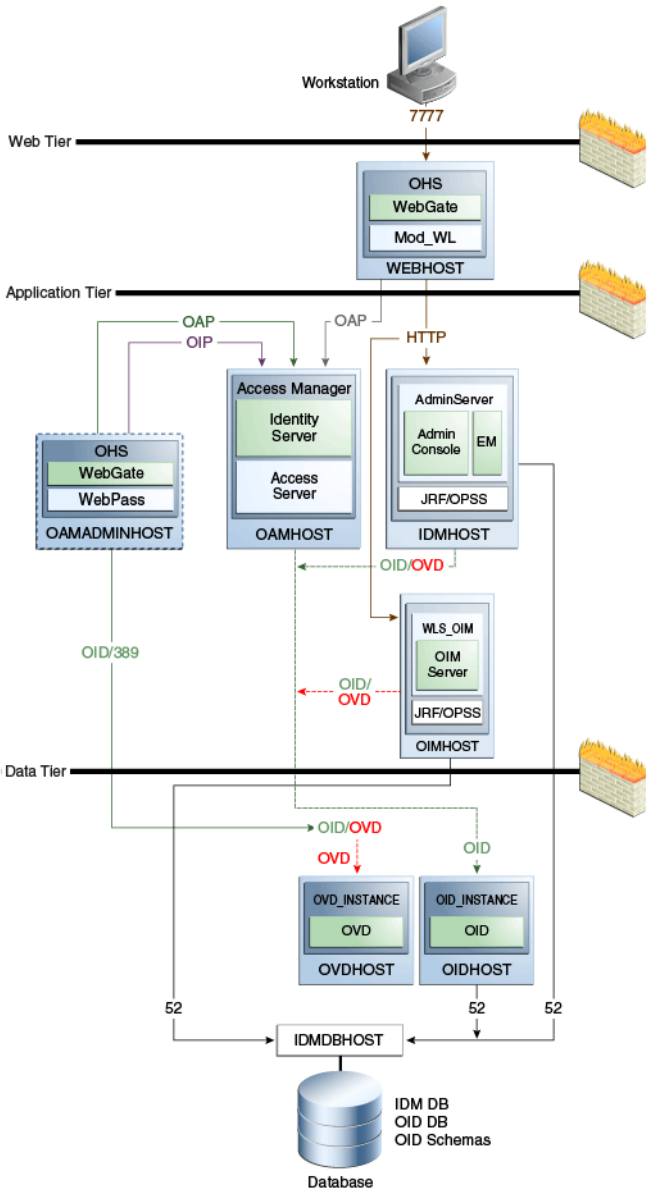
See Also: Table 1–1 for definitions of acronyms used in this section.

1.2.1.1 Single Domain Architecture

In the single-domain architecture, the Oracle Access Management Access Manager and Oracle Identity Manager servers are configured on the same Oracle WebLogic Server.

Figure 1–1 shows the basic single-domain integration topology:

Figure 1–1 Basic Integration Topology with One Administration Server



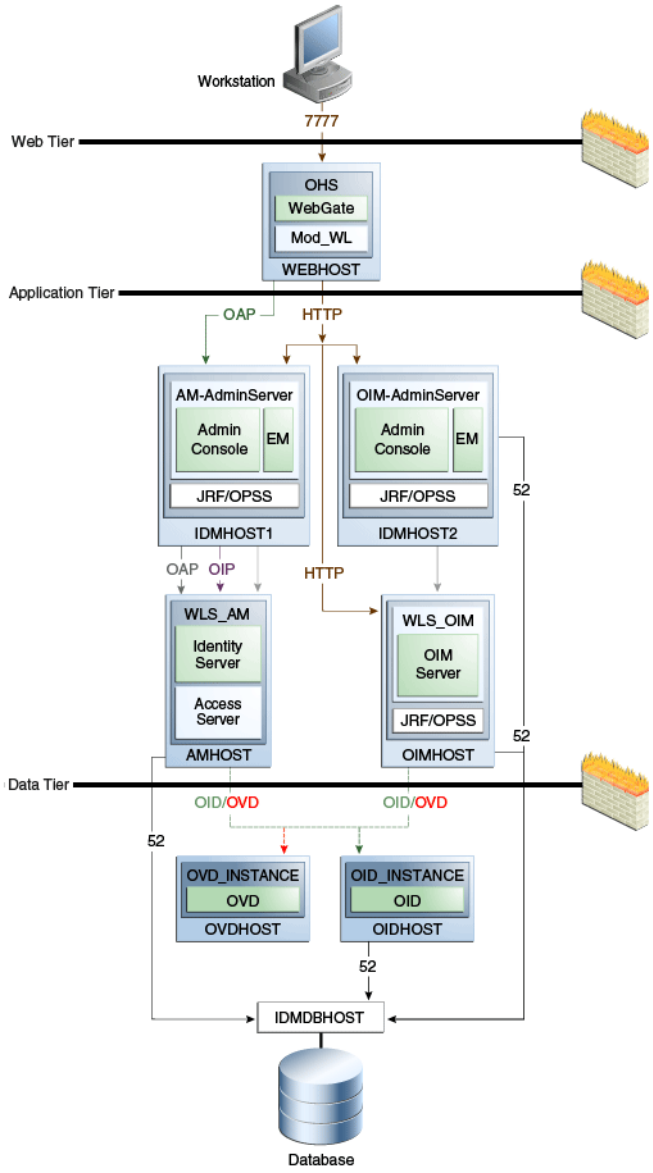
In this topology all the IdM components are configured in the same WebLogic domain, so they are administered by one WebLogic administration server.

> **Note:** The figure shows some representative ports. For a complete list, see About Firewalls and Ports in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

1.2.1.2 Double (Split) Domain Architecture

Figure 1–2 shows a variation of the previous integration topology. Here, the Access Manager and Oracle Identity Manager servers are configured on separate WebLogic domains:

Figure 1–2 Basic Integration Topology with Two Administration Servers



In this topology the Access Manager server (AMHOST) and the Oracle Identity Manager server (OIMHOST) are configured in separate WebLogic domains, so each is administered by its own administration server.

> **Note:** The figure shows some representative ports. For a complete list, see About Firewalls and Ports in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

1.2.1.3 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.

1.2.1.4 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.

1.2.1.5 Understanding the Application Tier

The application tier is the tier where Java EE applications are deployed. Products such as Oracle Identity Manager, 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.

1.2.1.6 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`), 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 either use Oracle Virtual Directory to present that information or use Oracle Directory Integration Platform to synchronize the users and groups from the other directory to Oracle Internet Directory.

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 *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity 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 12.

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.
IdM Diagnostic Tool	A command-line tool to verify the health of integrated identity management components.
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.

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

Term	Definition
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.
Oracle WebLogic Server domain	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. Managed Servers in a WebLogic Server domain can be grouped together into a cluster. An Oracle WebLogic Server domain is a peer of an Oracle instance. Both contain specific configurations outside of their Oracle homes. 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.
system component	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.
Java component	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.

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

Term	Definition
Oracle Fusion Middleware farm	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. 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.
Oracle Identity Management	The suite of identity and access management components in Oracle Fusion Middleware. See Section 1.3 for details.
WebLogic Administration Server	The Administration Server is the central point from which you configure and manage all resources in the WebLogic domain.
WebLogic Managed Server	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.

1.3 About Oracle Identity Management Components

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

- Oracle Internet Directory
- Oracle Virtual Directory
- Oracle Access Management Access Manager
- Oracle Identity Manager
- Oracle Adaptive Access Manager
- Oracle Access Management Identity Federation
- Oracle Identity Navigator

1.3.1 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:

- Chapter 3, "Enabling LDAP Synchronization in Oracle Identity Manager"
- Chapter 5, "Integrating Oracle Internet Directory with Access Manager"

1.3.2 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:

- Chapter 6, "Configuring Oracle Virtual Directory for Integration with Oracle Access Management Access Manager"

1.3.3 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 8, "Integrating Access Manager and Oracle Adaptive Access Manager"
- Chapter 9, "Integrating Access Manager, OAAM, and OIM"
- Chapter 10, "Integrating with Identity Federation"

1.3.3.1 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 *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

1.3.4 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 9, "Integrating Access Manager, OAAM, and OIM".

1.3.5 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.

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

- Chapter 8, "Integrating Access Manager and Oracle Adaptive Access Manager".
- Chapter 9, "Integrating Access Manager, OAAM, and OIM".

1.3.6 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 11*g* 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 10, "Integrating with Identity Federation".

1.3.7 Oracle Identity Navigator

Oracle Identity Navigator is a web-based application that you access through a browser. You can use it to access consoles for Access Manager, Oracle Adaptive Access Manager, Oracle Identity Manager, Directory Services (ODSM), and other Oracle Identity Management components.

For details about integration with Access Manager, see Chapter 11, "Integrating with Oracle Identity Navigator".

1.4 Integration Quick Links

Table 1–2 provides links to the integration procedures described in this document.

Table 1–2 Links to Integration Procedures

Components to Integrate	Link
Post-install LDAP Synchronization with Oracle Identity Manager	Chapter 3
Oracle Virtual Directory and Oracle Identity Manager	Chapter 4
Oracle Virtual Directory and Access Manager	Chapter 6
Oracle Internet Directory and Access Manager	Chapter 5
Access Manager and Oracle Identity Manager	Chapter 7
Access Manager and Oracle Adaptive Access Manager	Chapter 8
Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager	Chapter 9
Access Manager and Identity Federation	Chapter 10
Access Manager and Oracle Identity Navigator	Chapter 11
Multi-Directory identity store	Chapter 12

1.5 Common Integration Scenarios

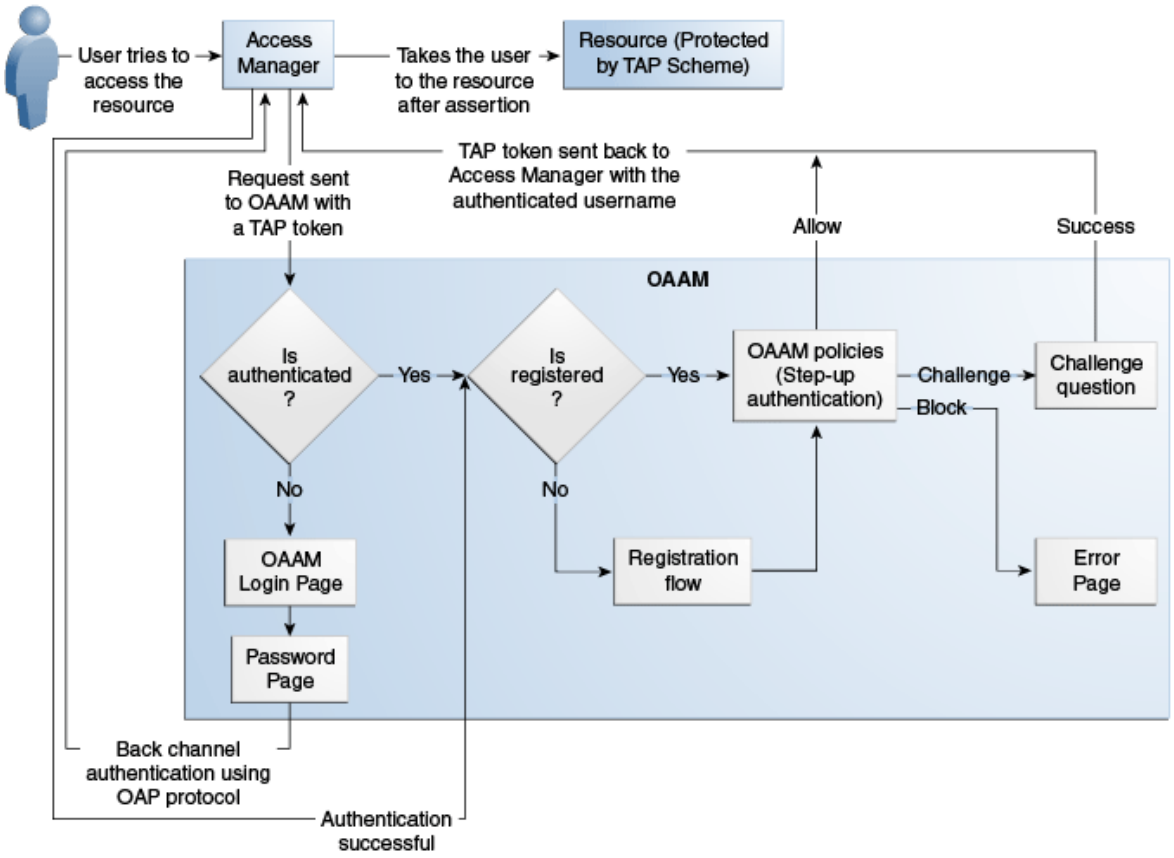
This section describes common scenarios to integration Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager and the resource protection and collection and password management benefits.

1.5.1 Resource Protection and Credential Collection Scenarios (Advanced Integration)

This section describes the process flow when a user tries to access a protected resource in an Access Manager and OAAM "Advanced" integration. The Advanced integration option provides advanced features such as OTP Anywhere and challenge processor and shared library frameworks, but requires a full OAAM deployment. Figure 1–3 illustrate the following scenarios:

- 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 Agent intercepts the (unauthenticated) request and redirects the user to the OAAM Server with encrypted TAP token.
3. The OAAM Server checks for the current authentication status of the user from the TAP token. The TAP token contains 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 will be taken through one of the following flows.

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 using Access Manager. When the user tries to access a resource protected by TAPscheme, Oracle Adaptive Access Manager does not show the user name and password pages since the user is already authenticated. However the following flows are executed in Oracle Adaptive Access Manager depending on whether the user has already registered with Oracle Adaptive Access Manager or not.

User has registered with Oracle Adaptive Access Manager

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

1. Oracle Adaptive Access Manager fingerprints the user device (device fingerprinting)
2. Oracle Adaptive Access Manager runs the post-authentication rules. It determines the user's risk score and executes any actions (for example, KBA or OTP) or alerts that are specified in the policy.
3. The user might also be taken to the challenge flow depending on the risk score.
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, for example, KBA or OTP. Registration is required depending on security requirements, which specify whether the registration is mandatory or optional.
2. Oracle Adaptive Access Manager fingerprints the user device (device fingerprinting).
3. Oracle Adaptive Access Manager runs the post-authentication rules. It determines the user's risk score and executes any actions (for example, KBA or OTP) or alerts that are specified in the policy.
4. If the risk score is sufficiently high, then the user might be blocked because it is not possible to take him to the challenge flow because of incomplete registration.

5. However, 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 user device and runs pre-authentication rules to determine if the user should be allowed to proceed to the OAAM password page.
4. If the user is allowed to proceed, the virtual authentication device rules are run during the Authentication Pad checkpoint. These rules determine which virtual authenticator to display in the OAAM password page.
5. 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.
6. 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.
8. The credentials collected from Oracle Adaptive Access Manager is 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.
9. Oracle Adaptive Access Manager interacts with the user to establish identity to perform the desired action. Oracle Adaptive Access Manager determines the user's risk score and executes any actions (for example, KBA or OTP) or alerts that are specified in the policy.
10. If the user is not registered, he may be asked to go through registration, for example, KBA or OTP.
11. Registration is required depending on security requirements, which specify whether the registration is mandatory or optional.
12. 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 (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. This deployment provides login security and Knowledge Based Authentication (KBA) without requiring a separate OAAM Server.

1. A user tries to access a resource protected by Access Manager.
2. Oracle Access Management WebGate intercepts the request and redirects the user 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.
4. Based on the rule result such as ALLOW, BLOCK, or DENY, Access Manager displays the appropriate pages.
5. If the user is allowed to proceed, Access Manager displays the password page.
6. The user submits his password on the password page.
7. The credentials collected from Access Manager is verified against the identity store.
8. After validation, Access Manager calls the OAAM APIs again to run the post-authentication rules.
9. Access Manager displays the appropriate set of pages based on the rule result, which are REGISTER USER, REGISTER QUESTIONS, REGISTER USER [optional], CHALLENGE, ALLOW, or BLOCK.

   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

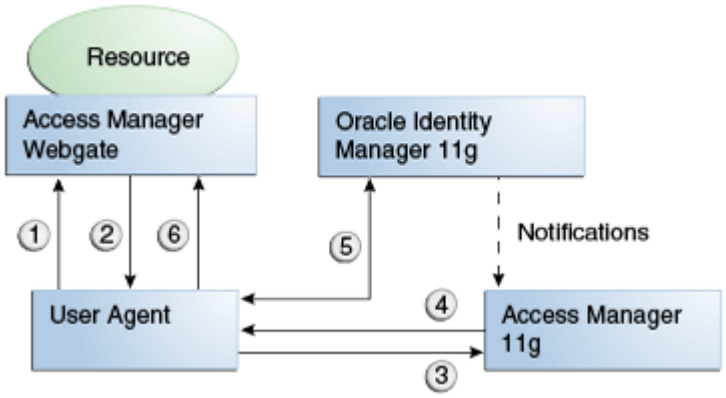
Common management scenarios supported by these deployment modes include:

- 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 11*g* WebGate intercepts the request, detects that the user is not authenticated, and redirects the user to the Oracle Access Management Credential Collector (or 10*g* 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 landing page. The options are:

- Self-registration using the link on the Access Manager login 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 custom 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.

Password Change Flow - Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager Integrated

In this scenario, the user is at the OAAM password page and clicks the **Change Your Password** link.

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 the Oracle Access Management Java APIs to validate the credentials.
10. If authentication is successful and the user has registered questions, but he wants to reset his password, the user clicks the **Change Password** link.
11. The user is redirected to the **Change Password** URL of Oracle Adaptive Access Manager, which allows the users to change his password.
12. Oracle Adaptive Access Manager collects the current password and the new password, and confirms the password from the user using its authenticators.
13. Password policy information, obtained from Oracle Identity Manager, is displayed to guide the user to select the appropriate password.
14. Oracle Adaptive Access Manager makes Oracle Identity Manager calls to update the password in the repository.
15. If the update is successful, Oracle Adaptive Access Manager redirects the user to the resource protected by Access Manager.

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 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.
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 clicks the **Forgot your password** link on the OAAM password page.
9. Oracle Adaptive Access Manager presents the user with a pre-registered set of challenge questions.
10. The user provides the answers to the challenge questions.
11. Oracle Adaptive Access Manager uses fuzzy logic to validate the answers to challenge questions.
12. If the user provided correct responses, he is redirected to the Password Reset page.
13. Password policy text from Oracle Identity Manager is retrieved by Oracle Adaptive Access Manager by making calls to Oracle Identity Manager, and then shown in the Reset Password page.
14. The user enters the new password.
15. Oracle Adaptive Access Manager calls Oracle Identity Manager to update the repository with the new password.
16. If the update is successful, Oracle Adaptive Access Manager redirects the user to the resource protected by Access Manager.

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.

When 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.

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 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, which displays help desk contact information.
5. The user contacts the help desk over the telephone and asks an administrator to unlock the account.
6. Oracle Identity Manager notifies Access Manager of the account unlock event.
7. The user attempts to access an application URL and this event triggers the normal Oracle Access Management single sign-on flow.

1.5.3.6 Challenge Setup

The Challenge Setup enables users to register challenge questions and answers.

Challenge Setup Flow for Access Manager-Oracle Identity Manager Integration

Access Manager detects and redirects on password trigger conditions:

- Password Policy is updated to increase the required number of challenges.
- Password Policy is updated to require challenges.

When such redirection happens, Oracle Identity Manager checks if the challenge questions are set. If not, it asks the user to set up challenge questions in addition to resetting the password.

The following describes the flow:

> **Note:** The flow assumes First Login is not required.

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. If a password triggering condition is detected, Access Manager redirects the user to the Oracle Identity Manager change password URL.

4. The 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.
5. Oracle Identity Manager interacts with the user to set up the challenges. On completion, Oracle Identity Manager updates the attributes that triggered the set challenges flow.
6. Oracle Identity Manager redirects the user to the application URL that the user attempted to access in Step 1.

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 challenges 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. This feature is available when Access Manager is integrated with Oracle Adaptive Access Manager.

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.
11. The user is redirected to Oracle Adaptive Access Manager where he can reset challenge questions.
12. After resetting the challenge registration, Oracle Adaptive Access Manager prompts the user to register for challenge.
13. If the user did not complete the registration, they are prompted for registration on the next login.

1.6 System Requirements and Certification

Refer to the system requirements and certification documentation for information about hardware and software requirements, platforms, databases, and other information. Both of these documents are available on Oracle Technology Network (OTN).

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:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-requirements-100147.html

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

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

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.

2

Using the idmConfigTool Command

The IdM configuration tool (idmConfigTool) supports a number of tasks to assist in installing, configuring, and integrating Oracle identity management (IdM) components.

This chapter contains these sections:

2.1 About the Tool

This section contains these topics:

2.1.1 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,
- to dump the configuration of IdM components Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Manager, and Oracle Access Manager, and
- to validate the configuration parameters for Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Manager, and Oracle Access Manager.

Section 2.1.2 explains the tasks the tool performs in each situation.

2.1.2 Tasks performed by the Tool

`idmConfigTool` helps you to perform the following tasks efficiently:

- Validating configuration properties representing the Identity Management components Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), Oracle Access Management Access Manager (OAM-AM) and Oracle Identity Manager (OIM).
- Pre-configuring the Identity Store components (Oracle Internet Directory and Oracle Virtual Directory) to install the other Identity Management components, including Access Manager and Oracle Identity Manager.
- Post-configuring the Access Manager, Oracle Identity Manager components and wiring of Access Manager and Oracle Identity Manager.
- Extracting the configuration of the Identity Management components Oracle Internet Directory, Oracle Virtual Directory, Access Manager and Oracle Identity Manager.

See Also: Section 2.3.1.

2.1.3 Components Supported by the Tool

`idmConfigTool` supports these component versions:

- Oracle Internet Directory 11*g*
- Oracle Virtual Directory 11*g*
- Oracle Access Management Access Manager 11*g*
- Oracle Access Manager 10*g*
- Oracle Identity Manager 11*g*
- Oracle Unified Directory (OUD) 11*g*

2.1.4 Location

`idmConfigTool` is located at:

IAM_ORACLE_HOME`/idmtools/bin`

2.1.5 Webgate Types Supported

`idmConfigTool` supports Access Manager 11g Webgates by default. It also supports 10g Webgates.

2.1.6 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.

2.2 Set Up Environment Variables

You must configure the environment before running the IdM configuration tool.

Set the following variables:

Variable	Set to
MW_HOME	Set the value to the full path of the installation's Middleware home.
JAVA_HOME	Ensure that the value contains the following directory: MW_HOME/jdkn
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.

2.3 Syntax and Usage

This section contains these topics:

- Command Syntax
- Requirements
- Generated Files
- Using the Properties File
- Using the Tool for OUD Identity Stores

2.3.1 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 OAM OIM WLS FUSION OAAM 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.

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.
`configOVD`	Oracle Virtual Directory	Creates Oracle Virtual Directory adapters.
`disableOVDAccessConfig`	Oracle Virtual Directory	Disables anonymous access to the Oracle Virtual Directory server. Post-upgrade command. *Note*: `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 Oracle Virtual Directory with split profile.
`upgradeLDAPUsersForSSO`	Oracle Identity Manager Access Manager	Updates existing users in Oracle Internet Directory 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

2.3.2 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.

2.3.3 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. This file is generated 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.

2.3.4 Using the Properties File

This section describes the properties file that can be used with idmConfigTool.

2.3.4.1 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.

It is not necessary to provide password-related properties in the properties file. Indeed, for security you are advised not to insert passwords into the properties file. When passwords are not provided, the tool prompts for the relevant properties at execution.

2.3.4.2 List of Properties

Table 2–1 lists the properties used for integration command options in the idmConfigTool command. The properties are listed in alphabetical order.

Table 2–1 Properties Used in IdM Configtool 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 hostname
ACCESS_SERVER_PORT	5575	Access Manager NAP port.
AUTOLOGINURI	/obrar.cgi	URI required by 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.
DOMAIN_LOCATION	ORACLE_BASE /admin/IDMDomain/aserver /IDMDomain	The location of the Oracle Identity Manager domain.
DOMAIN_NAME	IDM_Domain	The Oracle Identity Manager domain name.
IDSTORE_ADMIN_PORT	4321	The admin port for an Oracle Unified Directory (OUD) identity store.
IDSTORE_HOST	idstore.example.com	Host name of the LDAP identity store directory (corresponding to the IDSTORE_ DIRECTORYTYPE).

Table 2–1 (Cont.) Properties Used in IdM Configtool properties Files

Parameter	Example Value	Description
IDSTORE_PORT	4321	Port number of the LDAP identity store (corresponding to the IDSTORE_ DIRECTORYTYPE).
IDSTORE_BINDDN	cn=orcladmin	Administrative user in the identity store.
IDSTORE_PASSWORD		Password for the identity store bind DN.
IDSTORE_ USERNAMEATTRIBUTE	cn	Username attribute used to set and search for users in the identity store.
IDSTORE_LOGINATTRIBUTE	uid	The login attribute of the identity store which contains the user's login name.
IDSTORE_USERSEARCHBASE	cn=Users,dc=us,dc=example,dc=com	The location in the directory where users are stored.
IDSTORE_SEARCHBASE	dc=us,dc=example,dc=com	Search base for users and groups contained in the identity store.
IDSTORE_GROUPSEARCHBASE	cn=Groups,dc=us,dc=example,dc=com	The location in the directory where groups are stored.
IDSTORE_OAMSOFTWAREUSER	oamLDAP	The username used to establish the Access Manager identity store connection.
IDSTORE_OAMADMINUSER	oamadmin	The identity store administrator for Access Manager. Required only if the identity store is set as the system identity store.
IDSTORE_OAAMADMINUSER	oaamadmin	The identity store administrator for Oracle Adaptive Access Manager.
IDSTORE_SYSTEMIDBASE	cn=system, dc=test	Base for all the system users.
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.
IDSTORE_XELSYSADMINUSER		The administrator of the xelsysadm system account.
IDSTORE_OIMADMINUSER		The identity store administrator for Oracle Identity Manager.
IDSTORE_OIMADMINGROUP		The Oracle Identity Manager administrator group.
IDSTORE_SSL_ENABLED		Whether SSL to the identity store is enabled. Valid values: true | false
IDSTORE_KEYSTORE_FILE		Location of the keystore file containing identity store credentials. Required to establish an SSL connection to the identity store. Applies to Oracle Unified Directory identity stores.

Table 2–1 (Cont.) Properties Used in IdM Configtool properties Files

Parameter	Example Value	Description
IDSTORE_KEYSTORE_ PASSWORD		Password of the keystore file containing identity store credentials (IDSTORE_ KEYSTORE_FILE). Required to establish an SSL connection to the identity store. Applies to Oracle Unified Directory identity stores.
IDSTORE_NEW_SETUP		Used for identity store validation. Used in Oracle Fusion Applications environment.
IDSTORE_DIRECTORYTYPE	OVD	Directory type of the identity store for which the authenticator must be created. Set to OVD if you are using Oracle Virtual Directory server to connect to either Oracle Internet Directory or a non-OID 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 to OUD if your identity store is Oracle Unified Directory. Valid values: OID, OVD, OUD
IDSTORE_ADMIN_USER	cn=systemids,dc=example,dc=com	The administrator of the identity store directory. Note that the entry must contain the complete LDAP DN of the user; the username alone is not sufficient.
IDSTORE_WLSADMINUSER	weblogic_idm	The identity store administrator for Oracle WebLogic Server
IDSTORE_WLSADMINGROUP	WLS Administrators	The identity store administrator group for Oracle WebLogic Server.
IDSTOR_PASSWD		Password of the identity store administrator.
IDSTORE_PWD_ OAMSOFTWAREUSER		Password of the Access Manager software user in the identity store.
IDSTORE_PWD_OAMADMINUSER		Password of the Access Manager user identified as IDSTORE_ OAMSOFTWAREUSER.
IDSTORE_PWD_ XELSYSADMINUSER		Password of the XELSYSADMIN user in the identity store.
IDSTORE_PWD_ WEBLOGICADMINUSER		Password of the WebLogic administrator in the identity store.
IDSTORE_PWD_ OAAMADMINUSER		Password of the OAAM administrator in the identity store.
LDAPn_HOST	.	The hostname of the LDAP server
LDAPn_PORT		The LDAP server port number.
LDAPn_BINDDN	.	The bind DN for the LDAP server
LDAPn_PASSWORD		The LDAP server password.

Table 2–1 (Cont.) Properties Used in IdM Configtool properties Files

Parameter	Example Value	Description
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	/oamsso/logout.html	URI required by OPSS. Default value is /oamsso/logout.html
MDS_DB_URL	jdbc:oracle:thin:@DBHOST:1521:SID	URL of the MDS database.
MDS_DB_SCHEMA_USERNAME	edg_mds	Username of the MDS schema user.
OAM_SERVER_VERSION	10g	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.
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 11*g* server functions. Valid values: OPEN or SIMPLE.
OAM11G_SSO_ONLY_FLAG		Specifies whether Access Manager server can perform authorizations. If true, the Access Manager 11g server operates in authentication only mode, where all authorizations return true by default without any policy validations. If false, the server runs in default mode, where each authentication is followed by one or more authorization requests to the server. Valid values: true (no authorization) | false
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	OAMAdministrators	Specifies the account 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	Hostname of the load balancer to the Oracle HTTP (OHS) server front-ending the Access Manager server.

Table 2–1 (Cont.) Properties Used in IdM Configtool properties Files

Parameter	Example Value	Description
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.
OAM11G_SERVER_GLOBAL_SESSION_TIMEOUT		The global session timeout for sessions in the Access Manager server.
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
OAM11G_IDM_DOMAIN_OHS_HOST	sso.example.com	Host name of the load balancer which is in front of OHS.
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. Valid values: HTTP | HTTPS
OAM11G_OIM_OHS_URL	https://sso.example.com:443/test	
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_IDM_DOMAIN_WEBGATE_PASSWD		The Access Manager domain WebGate password.
OAM11G_OIM_WEBGATE_PASSWD		The password of the Oracle Identity Manager Webgate.
OAM11G_WLS_ADMIN_HOST	myhost.example.com	Host name of the Access Manager domain admin server.

Table 2–1 (Cont.) Properties Used in IdM Configtool properties Files

Parameter	Example Value	Description
OAM11G_WLS_ADMIN_PORT	7001	Port on which the Access Manager domain admin server is running.
OAM11G_WLS_ADMIN_USER	wlsadmin	The username of the Access Manager domain administrator.
OIM_FRONT_END_HOST	host123.example.com	The hostname 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 hostname of the Oracle Identity Manager managed server.
OIM_MANAGED_SERVER_PORT		The port number of the Oracle Identity Manager managed server.
OIM_T3_HOST		The hostname for the Oracle Identity Manager T3 server.
OIM_T3_PORT		The port number of the Oracle Identity Manager T3 server.
OVD_HOST		OVD Server hostname
OVD_PORT		OVD Server port number
OVD_BINDDN		OVD Server bind DN
OVD_PASSWORD		OVD Server password
OVD_SSL		Indicates whether the connection is over SSL. 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 11*g*. Valid values: true, false
POLICYSTORE_HOST	mynode.us.example.com	The hostname 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.

Table 2–1 (Cont.) Properties Used in IdM Configtool properties Files

Parameter	Example Value	Description
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.
POLICYSTORE_KEYSTORE_ PASSWORD		The password of the keystore file for an SSL-enabled policy store.
SPLIT_DOMAIN	true	Flag to force configOAM to create security providers in the domain against which it is run. Valid values are true, false.
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 ohsWebgate10g for configOAM and configOIM regardless of the WebGate version in use.
PRIMARY_OAM_SERVERS	idmhost1.example.com:5575 ,idmhost2.example.com:557 5	A comma-separated list of your Access Manager servers and their proxy ports.
WLSHOST	node01.example.com	The WebLogic Server host name
WLSPORT	7001	The WebLogic Server port number
WLSADMIN	wlsadmin	The WebLogic Server administrator login
WLSPASSWD		The WebLogic Server administrator.

2.3.5 Using the Tool for OUD Identity Stores

This section explains additional tasks you may need to perform when using idmConfigTool for a target identity store which is an instance of Oracle Unified Directory (OUD). Topics include:

- Creating the Global ACI for OUD
- Creating Indexes on OUD Replicas

2.3.5.1 Creating the Global ACI for OUD

When you use idmConfigTool for an identity store that is an instance of OUD, the global ACI is not created. Consequently you must first grant access to the changelog, and then create the ACI. 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:

```
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:

```
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/OUD/config/admin-truststore \
--bindDN cn=oudadmin \
--bindPasswordFile mypassword \
--no-prompt
```

3. Add the new ACI:

```
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:

```
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. Repeat Steps 1 through 3 for each OUD instance.

2.3.5.2 Creating Indexes on OUD 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, these replicas are not updated with the indexes and 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/OUD/bin/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/OUD/bin/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/OUD/bin/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.

2.4 Command Options and Properties

This section lists the properties for each command option. Topics include:

- disableOVDAccessConfig Command
- upgradeOIMTo11gWebgate

Notes:

- The command options show the command syntax on Linux only. See Section 2.3.1 for Windows syntax guidelines.
- The tool prompts for passwords. For security, it is recommended that you do not specify password attributes in the properties file.

2.4.1 preConfigIDStore Command

Syntax

```
./idmConfigTool.sh -preConfigIDStore input_file=input_properties
```

Properties

Table 2–2 lists the properties for this mode:

Table 2–2 Properties of preConfigIDStore

Property	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
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).)
IDSTORE_KEYSTORE_FILE	YES, if target identity store is Oracle Unified Directory. Use the format: oud_install_path /OUD/config/admin-keystore
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is Oracle Unified Directory.

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
```

2.4.2 prepareIDStore Command

Syntax

The prepareIDStore command takes `mode` as an argument to perform tasks for the specified component. The syntax for specifying the mode is:

```
./idmConfigTool.sh -prepareIDStore mode=mode
input_file=filename_with_Configproperties
```

where mode must be one of:

- OAM
- OIM
- OAAM
- WLS
- FUSION
- all (performs all the tasks of the above modes combined)

> **Note:** WLS mode must be run before OAM.

2.4.2.1 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

```
./idmConfigTool.sh -prepareIDStore mode=OAM
input_file=filename_with_Configproperties
```

Properties

Table 2–3 lists the properties for this mode:

Table 2–3 prepareIDStore mode=OAM Properties

Parameter	Required?
IDSTORE_HOST	YES

Table 2–3 (Cont.) prepareIDStore mode=OAM Properties

Parameter	Required?
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	
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).)

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
```

2.4.2.2 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

```
./idmConfigTool.sh -prepareIDStore mode=OIM
input_file=filename_with_Configproperties
```

Properties

Table 2–4 lists the properties in this mode:

Table 2–4 prepareIDStore mode=OIM 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_OIMADMINUSER	
IDSTORE_OIMADMINGROUP	
IDSTORE_SYSTEMIDBASE	
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).)

Example properties File

Here is a sample properties file for this option. With this set of properties, OIMADMINUSER is created in IDSTORE_SYSTEMIDBASE:

```
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
```

2.4.2.3 prepareIDStore mode=OAAM

The following are created in this mode:

- Create Oracle Adaptive Access Manager Administration User
- Create Oracle Adaptive Access Manager Groups
- Add 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 2–5 shows the properties in this mode:

Table 2–5 prepareIDStore mode=OAAM Properties

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_ USERNAMEATTRIBUTE	
IDSTORE_LOGINATTRIBUTE	
IDSTORE_USERSEARCHBASE	
IDSTORE_GROUPSEARCHBASE	
IDSTORE_SEARCHBASE	
IDSTORE_OAAMADMINUSER	YES
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).)

2.4.2.4 prepareIDStore mode=WLS

The following are created in the WLS (Oracle WebLogic Server) mode:

- Create Weblogic Administration User
- Create Weblogic Administration Group
- Add the Weblogic Administration User as a member of Weblogic Administration Group

Syntax

```
./idmConfigTool.sh -prepareIDStore mode=WLS
input_file=filename_with_Configproperties
```

Properties

Table 2–6 lists the properties in this mode:

Table 2–6 prepareIDStore mode=WLS Properties

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_ USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	

Table 2–6 (Cont.) prepareIDStore mode=WLS Properties

Parameter	Required?
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_WLSADMINUSER	YES
IDSTORE_WLSADMINGROUP	YES
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).)

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
```

2.4.2.5 prepareIDStore mode=fusion

The following actions are taken in this mode:.

- Create a Readonly User
- Create a ReadWrite User
- Create a Super User
- Add the readOnly user to the groups `orclFAGroupReadPrivilegeGroup` and `orclFAUserWritePrefsPrivilegeGroup`
- Add the `readWrite` user to the groups `orclFAUserWritePrivilegeGroup` and `orclFAGroupWritePrivilegeGroup`

Syntax

```
./idmConfigTool.sh -prepareIDStore mode=fusion
input_file=filename_with_Configproperties
```

Properties

Table 2–7 lists the properties in this mode:

Table 2–7 prepareIDStore mode=fusion Properties

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES

Table 2–7 (Cont.) prepareIDStore mode=fusion Properties

Parameter	Required?
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).)

Example properties File

Here is a sample properties file for this option, which creates IDSTORE_SUPERUSER:

```
IDSTORE_HOST : idstore.example.com
IDSTORE_PORT : 389
IDSTORE_BINDDN : cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
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=example,dc=com
IDSTORE_SUPERUSER: weblogic_fa
POLICYSTORE_SHARES_IDSTORE: true
```

2.4.2.6 prepareIDStore mode=all

The mode performs all the tasks that are performed in the modes OAM, OIM, WLS, OAAM, and FUSION.

Syntax

```
./idmConfigTool.sh -prepareIDStore mode=all
input_file=filename_with_Configproperties
```

Properties

Table 2–8 lists the properties in this mode:

Table 2–8 prepareIDStore mode=all Properties

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERSEARCHBASE	YES

Table 2–8 (Cont.) prepareIDStore mode=all Properties

Parameter	Required?
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_LOGINATTRIBUTE	
IDSTORE_SEARCHBASE	YES
IDSTORE_SYSTEMIDBASE	
IDSTORE_READONLYUSER	
IDSTORE_READWRITEUSER	
IDSTORE_SUPERUSER	
IDSTORE_OAMSOFTWAREUSER	
IDSTORE_OAMADMINUSER	
IDSTORE_OIMADMINUSER	
IDSTORE_OIMADMINGROUP	
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_OAAMADMINUSER	YES
IDSTORE_WLSADMINUSER	YES
IDSTORE_WLSADMINGROUP	YES
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).)
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	
POLICYSTORE_SHARES_IDSTORE	

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
```

2.4.3 configPolicyStore Command

Syntax

```
./idmConfigTool.sh -configPolicyStore input_file=input_properties
```

Properties

Table 2–9 lists the command properties.

Table 2–9 Properties for ConfigPolicyStore

Property	Required?
POLICYSTORE_HOST	YES
POLICYSTORE_PORT	YES
POLICYSTORE_BINDDN	YES
POLICYSTORE_SEARCHBASE	YES
POLICYSTORE_SYSTEMIDBASE	
POLICYSTORE_READONLYUSER	
POLICYSTORE_ READWRITEUSER	
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
```

2.4.4 configOAM Command

Syntax

```
./idmConfigTool.sh -configOAM input_file=input_properties
```

Properties

Table 2–10 lists the command properties.

Table 2–10 Properties of configOAM

Property	Required?
WLSHOST	YES
WLSPORT	YES
WLSADMIN	YES
IDSTORE_BINDDN	YES
IDSTORE_HOST	YES

Table 2–10 (Cont.) Properties of configOAM

Property	Required?
IDSTORE_PORT	YES
IDSTORE_DIRECTORYTYPE	
IDSTORE_USERNAMEATTRIBUTE	
IDSTORE_LOGINATTRIBUTE	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_OAMSOFTWAREUSER	
IDSTORE_OAMADMINUSER	
IDSTORE_SYSTEMIDBASE	YES
PRIMARY_OAM_SERVERS	
WEBGATE_TYPE	
ACCESS_GATE_ID	
OAM_TRANSFER_MODE	
COOKIE_DOMAIN	
COOKIE_EXPIRY_INTERVAL	
OAM11G_WG_DENY_ON_NOT_PROTECTED	
OAM11G_IDM_DOMAIN_OHS_HOST	
OAM11G_IDM_DOMAIN_OHS_PORT	
OAM11G_IDM_DOMAIN_OHS_PROTOCOL	
OAM11G_OAM_SERVER_TRANSFER_MODE	
OAM11G_IDM_DOMAIN_LOGOUT_URLS	
OAM11G_OIM_WEBGATE_PASSWD	
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	
OAM11G_SSO_ONLY_FLAG	
OAM11G_OIM_INTEGRATION_REQ	
OAM11G_IMPERSONATION_FLAG	Oracle Fusion Applications only.
OAM11G_SERVER_LBR_HOST	
OAM11G_SERVER_LBR_PORT	
OAM11G_SERVER_LBR_PROTOCOL	
OAM11G_SERVER_LOGIN_ATTRIBUTE	
OAM11G_IDSTORE_NAME	YES
POLICYSTORE_SHARES_IDSTORE	
SPLIT_DOMAIN	

Note: 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

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: ohsWebgate10g
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: true
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
```

2.4.5 configOIM Command

As of 11*g* 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.

Syntax

```
./idmConfigTool.sh -configOIM input_file=input_file_with_path
```

Properties

Table 2–11 lists the command properties.

Table 2–11 Properties for configOIM

Property	Required?
LOGINURI	required by Oracle Platform Security Services (OPSS).
LOGOUTURI	required by OPSS.
AUTOLOGINURI	required by OPSS.
ACCESS_SERVER_HOST	
ACCESS_GATE_ID	
ACCESS_SERVER_PORT	
COOKIE_DOMAIN	
COOKIE_EXPIRY_INTERVAL	
WEBGATE_TYPE	
OAM_TRANSFER_MODE	
SSO_ENABLED_FLAG	
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_DIRECTORYTYPE	
IDSTORE_LOGINATTRIBUTE	
IDSTORE_ADMIN_USER	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
MDS_DB_URL	
MDS_DB_SCHEMA_USERNAME	
WLSHOST	YES
WLSPORT	YES
WLSADMIN	YES
DOMAIN_NAME	
DOMAIN_LOCATION	
OIM_MANAGED_SERVER_NAME	
OAM_SERVER_VERSION	Required only when Access Manager server does not support 11g webgate in Oracle Identity Manager-Access Manager integration. In that case, value should be provided as '10g'.
OAM11G_WLS_ADMIN_HOST	Required if Access Manager and Oracle Identity Manager servers are configured on different Weblogic domains (that is, a cross-domain setup)

Table 2–11 (Cont.) Properties for configOIM

Property	Required?
OAM11G_WLS_ADMIN_PORT	Required if Access Manager and Oracle Identity Manager servers are configured on different Weblogic domains (that is, a cross-domain setup)
OAM11G_WLS_ADMIN_USER	Required if Access Manager and Oracle Identity Manager servers are configured on different Weblogic domains (that is, a cross-domain setup)

Example properties File

Here is a sample properties file for this option, which seeds the following keys in the credential store framework (CSF): SSOAccessKey, SSOKeystoreKey, SSOGlobalPP:

```
LOGINURI: /${app.context}/adfAuthentication
LOGOUTURI: /oamsso/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: ohsWebgate10g
SSO_ENABLED_FLAG: true
IDSTORE_PORT: 389
IDSTORE_HOST: idstore.example.com
IDSTORE_DIRECTORYTYPE: OID
IDSTORE_ADMIN_USER: cn=oamLDAP,cn=Users,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
```

2.4.6 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
```

2.4.7 upgradeLDAPUsersForSSO Command

Syntax

```
idmConfigTool.sh -upgradeLDAPUsersForSSO input_file=input_Properties
```

Properties

Table 2–12 lists the command properties.

Table 2–12 Properties for upgradeLDAPUsersForSSO

Property	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_ADMIN_USER	YES
IDSTORE_DIRECTORYTYPE	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
PASSWORD_EXPIRY_PERIOD	
IDSTORE_LOGINATTRIBUTE	

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
```

2.4.8 validate IDStore Command

Syntax

```
./idmConfigTool.sh -validate component=IDSTORE input_file=input_Properties
```

Properties

Table 2–13 lists the command properties.

Table 2–13 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
```

2.4.9 validate PolicyStore Command

Syntax

```
./idmConfigTool.sh -validate component=POLICYSTORE input_file=input_Properties
```

Properties

Table 2–14 lists the command properties.

Table 2–14 Properties for validate policystore

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
```

2.4.10 validate OAM Command (11g)

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 2–15 lists the command properties.

Table 2–15 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: true
OAM11G_OAM_ADMIN_USER_PASSWD:
```

2.4.11 validate OAM Command (10g)

Syntax

```
./idmConfigTool.sh -validate component=OAM10g input_file=input_Properties
```

Properties

Table 2–16 lists the command properties.

Table 2–16 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	

2.4.12 validate OIM 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 2–17 lists the command properties.

Table 2–17 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_HOST	YES
OIM_PORT	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_HOST: node06.example.com
OIM_PORT: 1400
```

2.4.13 configOVD Command

Syntax

```
./idmConfigTool.sh -configOVD input_file=input_Properties
```

Properties

Table 2–18 lists the command properties (where *n*=1,2..).

Table 2–18 configOVD properties

Property	Required?
OVD_HOST	YES
OVD_PORT	YES
OVD_BINDDN	YES
OVD_SSL	
LDAPn_TYPE	
LDAPn_HOST	YES
LDAPn_PORT	YES
LDAPn_BINDDN	YES
LDAPn_SSL	
LDAPn_BASE	YES
LDAPn_OVD_BASE	YES
USECASE_TYPE	YES

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
```

When using this file, the command is thus 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
```

2.4.14 ovdConfigUpgrade Command

Syntax

```
./idmConfigTool.sh -ovdConfigUpgrade input_file=input_Properties
```

Properties

Table 2–19 lists the command properties.

Table 2–19 ovdConfigUpgrade Properties

Property	Required?
OVD_HOST	
OVD_PORT	
OVD_BINDDN	
OVD_SSL	
LDAPn_BINDDN	

Table 2–19 (Cont.) ovdConfigUpgrade Properties

Property	Required?
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
```

2.4.15 disableOVDAccessConfig Command

Syntax

```
./idmConfigTool.sh -disableOVDAccessConfig input_file=input_Properties
```

Properties

Table 2–20 lists the command properties.

Table 2–20 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
```

2.4.16 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 2–11.

As indicated in the table, certain properties are required when Oracle Identity Manager and Access Manager are configured on different weblogic domains.

2.5 Examples

For examples of `idmConfigTool` usage, see the individual command options in Command Options and Properties.

Part II

Core Integrations

This part describes integrations between certain IdM components.

This part contains the following chapters:

3

Enabling LDAP Synchronization in Oracle Identity Manager

This chapter explains how to manually configure LDAP synchronization of Oracle Identity Manager with the LDAP identity store post-installation.

In earlier releases of Oracle Identity Manager, LDAP synchronization can be enabled only at the time of installing Oracle Identity Manager, and postinstallation enablement of LDAP synchronization is not allowed. From Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) onwards, postinstallation enablement of LDAP synchronization is supported. Oracle Identity Manager 11*g* Release 2 (11.1.2) also supports postinstallation enablement of LDAP synchronization.

> **See Also:** "Integration Between LDAP Identity Store and Oracle Identity Manager" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for more information about LDAP synchronization

When Oracle identity Manager with Oracle Internet Directory (OID) or iplanet (ODSEE) or Active Directory (AD) or Oracle Unified Directory (OUD) is selected during installation, the virtualization functionality of Oracle Virtual Directory (OVD) is utilized. Oracle Identity Manager includes the Identity Virtualization Library (libOVD) instead of the stand-alone OVD server. Oracle Identity Manager deployment can be with or without Identity Virtualization Library (libOVD). With Identity Virtualization Library (libOVD) included in Oracle Identity Manager, the common library is used by Oracle Identity Manager without running its own instance of OVD. Without Identity Virtualization Library (libOVD), Oracle Identity Manager must use an instance of OVD separately.

> **Note:** The common library is the definition for Identity Virtualization Library (libOVD) that resides in the same Java Virtual Machine (JVM) as Oracle Identity Manager. It is a library in Oracle Identity Manager and not a separate server.

When you select LDAP synchronization in the Oracle Identity Manager installer, you can select any one of the AD, iPlanet (ODSEE), OID, OVD, and OUD options. If you select any of AD, iPlanet (ODSEE), OID, or OUD, then Oracle Identity Manager is installed with Identity Virtualization Library (libOVD). If you select OVD, then LDAP synchronization is enabled, and no manual configuration steps for enabling LDAP synchronization is required. However, postinstall manual configuration to enable LDAP synchronization is required when LDAP synchronization has not been enabled at the time of installing Oracle Identity Manager.

This chapter describes the following configurations for postinstallation enablement of LDAP synchronization:

- Enabling Postinstallation LDAP Synchronization
- Customizing User Creation Through Oracle Identity Manager With Different Custom Object Classes
- Creating Identity Virtualization Library (libOVD) Adapters and Integrating With Oracle Identity Manager
- Enabling SSL Between Identity Virtualization Library (libOVD) and the Directory Server

In addition, this chapter contains the following sections:

- Provisioning Users and Roles Created Before Enabling LDAP Synchronization to LDAP
- Disabling LDAP Synchronization
- Creating OVD Adapters
- Managing Identity Virtualization Library (libOVD) Adapters
- Enabling Access Logging for Identity Virtualization Library (libOVD)
- Configuring LDAP Authentication When LDAP Synchronization is Enabled

3.1 Enabling Postinstallation LDAP Synchronization

To enable LDAP synchronization after Oracle Identity Manager has been deployed:

Note: In Oracle Identity Manager 11*g* Release 2 (11.1.2), the idmConfigTool utility must be run to preconfigure LDAP synchronization. Running the LDAPConfigPreSetup script to preconfigure LDAP synchronization generates errors. See "Using the idmConfigTool Command" on page 2-1 for information about using the idmConfigTool utility.

The idmConfigTool is run in the Enterprise Deployment environment. See *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management* for details. This is another way of setting up the prerequisites for LDAP synchronization.

In stand-alone Oracle Identity Manager deployment, for the steps to setup the prerequisites for LDAP synchronization, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

If idmConfigTool is not used to setup the prerequisites, then the database schema must be extended and other steps must be performed, as described in "Completing the Prerequisites for Enabling LDAP Synchronization" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

---

1. Set the *OIM_HOME* environment variable to the directory on which Oracle Identity Manager is deployed.
2. Copy the following files from the MDS to a temporary staging directory, such as /tmp:

Note: 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.

- 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/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, such as cn=ADRUsers,cn=Users,dc=us,dc=oracle,dc=com
   - $DefaultRoleContainer$ with a value, such as cn=ADRGroups,cn=Groups,dc=us,dc=oracle,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: Make sure that EventHandlers.xml is in the /db/ldapMetadata/ directory when imported into MDS.

5. Edit IT Resource configuration in Oracle Identity Manager. To do so:
   a. Login to the Oracle Identity System Administration as the System Administrator.
   b. In the left navigation pane, under Configuration, click **IT Resource**. The Manage IT Resource page is displayed.
   c. Search for the `Directory Server` IT resource.
   d. 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=oracle,dc=com.
   e. 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.
   f. Enter the values for the bind credentials, as shown:

      Admin Login: `cn=oimadmin`

      Admin Password: `1111111111`

      Note: The Oracle Identity Manager proxy user DN is in the following format:

      PROXY_USER,cn=system,*ROOT_SUFFIX*

      For example: cn=oimadmin,cn=system, dc=us,dc=oracle,dc=com
   g. 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=oracle,dc=com
6. For reconciliation jobs, seed the LDAP Reconciliation jobs or Load LDAP Recon jobs into Quartz tables, which are part of Oracle Identity Manager schema. To do so:
   a. Seed the LDAP Recon jobs by using the patch_weblogic.sh MDS utility available in *OIM_HOME*/bin/.

      Note: In a text editor, open the $OIM_ORACLE_HOME/server/bin/weblogic.profile file, and enter values for the properties before executing the patch_weblogic.sh script.
   b. Set ANT_HOME and JAVA_HOME accordingly.
   c. Create a backup of a $*OIM_ORACLE_HOME*/server/setup/deploy-files/setup.xml.

d. In a text editor, open the $*OIM_ORACLE_HOME*/server/setup/deploy-files/setup.xml file.

e. If the target for seeding Recon jobs is commented by default, then uncomment the following and have only that target in that file to seed the reconciliation jobs:

```
<target name="patch" description="This contains the list of targets to be
invoked post-patching">
               <antcall target="explode-archived-apps"/>
               <antcall target="seed-ootb-jobs"/>
               <!--antcall target="seed-ldap-recon-jobs"/--> == Uncomment
this line.
               <antcall target="update-oes-ootb-policies"/>
               <antcall target="seed-ootb-templates"/>
               <antcall target="unzip-db-deliverables-archive"/>
              <!--ant antfile="${appserver.type}/setup.xml" target="patch"
inheritrefs="true" /-->
</target>
```

The required target to seed the Recon jobs is seed-ldap-recon-jobs.

f. Run the patch_weblogic.sh script.

3.2 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>
```

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.

3.3 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 3–1 lists the files used for Identity Virtualization Library (libOVD) adapter configuration.

Table 3–1 Identity Virtualization Library (libOVD) Adapter Configuration Files

File	Description
Files in the $*MIDDLEWARE_HOME*/oracle_common/modules/oracle.ovd_11.1.1/ directory	Files related to Identity Virtualization Library (libOVD)

Table 3–1 (Cont.) Identity Virtualization Library (libOVD) Adapter Configuration Files

File	Description
Files in the $*MIDDLEWARE_HOME*/oracle_common/bin/ directory: libovdadapterconfig.sh libovdconfig.sh libovdadapterconfig.bat libovdconfig.bat	Script files to configure Identity Virtualization Library (libOVD)
Files in the $*MIDDLEWARE_HOME*/Oracle_IDM/libovd/ directory: adapter_template_oim_ldap.xml adapter_template_oim.xml	Template files to configure Identity Virtualization Library (libOVD)
Files in the $*MIDDLEWARE_HOME*/user_projects/domains/*DOMAIN_NAME*/config/fmwconfig/ovd/*ADAPTER_NAME*/ directory: adapters.os_xml By default, the value of *ADAPTER_NAME* is oim.	Configuration file after Identity Virtualization Library (libOVD) has been configured

To configure Identity Virtualization Library (libOVD) adapters and integrate with Oracle Identity Manager:

1. Before running the scripts to configure Identity Virtualization Library (libOVD), set the following environment variables:
   - set MIDDLEWARE_HOME to the appropriate Middleware home directory
   - set ORACLE_HOME to $MIDDLEWARE_HOME/oracle_common
   - set WL_HOME to $MIDDLEWARE_HOME/wlserver_10.3
   - set JAVA_HOME to appropriate jdk6 path ../jdk6
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 layout the directory structure, run the following command:

   ```
   sh $MW_HOME/oracle_common/bin/libovdconfig.sh -domainPath FULL_PATH_OF_
   DOMAIN -contextName oim -host ADMINSERVER_HOST -port ADMINSERVER_PORT
   -userName ADMINSERVER_USERNAME
   ```

   For example:

   ```
   sh $MW_HOME/oracle_common/bin/libovdconfig.sh -domainPath $MIDDLEWARE_
   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 OID 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 ADMINSERVER_HOST -port ADMINSERVER_PORT
-userName ADMINSERVER_USERNAME -adapterName ADAPTER_NAME -adapterTemplate
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.

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 OID 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 OUD.

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 3-10.

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 $MIDDLEWARE_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. To verify that the data is managed in the LDAP server configured with the -dataStore option, connect to the LDAP server directly through the ldapclient tool.

3.4 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

3.4.1 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 web site URLs:

   `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
```

3.4.2 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/aime1/iPlanet/dsInst/
   defaultCert
   Choose the PKCS#12 file password:
   Confirm the PKCS#12 file password:

   ls -lrt /tmp
   -rw------- 1 aime1 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

---

3.4.3 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
```

3.5 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*.

3.6 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 mentioned in "Provisioning Users and Roles Created Before Enabling LDAP Synchronization to LDAP" on page 3-12.

3.7 Creating OVD Adapters

When you select OID or ODSEE or AD during Oracle Identity Manager installation, and if LDAP synchronization is enabled at that time, then Identity Virtualization Library (libOVD) adapters are generated in the backend.

If you do not enable LDAP synchronization during Oracle Identity Manager installation, and want to enable LDAP synchronization after installing Oracle Identity Manager, then you must create and configure libOVD adapters. See "Creating Identity Virtualization Library (libOVD) Adapters and Integrating With Oracle Identity Manager" on page 3-6 and "Managing Identity Virtualization Library (libOVD) Adapters" on page 3-13 for details.

If you have OVD server configured and want to enable LDAP synchronization after installing Oracle Identity Manager, then the IT Resource page for the Directory Server IT resource type must be configured with the OVD server details. See step 5 in "Enabling Postinstallation LDAP Synchronization" on page 3-2.

If OVD server is not configured for the adapters, then you must create the OVD adapters for various default LDAP servers. For details, see "Creating Adapters in Oracle Virtual Directory" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

> **See Also:** "Configuring Oracle Virtual Directory for Integration with Oracle Identity Manager" on page 4-1 for information about configuring OVD for integration with Oracle Identity Manager

3.8 Managing Identity Virtualization Library (libOVD) Adapters

In an Oracle Identity Manager deployment with LDAP synchronization enabled and AD, iPlanet (ODSEE), or OID as a 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

3.9 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.
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.

3.10 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 as listed in the following table:

Authentication Provider	Control Flag
Default Authenticator	SUFFICIENT
OIM Signature Authenticator	SUFFICIENT
LDAP Authenticator	SUFFICIENT
Default Identity Asserter	No value

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.

4

Configuring Oracle Virtual Directory for Integration with Oracle Identity Manager

This chapter explains how to configure Oracle Virtual Directory for integration with Oracle Identity Manager (OIM).

The topics include:

- Creating Oracle Virtual Directory Adapters for Oracle Internet Directory and Active Directory
- Using the UserManagement Plug-In
- Using the Changelog Plug-In
- Troubleshooting Tips

4.1 Creating Oracle Virtual Directory Adapters for Oracle Internet Directory and Active 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 depends on whether you are configuring the Oracle Internet Directory adapter or the Active Directory Adapter.

   - **Oracle Internet Directory** adapter properties file:

     ```
     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=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
```

- **Active Directory** adapter properties file:

```
ovd.host:ovdhost1.mycompany.com
ovd.port:8899
ovd.binddn:cn=orcladmin
ovd.password:ovdpassword
ovd.oamenabled:true
ovd.ssl:true
ldap1.type:AD
ldap1.host:adidstore.myhost.mycompany.com
ldap1.port:636
ldap1.binddn:cn=adminuser
ldap1.password:adpassword
ldap1.ssl:true
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 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 parameter 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 for each Oracle Virtual Directory instance in your topology, with the appropriate value for `ovd.host` in the property file.

4.2 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.

4.2.1 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).

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.

4.3 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.

4.3.1 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.

4.3.2 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`

4.3.3 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, orclidxperson=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.

4.4 Troubleshooting Tips

This section 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 ORACLE_INSTANCE/bin
./opmnctl stopproc ias-component=ovd1
./opmnctl startproc ias-component=ovd1
```

See Also: "Using My Oracle Support for Additional Troubleshooting Information" on page 1-23.

5

Integrating Oracle Internet Directory with Access Manager

This chapter describes post-installation enablement of a centralized LDAP store for use with Oracle Access Management Access Manager. Oracle Internet Directory is featured in this chapter. Tasks are the same regardless of your chosen LDAP provider.

This chapter provides the following sections:

See Also: *Oracle Fusion Middleware Securing Oracle WebLogic Server*

5.1 Introduction

Oracle Access Management Access Manager (Access Manager) addresses each user population and LDAP directory store as an identity domain. Each identity domain maps to a configured LDAP User Identity Store that is registered with Access Manager. Multiple LDAP stores can be used with each one relying on a different supported LDAP provider.

During initial WebLogic Server domain configuration, the Embedded LDAP is configured as the one and only User Identity Store for Access Manager. Within the Embedded LDAP, the Administrators group is created with `weblogic` seeded as the default Administrator.

Note: The Embedded LDAP performs best with fewer than 10,000 users. With more users, consider a separate enterprise LDAP server. In a highly available configuration, Oracle recommends that an external LDAP is used as the User Identity Store.

Access Manager requires a System Store and a Default Store. During initial WebLogic domain configuration, the Embedded LDAP store is configured as the one and only User Identity Store that is designated as both the System Store and the Default Store:

- **System Store**: Only a single User Identity Store can (and must) be designated as the System Store. This is used to authenticate Administrators signing in to use the Oracle Access Management Console, remote registration tools, and custom administrative commands in WLST.

  Note: Once a remote User Store is designated as the System Store, you must change the `OAMAdminConsoleScheme` to use an LDAP Authentication Module that references the same System Store.

- **Default Store**: As the name implies, the LDAP store designated as the Default Store is the automatic choice for LDAP Authentication Methods unless you configure a different store.

  Note: Oracle Security Token Service uses only the designated Default Store. When adding User constraints to a Token Issuance Policy, for instance, the identity store from which the users are to be chosen must be Default Store.

After registering a User Identity Store with Access Manager, administrators can reference the store in one or more authentication plug-ins or modules that form the basis for Access Manager Authentication Schemes. When you register a partner (either using the Oracle Access Management Console or the remote registration tool), an application domain can be created and seeded with a policy that uses the default Authentication Scheme. When a user attempts to access an Access Manager-protected resource, she is authenticated against the store designated by the authentication plug-in or module.

Task overview: Configuring an LDAP store for Access Manager

1. Completing Prerequisites on page 5-2.
2. Registering Oracle Internet Directory With Access Manager on page 5-3.
3. Setting Up Authentication Providers with WebLogic Server on page 5-7.
4. Configuring Authentication Between Access Manager and Your User Identity Store on page 5-9.
5. Validating Authentication and Access on page 5-14.

5.2 Prerequisites

Before starting tasks in this chapter, be sure to get familiar with your installed LDAP directory server. The focus in this chapter is Oracle Internet Directory; however, the same tasks apply for any supported LDAP operating with Access Manager:

To prepare to integrate an LDAP store for Access Manager

1. Install the desired LDAP Directory Server (Oracle Internet Directory, in this example), as described in Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory.
2. Install and set up Access Manager with the desired LDAP directory, as described in Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management (see also "Configuring Oracle Internet Directory").

3. Extend the LDAP directory schema for Access Manager, as described in Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management.
4. Create Users and Groups in the LDAP directory, as described in Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management.
5. Proceed to "Registering Oracle Internet Directory With Access Manager".

5.3 Registering Oracle Internet Directory With Access Manager

This section describes post-installation registration of a supported LDAP user identity store to provide connectivity with OAM Servers. See the following topics:

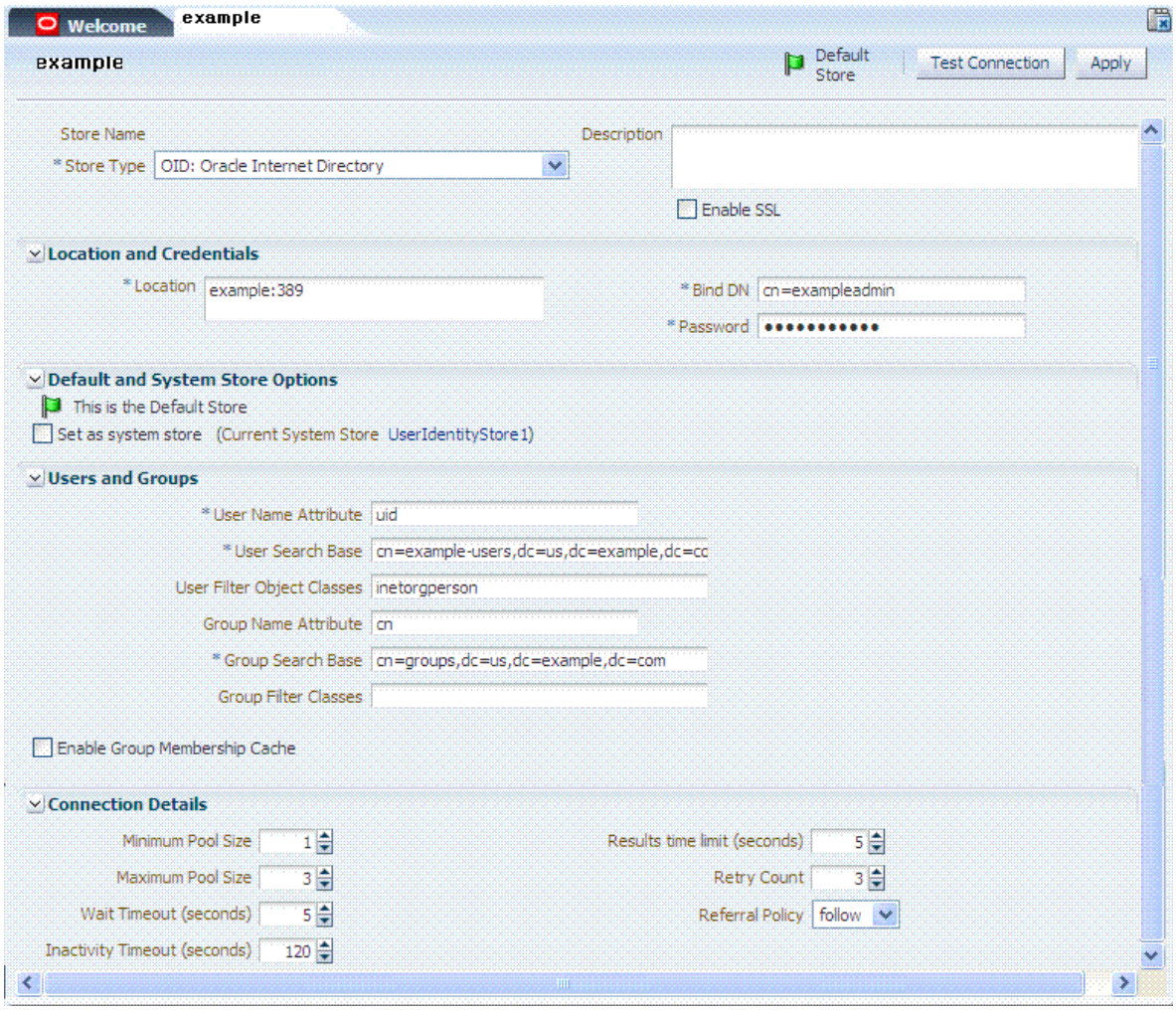
- About the LDAP Store Registration Page
- Registering a User Identity Store with Access Manager
- Designating the System Store, Administrators, or the Default Store

5.3.1 About the LDAP Store Registration Page

In this procedure, you register Oracle Internet Directory with Access Manager. The steps are the same regardless of the supported LDAP you are registering. Your completed registration page will look something like Figure 5–1.

> **See Also:** Oracle Fusion Middleware Administrator's Guide for Oracle Access Managementfor full details of each element.

Figure 5–1 Completed Registration for the Designated Default Store



Surrounding text describes this screen.

****

5.3.2 Registering a User Identity Store with Access Manager

Prerequisites

The user identity store must be installed and running, as described in Prerequisites

To register Oracle Internet Directory with Access Manager

1. Go to the Oracle Access Management Console and log in as an administrator. For example:

   `https://examplehost:port/oamconsole/`

2. In Oracle Access Management Console, open the User Identity Stores node:

   System Configuration tab
   Common Configuration section
   Data Source node

3. Click the **User Identity Stores** node, then click the **Create (+)** button in the tool bar.
4. In the Create: user Identity Store page, enter or select appropriate values for your LDAP store and deployment, then click **Apply**. For example:

   Store Name: *example*
   Store Type: OID Oracle Internet Directory
   Enable SSL:

   Location: *example:389*
   Bind DN *cn=exampleadmin*
   Password ********

   Users Name Attribute *uid*
   User Search Base *cn=example-users,dc=us,dc=example,dc=com*
   User Filter Object Classes *initorgperson*
   Group Name Attribute
   Group Search Base *cn=groups,dc=us,dc=example,dc=com*
   Group Filter Object Classes

   Enable Group Cache
   Group Cache Maximum Size (Mb) *0*
   Group Cache Time to Live (Seconds) *0*

   Minimum Pool Size *1*
   Results time limit (seconds) *5*
   Maximum Pool Size *0*
   Retry Count *3*
   Wait Timeout (seconds) *5*
   Referral Policy *follow*
   Inactivity Timeout (seconds) *120*

5. Click **Apply** to submit the registration.
6. **Test Connection**: Click the **Test Connection** button to confirm connectivity, then close the Confirmation window.
7. Close this page.
8. Proceed to "Designating the System Store, Administrators, or the Default Store".

5.3.3 Designating the System Store, Administrators, or the Default Store

When you open a User Identity Store registration page, you can select Default or System Store options and define Administrator users and roles. By default, the Access Manager Administrators role is the same as the WebLogic Administrators role (user `weblogic`). This can be changed if your enterprise requires independent sets of Administrators.

All Administrator roles, users, and groups must be stored in the LDAP store that is designated as the System Store with Access Manager. If the System Store designation changes, appropriate Administrator roles must be added to the new System Store.

Note: Administrator login works only when the `LDAP` Authentication Module used by the `OAMAdminConsoleScheme` used by the `IAMSuiteAgent` uses the LDAP store that is designated as the System Store.

Prerequisites

Registering a User Identity Store with Access Manager.

The following procedure presumes that Oracle Internet Directory will be set as both the System Store and Default Store. You environment will be different. Perform only steps that apply to you. Skip steps that do not apply to your deployment.

To designate a System Store, Administrators, or Default Store

1. From the Oracle Access Management Console, open the *DesiredStore* registration page:

   System Configuration tab
   Common Configuration section
   Data Source node
   User Identity Stores node
   DesiredStore (*example* in this case)

2. **Set the System Store**: Administrator roles and credentials must reside in this store.
   a. In the registration page, **Default and System Store Options** section, check the box beside **Set as system store** (for domain wide authentication and authorization operations).
   b. Click **Apply**, close the Confirmation window.
   c. **Authentication Module**: Later you will be instructed to set the `LDAP` Authentication Module used by `OAMAdminConsoleScheme` to use this System Store:"Configuring Authentication Between Access Manager and Your User Identity Store" on page 5-9.

3. **Add Administrator User Roles (System Store)**:
   a. In the LDAP store to be designated as the System Store, add Administrator roles, users, and groups using your vendor documentation as a guide.
   b. From the Oracle Access Management Console, open the registration page for the *DesiredStore* under Data Source, User Identity Stores node.
   c. Click the **Add (+)** button in the **Access System Administrators** table to display the **Add System Administrator Roles** dialog box.
   d. From the **Type** list, select **User** and click the **Search** button.
   e. In the results table, click your *DesiredUser* and click the **Add Selected** button.
   f. Repeat as need to add more Administrator User roles.
   g. Click **Apply** to submit user roles.

4. **Add Administrator Group Roles (System Store)**:Ensure that your Administrators group is available in the group search base.
   a. From the Oracle Access Management Console, open the registration page for the *DesiredStore* under Data Source, User Identity Stores node.

b. Click the **Add (+)** button in the **Access System Administrators** table to display the **Add System Administrator Roles** dialog box.

c. From the **Type** list, select **Group** and click the **Search** button.

d. In the results list, click your *DesiredGroup* and click the **Add Selected** button.

e. Repeat as need to add more Administrator Group roles.

f. Click **Apply** to submit Group roles.

5. **Test the New Role**: Close the browser window, then re-open it.

   a. Sign out of the Oracle Access Management Console and close the browser window.

   b. Start up the Oracle Access Management Console and attempt to log in using the previous Administrator role to confirm that this attempt fails.

   c. Log in using the new Administrator role to confirm that this attempt is successful.

      Login Failure: See "Administrator Lockout" in the Troubleshooting section of the Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.

6. **Set Default Store** (for migration only, when patching): The `LDAP` Authentication Module used by `OAMAdminConsoleScheme` should not point to this store unless it is also designated as the System Store.

   a. From the Oracle Access Management Console, open the *DesiredStore* registration page.

   b. Check the box beside **Set as default store**.

   c. Click **Apply**, close the Confirmation window.

7. Proceed to "Setting Up Authentication Providers with WebLogic Server".

5.4 Setting Up Authentication Providers with WebLogic Server

You perform this step to create an authenticator for your LDAP provider to avoid multiple login pages when accessing the Oracle Access Management Console.

Whether you authenticate through Oracle Access Management Console or directly through the WebLogic Server Administration Console, confirm that all authentication providers are set to SUFFICIENT for single sign-on:

WebLogic Provider
IAMSuiteAgent
OracleInternetDirectoryAuthenticator
DefaultIdentityAsserter

Note: Setting any provider to REQUIRED means re-authenticating rather than reaching both Access Manager and WebLogic Server with a single sign-on.

Prerequisites

Registering Oracle Internet Directory With Access Manager

To configure your LDAP provider with WebLogic Server

1. Log in to the WebLogic Server Administration Console as usual. For example:

   `http://AdminServerHost:7001/console`

2. **Add Your LDAP Authenticator:**

   a. Click **Security Realms**, ***myrealm***, then click **Providers**.

   b. Click **New**, enter a name, and select a type. For example:

      Name: *OID Authenticator*

      Type: *OracleInternetDirectoryAuthenticator*

      OK

   c. In the Authentication Providers table, click the newly added authenticator.

   d. On the Settings page, click the **Common** tab, set the Control Flag to **SUFFICIENT**, then click Save.

   e. Click the **Provider Specific** tab, then specify the following values for your deployment:

      Host: LDAP host. For example: *example*

      Port: LDAP host listening port. *3060*

      Principal: LDAP administrative user. For example: *cn=*********

      Credential: LDAP administrative user password. ********

      User Base DN: Same search base as the LDAP user.

      All Users Filter: For example: `(&(uid=*)(objectclass=person))`

      User Name Attribute: Set as the default attribute for username in the LDAP directory. For example: `uid`

      Group Base DN: The group searchbase (same as User Base DN)

      Note: Do not set the All Groups filter; the default works fine as is.

      Save.

3. **Set DefaultIdentityAsserter**:

   a. From **Security Realms**, ***myrealm***, **Providers**, click **Authentication**, click **DefaultIdentityAsserter** to see the configuration page.

   b. Click the **Common** tab and set the Control Flag to **SUFFICIENT**.

   c. **Save**.

4. **Reorder Providers**:

   a. On the Summary page where providers are listed, click the **Reorder** button

   b. On the **Reorder Authentication Providers** page, select a provider name and use the arrows beside the list to order the providers as follows:

      WebLogic Provider
      IAMSuiteAgent
      OracleInternetDirectoryAuthenticator
      DefaultIdentityAsserter

c. Click OK to save your changes

5. **Activate Changes**: In the Change Center, click **Activate Changes**.
6. Reboot Oracle WebLogic Server.
7. Proceed with "Configuring Authentication Between Access Manager and Your User Identity Store".

5.5 Configuring Authentication Between Access Manager and Your User Identity Store

External LDAP repositories can provide user, role, and group membership information to be used:

- When evaluating policies during authentication
- When evaluating identities for authorization conditions in a policy
- When using LDAP to search for identities for conditions in an authorization policy

This section outlines the authentication configuration required to use your new user identity store with Access Manager. While Oracle Internet Directory is featured, this task applies to all supported LDAP repositories. See following topics:

- About Access Manager Authentication Modules, Plug-ins, and Schemes
- Defining Authentication in Access Manager for Your User Identity Store
- Managing Access Manager Policies that Rely on Your LDAP Store

5.5.1 About Access Manager Authentication Modules, Plug-ins, and Schemes

Access to a resource or group of resources can be governed by a single authentication process. At the core is an Authentication Scheme that defines the Challenge Method and the Authentication Method or plug-in required to authenticate the user.

The Basic or Form Challenge Methods require an Authentication Method that points to a specific LDAP store. For instance, `OAMAdminConsoleScheme` relies on the LDAP module for Administrator Roles and credentials. If you define a new System Store, be sure to change the LDAP module to point to it.

Note: Correct any Authentication Methods that use the System Store to ensure these point to a new System Store.

Table 5–1 identifies the pre-configured Authentication Schemes that use the LDAP Challenge Method. For more information, see Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.

Table 5–1 Form and Basic Authentication Schemes Using LDAP Authentication Module

Scheme Name	Specifications	Purpose
BasicScheme	Authentication Level: 1 Challenge Method: Basic Authentication Module: LDAP	Protects Access Manager-related resources (URLs) for most directory types. **Note**: Authentication Level 1 is only one step higher than 0 public pages. Oracle recommends that you do not use Level: 1 in a custom Authentication Scheme.
BasicSessionlessScheme	Authentication Level: 1 Challenge Method: Basic Authentication Module: LDAP	Primarily used for clients that don't support URL redirect or cookies. Challenge Parameters: CookieLessMode=true
FAAuthScheme	Authentication Level: 2 Challenge Method: FORM Authentication Module: LDAP Context: customWar Context Value: /fusion_apps	Protects Fusion Applications.
LDAPScheme	Authentication Level: 2 Challenge Method: Form Authentication Module: LDAP	Protects Access Manager-related resources (URLs) for most directory types based on a Form Challenge Method.
OAAMAdvanced	Authentication Level: 2 Challenge Method: Form Authentication Module: LDAP Context Type: external	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 ending the partner.
OAAMBasic	Authentication Level: 2 Challenge Method: Form Authentication Module: LDAP Context Type: default Context Value: /oam	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. This is more of an integration when mod_osso is used as the agent. Challenge Parameters: oaamPostAuth=true oaamPreAuth=true
OAMAdminConsoleScheme	Authentication Level: 2 Challenge Method: FORM Authentication Module: LDAP Context Type: default Context Value: /oam	Authentication scheme for Oracle Access Management Console.
OIMScheme	Authentication Level: 1 Challenge Method: Form Authentication Module: LDAP Context Type: default Context Value: /oam	Protects Oracle Identity Manager-related resources with a default context type. Note: When integrating Access Manager and Oracle Identity Manager, Access Manager downgrades the user's authentication level when any of the following is detected: password expiry forced password change challenge setup not done

5.5.2 Defining Authentication in Access Manager for Your User Identity Store

The following procedure guides as you set up an LDAP Authentication Method that points to your registered User Identity Store and an Authentication Scheme that uses this LDAP module for Form or Basic authentication. `OAMAdminConsoleScheme` is used in this example on the presumption that you designated your new LDAP store as the System Store. Your environment might be different.

Prerequisites

Setting Up Authentication Providers with WebLogic Server

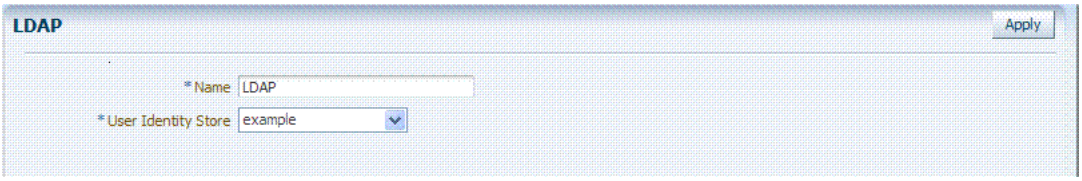
Ensure that the designated User Identity Store contains any user credentials required for authentication.

To use your identity store for authentication with Access Manager

1. **Authentication Modules and Plug-ins**: Open the following in Oracle Access Management Console.

   System Configuration tab
   Access Manager Settings section
   Authentication Modules node

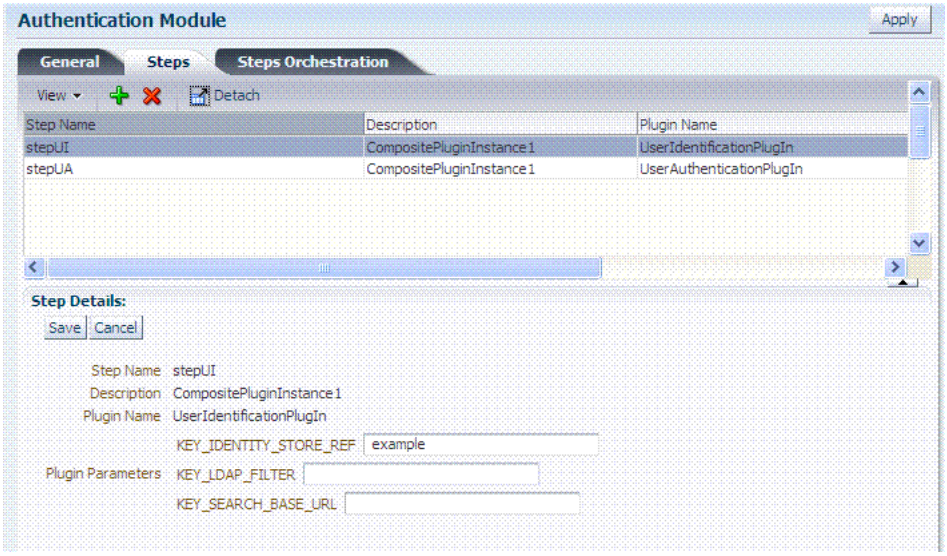
   a. **LDAP Modules**: Open **LDAP Authentication** module, select your User Identity Store, and click **Apply**.



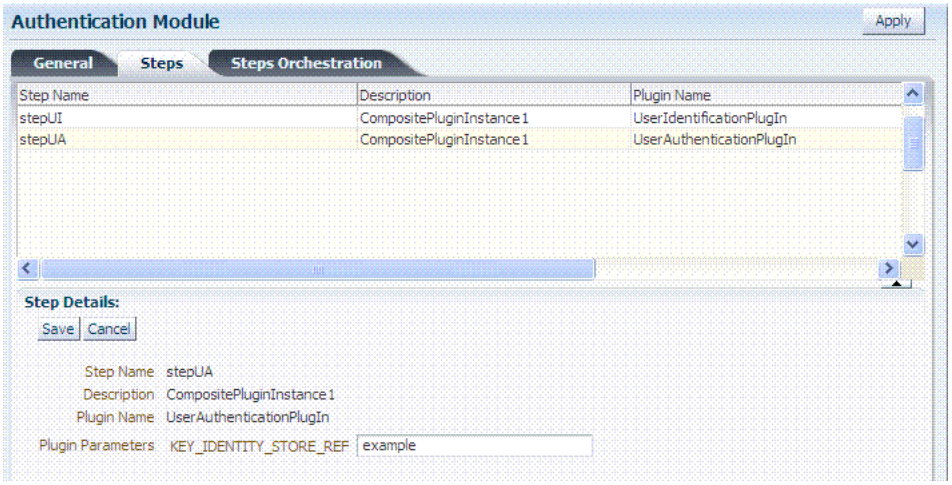
   See Also: Oracle Fusion Middleware Administrator's Guide for Oracle Access Management

   b. **Custom Authentication Modules**: In `LDAPPlugin` Steps (stepUI, `UserIdentificationPlugIn`), specify your KEY_IDENTITY_STORE_REF, and click **Apply**. For example:

   System Configuration tab
   Access Manager section
   Authentication Modules
   Custom Authentication module
   LDAPPlugin
   Steps tab
   stepUI `UserIdentificationPlugIn`



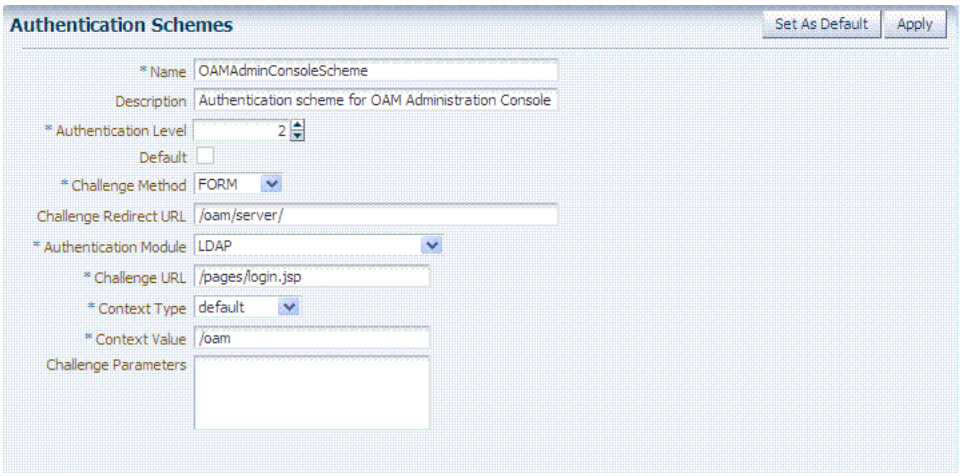
   Repeat this step for the stepUA `UserAuthenticationPlugIn` plug-in, and Apply your changes, as shown here:



See Also: Oracle Fusion Middleware Administrator's Guide for Oracle Access Management

2. **Authentication Scheme Challenge Methods**: Form and Basic Challenge Methods require a reference to the LDAP Authentication Module or Plug-in that points to your User Identity Store. For example:

   Oracle Access Management Console
   Policy Configuration tab
   Shared Components node
   Authentication Schemes node
   DesiredScheme (`OAMAdminConsoleScheme` or any Form or Basic scheme)



   a. Confirm that the Authentication Module references the LDAP module or plug-in that points to your Identity Store.

   b. Click **Apply** to submit the changes (or close the page without applying changes).

   c. Dismiss the Confirmation window.

   See Also: Oracle Fusion Middleware Administrator's Guide for Oracle Access Management

3. Proceed to "Managing Access Manager Policies that Rely on Your LDAP Store".

5.5.3 Managing Access Manager Policies that Rely on Your LDAP Store

Access Manager policies protect specific resources. The policies and resources are organized in an Application Domain. This section describes how to configure authentication policies to use the Authentication Scheme that points to your User Identity Store.

When you register a partner (either using the Oracle Access Management Console or the remote registration tool) using the Auto Create Policies option, an application domain is created and seeded with policies. The seeded Authentication Policy uses the Authentication Scheme that is designated as the Default. Alternatively, you can create an application domain and policies without registering a partner.

> **See Also:** Oracle Fusion Middleware Administrator's Guide for Oracle Access Management for more information.

Prerequisites

Defining Authentication in Access Manager for Your User Identity Store

To create an application domain and policies that use LDAP authentication

1. From the Oracle Access Management Console, open:

   Oracle Access Management Console
   Policy Configuration tab
   Application Domains node

2. Locate and open the desired Application Domain (or click the Create (+) button, enter a unique name, and save it).
3. **Resource Definitions**: Add a definition as described in Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.
4. **Authentication Policies**: Open (or Create) the desired Authentication Policy. For example:
   a. On the Policy page: Select the scheme that references the LDAP module or plug-in that points to your User Identity Store.

      Authentication Scheme: LDAP (or another LDAP module or plug-in)

   b. Click **Apply**, close the Confirmation window.
   c. **Resources for Authentication Policy**:

      Click the Resources tab on the Authentication Policy page.
      Click the Add button on the tab.
      Choose a URL from the list.
      Repeat these steps as needed to add more resources.

   d. Complete the Authentication Policy with any desired Responses.
5. **Authorization Policy Conditions**: Create or modify an Authorization Policy for specific resources and include with any Responses, Conditions, and Rules as described in the Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.
6. **Token Issuance Policy Conditions**: Choose the desired user identity store when setting Identity Conditions in Token Issuance Policies. See he Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.
7. Proceed to "Validating Authentication and Access".

5.6 Validating Authentication and Access

The procedure here provides several methods for confirming that Agent registration and authentication and authorization policies are operational. The procedures are nearly identical for both OAM Agents and OSSO Agents (mod_osso). OSSO Agents use only the authentication policy, not the authorization policy.

Prerequisites

- Users and groups who are granted access must exist in the LDAP User Identity Store that is registered with Access Manager and designated in the Authentication Module or Plug-in used by the Authentication Scheme that is protecting the resource
- Agents must be registered to operate with Access Manager. After registration, protected resources should be accessible with proper authentication without restarting the Administration or Managed Server.
- Application domain, authentication policies, and authorization policies must be configured for specific resources.

To verify authentication and access

1. Using a Web browser, enter the URL for an application protected by the registered Agent to confirm that the login page appears (proving that the authentication redirect URL was specified appropriately). For example:

   `http://exampleWebserverHost.sample.com:8100/resource1.html`

2. Confirm that you are redirected to the login page.
3. On the Sign In page, enter a valid username and password when asked, and click Sign In.
4. Confirm that you are redirected to the resource and proceed as follows:
   - **Success**: If you authenticated successfully and were granted access to the resource; the configuration is working properly.
   - **Failure**: If you received an error during login or were denied access to the resource, check the following:
     - Authentication Failed: Sign in again using valid credentials.
     - **Access to URL ... denied**: This userID is not authorized to access this resource.
     - **Resource not Available**: Confirm that the resource is available.
     - **Wrong Redirect URL**: Verify the redirect URL in the Oracle Access Management Console.

6

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

This chapter explains how to configure Oracle Virtual Directory for integration with Oracle Access Management Access Manager (Access Manager).

This chapter includes the following sections:

> **Note:** You can use Oracle Virtual Directory with most LDAP-enabled technologies. The information in this chapter highlights Oracle Virtual Directory features and capabilities that simplify common integrations.
>
> Contact your Oracle support representative for assistance with other Oracle Virtual Directory integrations.

6.1 Creating and Configuring Oracle Virtual Directory Adapters

Perform the following steps to configure Oracle Virtual Directory for integration with Access Manager using 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 also the appropriate adapter type; either LDAP, Database, or Custom, for the data repository that Access Manager uses.

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 6.1.1, "Creating and Configuring an LDAP Adapter"
- Section 6.1.2, "Creating and Configuring a Database Adapter"
- Section 6.1.3, "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.

   Go to the following sections for more information about configuring each type of adapter:

   - "Configuring an LDAP Adapter" on page 6-2
   - "Configuring a Database Adapter" on page 6-9
   - "Configuring Custom Adapters" on page 6-12

6.1.1 Creating and Configuring an LDAP Adapter

This section provides instructions for creating and configuring an LDAP Adapter for Access Manager.

6.1.1.1 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*.

6.1.1.2 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*

6.1.1.2.1 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 11*g* Release 2 (11.1.2) 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 6-9 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 6–1 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 = {...}`
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 Sun Microsystem's 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 kerb5.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.

6.1.1.2.2 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.

6.1.2 Creating and Configuring a Database Adapter

This section describes how to create and configure a Database adapter for Access Manager.

6.1.2.1 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*.

6.1.2.2 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* be 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.*

6.1.3 Creating and Configuring a Custom Adapter

This section describes how to create and configure a Custom adapter for Access Manager.

6.1.3.1 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*.

6.1.3.2 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.

6.2 Using the OAMPolicyControl Plug-In

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 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.

6.2.1 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.

7

Integrating Access Manager and Oracle Identity Manager

This chapter explains how to integrate Oracle Access Management Access Manager (Access Manager), Oracle Identity Manager, Oracle Virtual Directory, and Oracle Internet Directory. The following configuration instructions assume these components have been installed in a single-node topology, as discussed in Chapter 1, "Introduction".

If you are integrating Access Manager with Oracle Identity Manager for an enterprise deployment, for information see the configuration scenarios described in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

For prerequisite and detailed instructions required for installing the components described in this example integration configuration, see *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* and *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

> **Note:** The instructions in this chapter assumes the that Oracle Internet Directory is configured as the Identity Store and is front-ended by Oracle Virtual Directory to virtualize the data sources. Other component configurations are possible. Refer to the system requirements and certification documentation on Oracle Technology Network for more information about supported configurations.

This chapter contains these sections:

- Section 7.12, "Testing the Integration"
- Section 7.13, "Troubleshooting Common Problems"

7.1 About the Integration

This integration scenario enables you to manage identities with Oracle Identity Manager and control access to resources with Access Manager. Access Manager provides a centralized and automated single sign-on (SSO) solution. Access Manager uses a database for policy and configuration data and a single directory for identity data. This integration scenario assumes a single directory server, namely Oracle Internet Directory, is front-ended by Oracle Virtual Directory. Oracle Identity Manager is a user provisioning and administration solution that automates user account management.

You can deploy the Identity Management components in a single WebLogic Server domain, which may be convenient for a development or test environment. You can also configure the components to be in a cross domain (also known as split domain) deployment where Access Manager and Oracle Identity Manager are installed in different WebLogic Server domains.

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

7.2 Integration Roadmap

Table 7–1 lists the high-level tasks for integrating Access Manager and Oracle Identity Manager with Oracle Virtual Directory and Oracle Internet Directory.

Table 7–1 Integration Flow for Oracle 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 Integration Prerequisites.
2	Enable LDAP synchronization for Oracle Identity Manager.	For information, see: ■ "Configuring OIM Server", ■ "Completing the Prerequisites for Enabling LDAP Synchronization", and ■ "Creating Adapters in Oracle Virtual Directory" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. See the Oracle Identity Manager details in Table 7–2, " Required Components for Integration Scenario".
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.

Table 7–1 (Cont.) Integration Flow for Oracle Access Manager and Oracle Identity

No.	Task	Information
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	Edit the OVD User and Changelog Adapters so the `oamEnabled` parameter is set to `true`.	For information, see "Creating Adapters in Oracle Virtual Directory" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. See Oracle Virtual Directory details in Table 7–2, " Required Components for Integration Scenario".
8	Stop the Oracle WebLogic Server managed servers for Access Manager and Oracle Identity Manager	For information, see "Starting and Stopping Oracle WebLogic Server Instances" in *Oracle Fusion Middleware Administrator's Guide*.
9	Extend Access Manager to support Oracle Identity Manager	For information, see Configuring Access Manager for Integration.
10	Integrate Access Manager and Oracle Identity Manager	For information, see Integrating Access Manager with Oracle Identity Manager.
11	Configure the Webgate on the OHS server to point to the 11*g* OAM Server	For information, see Configuring Oracle HTTP Server.
12	Configure centralized logout for the IAMSuiteAgent.	For information, see "Configuring Centralized Logout for the IAMSuiteAgent" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
13	Remove the IDM Domain Agent and start the Oracle WebLogic Server Administration and Managed Servers.	For information, see Starting Servers with Domain Agent Removed.
14	Test the integration.	For information, see Testing the Integration.
15	Depending upon your environment, migrate the Domain Agent to OHS 10*g* Webgate	For information, see Migrating from the Domain Agent to 10g Webgate with OHS 11g.
16	Depending upon your environment, update the SOA server default composites.	For information, see Updating SOA Server Default Composite.

7.3 Integration Prerequisites

Prior to configuring Access Manager with Oracle Identity Manager, you must have installed all the required components, including any dependencies, and configure the environment in preparation of the integration tasks that follow. For more information about the integration topologies, see Section 1.2, "Integration Topologies".

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 *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* and *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Table 7–2 lists the required components that must be installed and configured before the Access Manager and Oracle Identity Manager integration tasks are performed.

Table 7–2 Required Components for Integration Scenario

Component	Information
Oracle database	For more information, *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
Oracle WebLogic Server 10.3.6	For more information, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*
Repository Creation Utility (RCU)	Oracle Fusion Middleware Repository Creation Utility (RCU) is available on the Oracle Technology Network (OTN) web site. For more information about using RCU, see *Oracle Fusion Middleware Repository Creation Utility User's Guide*. **Note**: All required schema must be created before installing some of the Oracle Identity and Access Management components. For more information, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
Access Manager	For more information, see "Installing Oracle Identity and Access Management" and "Configuring Access Manager" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
Oracle HTTP Server	For more information, see "Installing and Configuring Oracle HTTP Server 11g Webgate for OAM" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. The OHS profile must be updated so the Oracle Identity Manager administration pages launch correctly after integration with Access Manager is completed. For more information, see Configuring Oracle HTTP Server.

Table 7–2 (Cont.) Required Components for Integration Scenario

Component	Information
Oracle Identity Manager	For more information, see "Installing and Configuring Oracle Identity and Access Management" and "Configuring Oracle Identity Manager" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. **Note**: When configuring Oracle Identity Manager, the LDAP directory must be preconfigured before you can use it as an Identity Store. Ensure that all installation instructions are followed, including any prerequisites for enabling LDAP synchronization. For more information, see: ■ "Configuring OIM Server", ■ "Completing the Prerequisites for Enabling LDAP Synchronization", and ■ "Creating Adapters in Oracle Virtual Directory" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. **Note**: You must create the wlfullclient.jar when installing Oracle Identity Manager and this file must be present before performing the integration steps. Follow the installation instructions carefully.
Oracle Virtual Directory	For more information, see "Configuring Oracle Virtual Directory" in *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. Before you can start using Oracle Virtual Directory with an Identity Store, you must create adapters for each of the directories you want to use. For each adapter, the `oamEnabled` parameter must be set to `true` for this integration scenario. For more information, see "Creating Adapters in Oracle Virtual Directory" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
Oracle Internet Directory	For more information, see "Configuring Oracle Internet Directory" in *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
Oracle SOA Suite	For more information, see *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*

7.4 Configuring the Identity Store

The Identity Store must be configured so it can be used by Access Manager, Oracle Identity Manager, and Oracle WebLogic Server. It must be seeded with the required users and groups.

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

7.4.1 Extending Directory Schema for Access Manager

Use `idmConfigTool` to configure the Identity Store to extend the schema in Oracle Internet Directory. For more information about the `idmConfigTool` command, see Chapter 2, "Using the idmConfigTool Command".

1. Set the environment variables required for `idmconfigtool`. For information, see Section 2.2, "Set Up Environment Variables".
2. Create a properties file, for example, named `extendOAMPropertyFile`, with contents similar to the following.

```
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=mycompany,dc=com
```

   Where:

   - `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, then `IDSTORE_HOST` should point to Oracle Internet Directory, even if you are fronting Oracle Internet Directory with Oracle Virtual Directory.

     If you are using a directory other than Oracle Internet Directory, specify the Oracle Virtual Directory host (which should be `IDSTORE.mycompany.com`.)
   - `IDSTORE_BINDDN` is an administrative user in the Identity Store directory.
   - `IDSTORE_USERNAMEATTRIBUTE` is used to set and search for users in the identity store.
   - `IDSTORE_LOGINATTRIBUTE` is the login attribute of the identity store which contains the user's login name.
   - `IDSTORE_USERSEARCHBASE` is the location in the directory where users are stored.
   - `IDSTORE_GROUPSEARCHBASE` is the location in the directory where groups are stored.
   - `IDSTORE_SEARCHBASE` is the location in the directory where users and groups are stored.
   - `IDSTORE_SYSTEMIDBASE` is the location of a container in the directory where users can be placed when you do not want them in the main user container. This happens rarely but one example is the Oracle Identity Manager reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.
3. Configure the Identity Store by using `idmConfigTool` with the `-preConfigIDStore` command, which is located at:

```
IAM_ORACLE_HOME/idmtools/bin
```

   The syntax of the command on Linux is:

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

The syntax on Windows is:

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

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 Virtual Directory:

```
Enter ID Store Bind DN password:
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/idm_
idstore_groups_template.ldif
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/idm_
idstore_groups_acl_template.ldif
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/systemid_pwdpolicy.ldif
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/idstore_tuning.ldif
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oid_
schema_extn.ldif
May 25, 2011 2:37:19 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/schema/OID_oblix_pwd_
schema_add.ldif
May 25, 2011 2:37:19 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/schema/OID_oim_pwd_schema_
add.ldif
May 25, 2011 2:37:19 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/schema/OID_oblix_schema_
add.ldif
May 25, 2011 2:37:34 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/schema/OID_oblix_schema_
index_add.ldif
The tool has completed its operation. Details have been logged to
automation.log
```

4. 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 tool.

   In addition to creating users, `idmConfigTool` creates the groups `OrclPolicyAndCredentialWritePrivilegeGroup` and `OrclPolicyAndCredentialReadPrivilegeGroup`.

7.4.2 Creating Users and Groups for Access Manager

Use `idmConfigTool` to seed the Identity Store with the users required by Access Manager as follows. For more information about the `idmConfigTool` command, see Chapter 2, "Using the idmConfigTool Command".

1. Set the environment variables required for `idmconfigtool`.

2. Create a properties file, for example, named `preconfigOAMPropertyFile`, with contents similar to the following. This file will be used to preconfigure the Identity Store.

```
IDSTORE_HOST : idstore.mycompany.com
IDSTORE_PORT : 389
IDSTORE_BINDDN : cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=mycompany,dc=com
POLICYSTORE_SHARES_IDSTORE: true
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN:OAMAdministrators
IDSTORE_OAMSOFTWAREUSER:oamLDAP
IDSTORE_OAMADMINUSER:oamadmin
```

   Where:

   - `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, then `IDSTORE_HOST` should point to Oracle Internet Directory, even if you are fronting Oracle Internet Directory with Oracle Virtual Directory.

     If you are using a directory other than Oracle Internet Directory, specify the Oracle Virtual Directory host.

   - `IDSTORE_BINDDN` is an administrative user in the Identity Store directory.
   - `IDSTORE_USERNAMEATTRIBUTE` is used to set and search for users in the identity store.
   - `IDSTORE_LOGINATTRIBUTE` is the login attribute of the identity store which contains the user's login name.
   - `IDSTORE_USERSEARCHBASE` is the location in the directory where users are stored.
   - `IDSTORE_GROUPSEARCHBASE` is the location in the directory where groups are stored.
   - `IDSTORE_SEARCHBASE` is the location in the directory where users and groups are stored.
   - `POLICYSTORE_SHARES_IDSTORE` is set to `true` if your Policy and Identity Stores are in the same directory. If not, it is set to `false`.
   - `OAM11G_IDSTORE_ROLE_SECURITY_ADMIN` is the name of the group which is used to allow access to the Oracle Access Management administration console.
   - `IDSTORE_OAMSOFTWAREUSER` is the name of the user you use to interact with the LDAP server.
   - `IDSTORE_OAMADMINUSER` is the name of the user you want to create as your Oracle Access Management Administrator.

3. Configure the Identity Store by using `idmConfigTool` with the `-prepareIDStore` command, which is located at:

```
IAM_ORACLE_HOME/idmtools/bin
```

   The syntax of the command on Linux is:

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

The syntax on Windows is:

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

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

Sample command output:

```
Enter ID Store Bind DN password:
May 25, 2011 2:44:59 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
schema_extn.ldif
*** Creation of Oblix Anonymous User ***
May 25, 2011 2:44:59 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
10g_anonymous_user_template.ldif
Enter User Password for oblixanonymous:
Confirm User Password for oblixanonymous:
*** Creation of oamadmin ***
May 25, 2011 2:45:08 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
user_template.ldif
Enter User Password for oamadmin:
Confirm User Password for oamadmin:
*** Creation of oamLDAP ***
May 25, 2011 2:45:16 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
user_template.ldif
Enter User Password for oamLDAP:
Confirm User Password for oamLDAP:
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/common/oam_user_group_read_
acl_template.ldif
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oim_
group_template.ldif
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
group_member_template.ldif
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
config_acl.ldif
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oid_
schemaadmin.ldif
The tool has completed its operation. Details have been logged to
automation.log
```

4. Check the log file for any errors or warnings and correct them. The automation.log file is created in the directory from where you run the tool.

7.4.3 Creating Users and Groups for Oracle Identity Manager

Use `idmConfigTool` to seed the Identity Store with the users required by Oracle Identity Manager as follows. For more information about the `idmConfigTool` command, see Chapter 2, "Using the idmConfigTool Command".

A system user is required for performing operations in Oracle Internet Directory on behalf of Oracle Identity Manager. Create this user in the system container and give it the permissions appropriate for controlling all the containers Oracle Identity Manager communicates with. Oracle Virtual Directory uses these credentials to connect to the backend directories.

1. Set the environment variables required for `idmconfigtool`.
2. Create a properties file, for example, named `preconfigOIMPropertyFile`, with contents similar to the following. The file will be used to preconfigure the Identity Store.

```
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=mycompany,dc=com
IDSTORE_OIMADMINUSER: oimLDAP
IDSTORE_OIMADMINGROUP: OIMAdministrators
```

   Where:

   - `IDSTORE_HOST` and `IDSTORE_PORT` are, respectively, the host and port of your Identity Store directory. If your Identity Store is in Oracle Internet Directory, then `IDSTORE_HOST` should point to Oracle Internet Directory, even if you are fronting Oracle Internet Directory with Oracle Virtual Directory.

     If you are using a non-OID directory, then specify the Oracle Virtual Directory host (which should be `IDSTORE.mycompany.com`).
   - `IDSTORE_BINDDN` is an administrative user in the Identity Store directory.
   - `IDSTORE_USERNAMEATTRIBUTE` is used to set and search for users in the Identity Store.
   - `IDSTORE_LOGINATTRIBUTE` is the login attribute of the Identity Store which contains the user's login name.
   - `IDSTORE_USERSEARCHBASE` is the location in your Identity Store where users are placed.
   - `IDSTORE_GROUPSEARCHBASE` is the location in your Identity Store where groups are placed.
   - `IDSTORE_SEARCHBASE` is the location in the directory where users and groups are stored.
   - `POLICYSTORE_SHARES_IDSTORE` is set to `true` if your Policy and Identity Stores are in the same directory. If not, it is set to `false`.
   - `IDSTORE_SYSTEMIDBASE` is the location in your directory where the Oracle Identity Manager reconciliation user is placed.
   - `IDSTORE_OIMADMINUSER` is the user that Oracle Identity Manager uses to connect to the Identity Store.
   - `IDSTORE_OIMADMINGROUP` is the name of the group you want to create to hold your Oracle Identity Manager administrative users.

3. Configure the Identity Store by using `idmConfigTool` with the `-prepareIDStore` command, which is located at:

   `IAM_ORACLE_HOME/idmtools/bin`

   The syntax of the command on Linux is:

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

   The syntax on Windows is:

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

   When the command runs, you are prompted to enter the password of the account used to connect to the Identity Store. You are also asked to create passwords for the following accounts:

   - `IDSTORE_OIMADMINUSER`
   - `xelsysadm`. It is recommended you set this to the same value as the account you create as part of the Oracle Identity Manager configuration.

   Sample command output:

```
Enter ID Store Bind DN password:
*** Creation of oimLDAP ***
Apr 5, 2011 4:58:51 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oim_user_template.ldif
Enter User Password for oimLDAP:
Confirm User Password for oimLDAP:
Apr 5, 2011 4:59:01 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oim_group_template.ldif
Apr 5, 2011 4:59:01 AM oracle.ldap.util.LDIFLoader loadOneLdifFileINFO: ->
LOADING:
 /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oim_group_member_
template.ldif
Apr 5, 2011 4:59:01 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oim_groups_acl_
template.ldif
Apr 5, 2011 4:59:01 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
 /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oim_reserve_
template.ldif
*** Creation of Xel Sys Admin User ***
Apr 5, 2011 4:59:01 AM oracle.ldap.util.LDIFLoader loadOneLdifFileINFO: ->
LOADING:
 /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_user_template.ldif
Enter User Password for xelsysadm:
Confirm User Password for xelsysadm:
The tool has completed its operation. Details have been logged to
/home/oracle/idmtools/oim.log
```

4. Check the log file for any errors or warnings and correct them. The automation.log file is created in the directory from where you run the tool.

7.4.4 Creating Users and Groups for Oracle WebLogic Server

To enable single sign-on for your administrative consoles, you must ensure that there is a user in your Identity Store that has the permissions to log in to your WebLogic

Server administration console and Oracle Enterprise Manager Fusion Middleware Control. Use idmConfigTool to seed the Identity Store with the users required by WebLogic Server as follows. For more information about idmConfigTool command, see Chapter 2, "Using the idmConfigTool Command".

1. Set the environment variables required for idmconfigtool.
2. Create a properties file, for example, named preconfigWLSPropertyFile, with contents similar to the following. The file will be used to preconfigure the Identity Store.

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

   Where:

   - 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, then IDSTORE_HOST should point to Oracle Internet Directory, even if you are fronting Oracle Internet Directory with Oracle Virtual Directory.

     If you are using a directory other than Oracle Internet Directory, specify the Oracle Virtual Directory host (which should be IDSTORE.*mycompany*.com.)
   - IDSTORE_BINDDN is an administrative user in the Identity Store directory.
   - IDSTORE_USERNAMEATTRIBUTE is used to set and search for users in the Identity Store.
   - IDSTORE_LOGINATTRIBUTE is the login attribute of the Identity Store which contains the user's login name.
   - IDSTORE_WLSADMINUSER is the Identity store administrator for Oracle WebLogic Server.
   - IDSTORE_WLSADMINGROUP is the Identity Store administrator group for Oracle WebLogic Server.
   - IDSTORE_USERSEARCHBASE is the location in the directory where users are stored.
   - IDSTORE_GROUPSEARCHBASE is the location in the directory where groups are stored.
   - IDSTORE_SEARCHBASE is the location in the directory where users and groups are stored.
   - POLICYSTORE_SHARES_IDSTORE is set to true if your Policy and Identity Stores are in the same directory. If not, it is set to false.

3. Configure the Identity Store by using idmConfigTool with -prepareIDStore command, which is located at:

```
IAM_ORACLE_HOME/idmtools/bin
```

The syntax of the command on Linux is:

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

The syntax on Windows is:

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

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

Sample command output:

```
Enter ID Store Bind DN password:
May 25, 2011 2:44:59 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
schema_extn.ldif
*** Creation of Oblix Anonymous User ***
May 25, 2011 2:44:59 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
10g_anonymous_user_template.ldif
Enter User Password for oblixanonymous:
Confirm User Password for oblixanonymous:
*** Creation of oamadmin ***
May 25, 2011 2:45:08 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
user_template.ldif
Enter User Password for oamadmin:
Confirm User Password for oamadmin:
*** Creation of oamLDAP ***
May 25, 2011 2:45:16 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
user_template.ldif
Enter User Password for oamLDAP:
Confirm User Password for oamLDAP:
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/common/oam_user_group_read_
acl_template.ldif
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oim_
group_template.ldif
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
group_member_template.ldif
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oam_
config_acl.ldif
May 25, 2011 2:45:21 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oid_
schemaadmin.ldif
The tool has completed its operation. Details have been logged to
automation.log
```

4. Check the log file for any errors or warnings and correct them. The automation.log file is created in the directory from where you run the tool.

7.5 Configuring Access Manager for Integration

Before integrating Oracle Identity Manager with Access Manager 11*g*, you must extend Access Manager 11*g* to support Oracle Identity Manager. For more information about `idmConfigTool` command, see Chapter 2, "Using the idmConfigTool Command"

1. Set the environment variables required for `idmconfigtool`.
2. Update the domain agent password as follows:
   a. Log in to the Oracle Access Management administration console:

      `http://oam_adminserver_host:port/oamconsole`

   b. Navigate to the **System Configuration** tab, then **Access Manager Settings**, then **SSO Agents**.

      Double-click **OAM Agents**. A Webgate page displays.

      Click **Search** to list all Webgate agents.

      Double-click **IAMSuiteAgent**. Update the field **Access Client Password** with the desired password.

   c. Log in to the Oracle WebLogic Server administration console:

      `http:oam_adminserver_host:port/console`

   d. Navigate to **Security Realms**, then **myrealm**. Open the **Providers** tab and edit **IAMSuiteAgent**.

      Open the **Provider Specific** tab and update the agent password. Save the changes.

   e. Restart the OAM Server.
3. Create a properties file, for example, named `OAMconfigPropertyFile`, with contents similar to the following:

```
WLSHOST: adminvhn.mycompany.com
WLSPORT: 7001
WLSADMIN: weblogic
WLSPASSWD: weblogic password
ADMIN_SERVER_USER_PASSWORD: for example, welcome1
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_OAMSOFTWAREUSER: oamLDAP
IDSTORE_OAMADMINUSER: oamadmin
IDSTORE_DIRECTORYTYPE: OVD
POLICYSTORE_SHARES_IDSTORE: true
PRIMARY_OAM_SERVERS: oamhost1.mycompany.com:5575,oamhost2.mycompany.com:5575
WEBGATE_TYPE: ohsWebgate10g
ACCESS_GATE_ID: Webgate_IDM
OAM11G_IDM_DOMAIN_OHS_HOST:sso.mycompany.com
OAM11G_IDM_DOMAIN_OHS_PORT:443
OAM11G_IDM_DOMAIN_OHS_PROTOCOL:https
OAM11G_WG_DENY_ON_NOT_PROTECTED: false
```

```
OAM11G_IMPERSONATION_FLAG: true (if used)
OAM_TRANSFER_MODE: simple
OAM11G_OAM_SERVER_TRANSFER_MODE:simple
OAM11G_IDM_DOMAIN_LOGOUT_URLS:
/console/jsp/common/logout.jsp,/em/targetauth/emaslogout.jsp,/oamsso/logout.htm
l,/cgi-bin/logout.pl
OAM11G_OIM_WEBGATE_PASSWD: webgate password
OAM11G_SERVER_LOGIN_ATTRIBUTE: uid
COOKIE_DOMAIN: .mycompany.com
OAM11G_IDSTORE_NAME: name of ID store
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
OAM11G_SSO_ONLY_FLAG: false
OAM11G_OIM_INTEGRATION_REQ: true
OAM11G_SERVER_LBR_HOST:sso.mycompany.com
OAM11G_SERVER_LBR_PORT:443
OAM11G_SERVER_LBR_PROTOCOL:https
COOKIE_EXPIRY_INTERVAL: 120
OAM11G_OIM_OHS_URL:https://sso.mycompany.com:443/
SPLIT_DOMAIN: true
```

Where:

- WLSHOST and WLSPORT are, respectively, the host and port of your administration server, this will be the virtual name.
- WLSADMIN and WLSPASSWD are, respectively, the WebLogic Server administrative user and password you use to log in to the WebLogic Server administration console.
- IDSTORE_HOST and IDSTORE _PORT are, respectively, the host and port of your Identity Store directory.

  Note: If using a directory server other than Oracle Internet Directory, specify the Oracle Virtual Directory host and port.

- IDSTORE_BINDDN is an administrative user in Oracle Internet Directory.

  Note: If using a directory server other than Oracle Internet Directory, specify an Oracle Virtual Directory administrative user.

- IDSTORE_USERNAMEATTRIBUTE is used to set and search for users in the Identity Store.
- IDSTORE_LOGINATTRIBUTE is the login attribute of the Identity Store which contains the user's login name.
- IDSTORE_USERSEARCHBASE is the container under which Access Manager searches for the users.
- IDSTORE_SEARCHBASE is the location in the directory where users and groups are stored.
- IDSTORE_GROUPSEARCHBASE is the location in the directory where groups are stored.
- IDSTORE_OAMSOFTWAREUSER is the name of the user you use to interact with the LDAP server.

- IDSTORE_OAMADMINUSER is the name of the user you use to access your Oracle Access Management administration console.
- IDSTORE_DIRECTORYTYPE is the Identity Store directory type.
- PRIMARY_OAM_SERVERS is a comma-separated list of your Access Manager servers and the proxy ports they use.

Note: To determine the proxy ports your Access Manager servers:

1. Log into the Oracle Access Management administration console at `http://admin.mycompany.com:7001/oamconsole`
2. Click the **System Configuration** tab.
3. Expand **Server Instances** under the Common Configuration section.
4. Click on an Access Manager server, such as **WLS_OAM1**, and click **Open**.
5. Proxy port is shown as **Port**.

- WEBGATE_TYPE is the type of Webgate agent you want to create. Valid values are ohsWebgate10g.
- ACCESS_GATE_ID is the name you want to assign to the Webgate. Do *not* change the property value shown above.
- OAM11G_IDM_DOMAIN_OHS_HOST is the name of the load balancer which is in front of OHS.
- OAM11G_IDM_DOMAIN_OHS_PORT is the port that the load balancer listens on.
- OAM11G_IDM_DOMAIN_OHS_PROTOCOL is the protocol to use when directing requests at the load balancer.
- OAM11G_WG_DENY_ON_NOT_PROTECTED is set to deny on protected flag for 10g Webgate. Valid values are true and false.
- OAM11G_IMPERSONATION_FLAG is set to enable (true) or disable (false) impersonation in the OAM Server.
- OAM_TRANSFER_MODE is the security model in which the access servers function.
- OAM11G_OAM_SERVER_TRANSFER_MODE is the security model for the Access Manager servers.
- OAM11G_IDM_DOMAIN_LOGOUT_URLS is set to the various logout URLs.
- OAM11G_OIM_WEBGATE_PASSWD is the password you want to assign to the Webgate.
- OAM11G_SERVER_LOGIN_ATTRIBUTE setting to uid ensures that when users log in their username is validated against the uid attribute in LDAP.
- COOKIE_DOMAIN is the domain in which the Webgate functions.
- OAM11G_IDSTORE_NAME is the name of the Identity Store. If you already have an Identity Store in place which is different from the default created by this tool, set this parameter to the name of that Identity Store.
- OAM11G_IDSTORE_ROLE_SECURITY_ADMIN is the account to administer role security in identity store.
- OAM11G_SSO_ONLY_FLAG configures Access Manager 11*g* as authentication only mode or normal mode, which supports authentication and authorization.

If OAM11G_SSO_ONLY_FLAG is true, the Access Manager 11*g* 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 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_SSO_ONLY_FLAG determines whether Access Manager is used in authentication-only mode.
- OAM11G_SERVER_LBR_HOST is the name of the OAM Server fronting your site. This and the following two parameters are used to construct your login URL.
- OAM11G_SERVER_LBR_PORT is the port that the load balancer is listening on.
- OAM11G_SERVER_LBR_PROTOCOL is the URL prefix to use.
- COOKIE_EXPIRY_INTERVAL is the cookie expiration period.
- OAM11G_OIM_OHS_URL is the URL of the load balancer or OHS fronting the OIM server.
- SPLIT_DOMAIN set to true is required to suppress the double authentication of Oracle Access Management administration console in a split domain scenario.

4. Configure the Identity Store by using idmConfigTool with the -configOAM command, which is located at:

   ```
   IAM_ORACLE_HOME/idmtools/bin
   ```

   The syntax of the command on Linux is:

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

   The syntax on Windows is:

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

   When the command runs, you are prompted to enter the password of the account used to connect to the Identity Store. You are also asked to create passwords for the following accounts:

   - IDSTORE_PWD_OAMSOFTWAREUSER
   - IDSTORE_PWD_OAMADMINUSER

   Sample command output:

   ```
   Enter ID Store Bind DN password:
   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.
6. Restart WebLogic Administration Server.

7.6 Integrating Access Manager with Oracle Identity Manager

Integrate Oracle Identity Manager with Access Manager as follows. For information about `idmConfigTool` command, see Chapter 2, "Using the idmConfigTool Command".

1. Set the environment variables required for `idmconfigtool`.
2. Create a properties file, for example, named `OIMconfigPropertyFile`, with contents similar to the following:

```
LOGINURI: /${app.context}/adfAuthentication
LOGOUTURI: /oamsso/logout.html
AUTOLOGINURI: None
ACCESS_SERVER_HOST: OAMHOST1.mycompany.com
ACCESS_SERVER_PORT: 5575
ACCESS_GATE_ID: Webgate_IDM
COOKIE_DOMAIN: .mycompany.com
COOKIE_EXPIRY_INTERVAL: 120
OAM_TRANSFER_MODE: SIMPLE
WEBGATE_TYPE: ohsWebgate10g
OAM_SERVER_VERSION: 11g (use 10g if Oracle Access Manager 10g is used)
OAM11G_WLS_ADMIN_HOST: OAM_DOMAIN_ADMIN_HOST (if cross domain is used)
OAM11G_WLS_ADMIN_PORT: 17001 (if cross domain is used)
OAM11G_WLS_ADMIN_USER: weblogic (if cross domain is used)
SSO_ENABLED_FLAG: true
IDSTORE_PORT: 389
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_DIRECTORYTYPE: OVD
IDSTORE_ADMIN_USER: oamdmin. Note that the entry contains the complete LDAP DN
of the user (the username alone in insufficient). For example,
cn=oamLDAP,cn=Users,dc=mycompany,dc=com
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
MDS_DB_URL: jdbc:oracle:thin:@DBHOST:PORT:SID
MDS_DB_SCHEMA_USERNAME: idm_mds
WLSHOST: adminvhn.mycompany.com
WLSPORT: 7001
WLSADMIN: weblogic
DOMAIN_NAME: IDM_Domain
OIM_MANAGED_SERVER_NAME: WLS_OIM1
DOMAIN_LOCATION: ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain
```

Where:

- The `ACCESS_SERVER_PORT` must be the Access Manager NAP port.
- If your OAM Servers are configured to accept requests using the simple mode, set `OAM_TRANSFER_MODE` to `SIMPLE`. Otherwise set `OAM_TRANSFER_MODE` to `OPEN`.
- Set `WEBGATE_TYPE` to `ohsWebgate10g`.
- Set `OAM_SERVER_VERSION` to `10g` if using a 10*g* Webgate.
- For information about split domain integration topology, see Chapter 1, "Introduction".

- Set IDSTORE_PORT to your Oracle Internet Directory port if you are using Oracle Internet Directory as your Identity Store. If not, set it to your Oracle Virtual Directory port.
- Set IDSTORE_HOST to your Oracle Internet Directory host or load balancer name if you are using Oracle Internet Directory as your Identity Store. If not, set it to your Oracle Virtual Directory host or load balancer name.
- Set IDSTORE_DIRECTORYTYPE to OVD if you are using Oracle Virtual Directory server to connect to either a non-OID directory or Oracle Internet 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.
- MDS_DB_URL in this case represents a single instance database. The string following the '@' symbol must have the correct values for your environment. SID must be the actual SID, *not* a service name. If you are using a single instance database, then set MDS_URL to: jdbc:oracle:thin:@DBHOST:1521:SID.
- The value of IDSTORE_ADMIN_USER must contain the complete LDAP DN of the user. The entry should be similar to "cn=oamadmin,cn=Users,dc=us,dc=oracle,dc=com" instead of just "oamadmin".

3. Configure the Identity Store by using idmConfigTool with the -configOIM command, which is located at:

   ```
   IAM_ORACLE_HOME/idmtools/bin
   ```

   The syntax of the command on Linux is:

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

   The syntax on Windows is:

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

   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

   Sample output:

   ```
   Enter sso access gate password:
   Enter mds db schema password:
   Enter idstore admin password:
   Enter admin server user password:

   ********* Seeding OAM Passwds in OIM *********

   Enter ssoKeystore.jks Password:
   Enter SSO Global Passphrase:
   ```

```
Completed loading user inputs for - CSF Config

Updating CSF with Access Gate Password...

WLS ManagedService is not up running. Fall back to use system properties for
configuration.
Updating CSF ssoKeystore.jks Password...

Updating CSF for SSO Global Passphrase Password...


********* ********* *********


********* Activating OAM Notifications *********


Completed loading user inputs for - MDS DB Config

Initialized MDS resources

Apr 11, 2011 4:57:45 AM oracle.mds
NOTIFICATION: transfer operation started.
Apr 11, 2011 4:57:46 AM oracle.mds
NOTIFICATION: 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

Apr 11, 2011 4:57:46 AM oracle.mds
NOTIFICATION: transfer operation started.
Apr 11, 2011 4:57:47 AM oracle.mds
NOTIFICATION: 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

Apr 11, 2011 4:57:47 AM oracle.mds
NOTIFICATION: transfer operation started.
```

```
Apr 11, 2011 4:57:47 AM oracle.mds
NOTIFICATION: 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 - Dogwood Admin WLS


Completed loading user inputs for - LDAP connection info

Connecting to t3://adminvhn.mycompany.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

Validated authentication provider state successfuly.

Created OAMIDAsserter successfuly

Created OIDAuthenticator successfuly

Created OIMSignatureAuthenticator successfuly

Setting attributes for OID Authenticator

All attributes set. Configured in OID Authenticator now

lDAP details configured in OID authenticator

Control flags for authenticators set sucessfully

Reordering of authenticators done sucessfully

Saving the transaction

Transaction saved

Activating the changes

Changes Activated. Edit session ended.
```

```
    Connection closed sucessfully


    ********* ********* *********
```

4. Check the log file for errors and correct them if necessary.
5. Restart the Oracle Identity Manager managed server and the WebLogic Administration Server.

7.7 Configuring Oracle HTTP Server

The Oracle HTTP Server with 11*g* Webgate must be installed. For more information, see "Installing and Configuring Oracle HTTP Server 11g Webgate for OAM" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. For information about installing with 10*g* Webgate, see "Managing 10g Webgates with Access Manager 11g" and "Configuring Apache, OHS, IHS for 10g Webgates" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

The Oracle HTTP Server (OHS) profile must be edited so the OHS server points to the OIM server that is being protected by Access Manager. Edit the OHS profile to include the following lines.

```
<Location /identity>
    SetHandler weblogic-handler
    WLCookieName oimjsessionid
    WebLogicHost <OIM managed server host>
WebLogicPort <OIM managed server host>
    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 host>
WLCookieName oimjsessionid
WLLogFile "${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 host>
WLCookieName oimjsessionid
```

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

The OHS instance must be restarted afterward.

7.8 Configuring Centralized Logout

For information, see "Configuring Centralized Logout for the IAMSuiteAgent" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

7.9 Starting Servers with Domain Agent Removed

The IDMDomain Agent provides single sign-on capability for administration consoles. The Webgate handles single sign-on, so you must remove the IDMDomain Agent and restart the Oracle WebLogic Server Administration Server and all running Managed Servers.

1. Log in to the WebLogic Server administration console using the URL: http://admin.*mycompany*.com/console.
2. Select **Security Realms** from the **Domain Structure** menu.
3. Click **myrealm**.
4. Click the **Providers** tab.
5. Click **Lock and Edit** from the Change Center.
6. In the list of authentication providers, select **IAMSuiteAgent**.
7. Click **Delete**.
8. Click **Yes** to confirm the deletion.
9. Click **Activate Changes** from the Change Center.
10. Restart WebLogic Administration Server and all running Managed Servers.

    For information, see "Starting and Stopping Oracle WebLogic Server Instances" in *Oracle Fusion Middleware Administrator's Guide*

7.10 Additional Configuration Tasks

This section describes additional configuration that you may need to perform depending on your requirements.

This section contains the following topics:

- Migrating from the Domain Agent to 10g Webgate with OHS 11g
- Updating SOA Server Default Composite

7.10.1 Migrating from the Domain Agent to 10*g* Webgate with OHS 11*g*

Perform this task only if you want to use Oracle HTTP Server 10*g* Webgate for Access Manager after setting up integration between Oracle Identity Manager and Access Manager. Follow the instructions in "Migrating from Domain Agent to Oracle HTTP Server 10g Webgate for OAM" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Next, complete the configuration by performing these actions:

- Update Webgate Type and ID
- Set the Webgate Preferred Host
- Create the Oracle Identity Manager SSO Keystore

7.10.1.1 Update Webgate Type and ID

Perform these steps to update the Webgate Type and Webgate ID using Oracle Enterprise Manager Fusion Middleware Control:

1. Navigate to **Identity and Access**, then **OIM**, then **oim(11.1.1.3.0)**.
2. Right-click on **oim (11.1.1.3.0)** and select **System Mbean Browser**.
3. Navigate to **Application Defined Mbeans**, then **oracle.iam**, then Server: oim_server1, then Application:oim, then **XMLConfig**, then **Config**, then **XMLConfig.SSOConfig**, then **SSOConfig**.

7.10.1.2 Set the Webgate Preferred Host

This step is required to redirect users to the Oracle Access Management login page for Oracle Identity Manager if they type in a URL of the form:

`http://`*`OHS_HOST:OHS_PORT`*`/admin/faces/pages/Admin.jspx`

Perform these steps to set the preferred Webgate host:

1. Log in to the Oracle Access Management administration console, click **System Configuration** tab, and navigate to **Access Manager Settings**, then **SSO Agents**, then **OAM Agent**.
2. Click the **Search** button. A list of Webgate IDs appears. Open the desired registration page.
3. Update the Preferred Host field and set it to IAMSuiteAgent.
4. Click **Apply**.
5. Restart Oracle HTTP Server.

7.10.1.3 Create the Oracle Identity Manager SSO Keystore

Note: This step is needed if WebGate is configured in simple mode.

Follow the instructions in "Creating Oracle Identity Manager SSO Keystore" in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

7.10.2 Updating SOA Server Default Composite

In an integrated environment, Oracle Identity Manager is front ended by OHS. All SOA server default composites must be updated. Perform the following steps:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control Console.
2. Navigate to **SOA**, then **soa-infra** (***SOA server name***), then **default**.

   Update the composite types applicable to your environment. For example: `ApprovalTask`, `Human Workflow`, `DisconnectedProvisiong`, etc.

See Also: The Fusion Middleware Control online help and SOA Suite documentation

3. For each default composite, perform the following:
   a. Click the ***composite name***.
   b. From Component Metrics select the composite type. For example, click **ApprovalTask**.
   c. Select the **Administration** tab and update the fields as follows:

      Host Name: *OHS host name*

      HTTP Port: If SSL mode, leave blank. If non-SSL mode, enter *OHS HTTP port*.

      HTTPS Port: If SSL mode, enter *OHS HTTS port*. If non-SSL mode, leave blank.
   d. Click **Apply**.

Note: If the values are not updated correctly, the composite page in Oracle Identity Manager will open as a blank page.

7.11 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 7.11.1, "Validate OIM SSOConfig".
- The realm security providers in *OIM_DOMAIN_HOME*/config.xml. See Section 7.11.2, "Validate Security Provider Configuration".
- The OIM domain credential store in *OIM_DOMAIN_HOME*/config/fmwconfig/cwallet.sso. See Section 7.11.3, "Validate OIM Domain Credential Store".
- The orchestration event-handlers required for SSO integration in Eventhandler.xml, stored in the OIM Metadata store. See Section 7.11.4, "Validate Event Handlers for SSO".
- The SSO logout configuration in *OIM_DOMAIN_HOME*/config/fmwconfig/jps-config.xml. See Section 7.11.5, "Validate SSO Logout Configuration".

7.11.1 Validate OIM SSOConfig

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

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

For more information, see "Getting Started Using the Fusion Middleware Control MBean Browsers" in *Oracle Fusion Middleware 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 `TapEndpoinURL` attribute is present.
   - If using NAP 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.

7.11.2 Validate Security Provider Configuration

To validate the security provider configuration:

1. In WebLogic Server Administration Console, navigate to the **OIM domain**.
2. Navigate to **Security Realms**, **myrealm**, then **Providers** tab.
3. Confirm the Authentication Providers are configured as follows.

Authentication Provider	Control Flag
OAM ID Asserter	REQUIRED
DefaultAuthenticator	SUFFICIENT
OIM Signature Authenticator	SUFFICIENT
OIM Authenticator	OPTIONAL
LDAP Authenticator	SUFFICIENT

4. Navigate to **OIM Authenticator**, **Provider Specific**. Verify that the **SSOMode** checkbox is selected.
5. The LDAP Authenticator varies depending upon which LDAP provider is being used. Verify it is configured correctly by selecting **Users and Groups** tab, and confirming the LDAP users are listed in **Users** tab.

7.11.3 Validate OIM 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

7.11.4 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 EventHanlders.xml file, located at /db/ssointg/EventHandlers.xml.

To confirm all event handlers are configured correctly, do the following:

- Connect to the OIM MDS scheme and look for /db/ssointg/EventHandlers.xml in the MDS_PATHS table, PATH_FULLNAME column.
- Export the EventHandlers.xml file. For more information, see 'Deploying and Undeploying Customizations" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

7.11.5 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.

The following example is of the single logout configuration in *OIM_DOMAIN_HOME*/config/fmwconfig/jps-config.xml file:

```
<propertySet name="props.auth.uri.0">
            <property name="logout.url" value="/oamsso/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>
```

7.12 Testing the Integration

The final task is to verify the integration by performing, in order, the steps shown in Table 7–3.

Table 7–3 Verifying Access Manager-Oracle Identity Manager Integration

Step	Description	Expected Result
1	Access the Oracle Access Management administration console using the URL: `http://admin_server_host:admin_server_port/oamconsole`	Provides access to the administration console.

2	Access the Oracle Identity Manager administration page with the URL:
	▪ For Oracle Identity Self Service:
	`http://hostname:port/identity/faces/home`
	▪ For Oracle Identity System Administration:
	`http://hostname:port/sysadmin/faces/home`
	where *hostname:port* can be for either OIM or OHS, depending on whether a Domain Agent or Webgate is used.
		The Oracle Access Management login page should appear.
		Verify the links for "Forgot Password", "Self Register" and "Track Registration" features appear in the login page. For more information about these features, see Section 1.5.3, "Password Management Scenarios".

3	Log in as an Oracle Identity Manager administrator.	The Oracle Identity Manager Admin Page should be accessible.
4	Create a new user using Oracle Identity Self Service. Close the browser and try accessing the OIM Identity Page. When prompted for login, provide valid credentials for the newly-created user.	You should be redirected to Oracle Identity Manager and be required to reset the password. After resetting the password and setting the challenge question, user should be automatically logged into the application. Auto-login should work.
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 a test user, then lock the test user account. Click the Logout link on the OIM console.	The user must be logged out and redirected back to the login page.
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.

7.13 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."

7.13.1 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 Re-Directed to Wrong Login Page
- Login Fails
- Oracle Access Management Console Login Page Does Not Display
- Authenticated User is Re-Directed to Oracle Identity Manager Login Page
- User is Re-Directed to Oracle Identity Manager Login Page
- New User is Not Re-Directed to Change Password
- User is Re-Directed in a Loop

7.13.1.1 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.

7.13.1.2 User is Re-Directed to Wrong Login Page

After accessing an Oracle Identity Manager resource using OHS (for example, `http://OHS_HOST:OHS_PORT/identity`), the user is re-directed 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 11*g* 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 Installation Guide for Oracle Identity and Access Management* and *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

7.13.1.3 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 **System Configuration**, **Data Sources**, **OIMIDStore**.
3. Verify the Default Store and System Store configuration.
4. Click **Test Connection** to verify the connection.

7.13.1.4 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

Restart the OAM Server.

Cause 2

The Webgate is not correctly deployed on OHS and is not configured correctly for the 10*g* or 11*g* 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 10*g* or 11*g* SSO Agent and then re-configure Webgate to use this Agent.

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

7.13.1.5 Authenticated User is Re-Directed to Oracle Identity Manager Login Page

User authenticated using the Oracle Access Management Console but is re-directed 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 7.11.2.

Cause 2

`OAMIDAsserter` is not configured correctly in Oracle WebLogic Server.

Solution 2

To resolve this problem:

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

7.13.1.6 User is Re-Directed 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 re-directs 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.DefaultRegistrationServi
ceProvider</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.mycompany.com</Setting>

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

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

</Setting>

             </Setting>

           </Setting>
```

7.13.1.7 New User is Not Re-Directed to Change Password

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

Cause

The Oracle Virtual Directory adapters 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 7.13.1.5). For example:

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

7.13.1.8 User is Re-Directed in a Loop

A new user attempts to access Oracle Identity Manager Self-Service and after successful authentication, the user is re-directed 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.mycompany.com

  WebLogicPort 8003

  WLLogFile "$
Unknown macro: {ORACLE_INSTANCE}
/diagnostics/logs/mod_wl/oim_component.log"

  </Location>
```

7.13.2 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 NAP 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 *Oracle Fusion Middleware Administrator's Guide*.

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

- If the version is 10*g*, the NAP channel is used during auto-login. See Section 7.13.2.1, "TAP Protocol Issues".

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

- If the version is 11*g*, the TAP channel is used during auto-login. See Section 7.13.2.2, "NAP Protocol Issues",

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

Note: In an 11gR2 Oracle Identity Manager and Access Manager integrated environment, the TAP protocol is configured for auto-login by default.

7.13.2.1 TAP Protocol Issues

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

7.13.2.1.1 404 Not Found Error After re-setting the password, user is re-directed 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.

7.13.2.1.2 System Error After re-setting the password, user is re-directed 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 OAM 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 OAM 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

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

Cause 3

After re-setting 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 sync 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 re-setting 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

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

7.13.2.2 NAP Protocol 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. Login to Oracle Access Management Console.
2. Navigate to the **IAMSuiteAgent**.
3. Check the host identifiers for `host:port` combination in the identifier. For example: `IAMSuiteAgent:/oim`
4. 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 pass phrase are seeded in correctly. For more information, see Section 7.11.3.

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 pass phrase also are seeded in correctly. For more information, see Section 7.11.3.

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 7.11.3.

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 7.13.1.1.
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 7.11.1.
   - If cookie domain is correct, then check for any time differences on the machines which host the OIM and OAM Servers.

7.13.3 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 NAP APIs to terminate the session. Communication is over the NAP channel.

To troubleshoot session termination issues:

1. Verify the NAP-related configuration is stored in Oracle Identity Manager `SSOConfig`. See Section 7.11.1.
2. Verify /db/sssointg/EvenHandlers.xml is in Oracle Identity Manager MDS. See Section 7.11.4.
3. Verify that `AccessGateID` attribute in Oracle Identity Manager `SSOConfig` points to a 10*g* 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 pass phrase (`SSOGobalPP`) in the OIM domain credential store.

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

7.13.4 Account Self-Locking Issues

If the user account is self-locked due to multiple invalid login attempts, the user can unlock it by logging in later with the correct password and then re-setting the password in Oracle Identity Manager.

If the user reset password operation fails:

1. Check if the user is locked in Oracle Identity Manager:
   a. Login to Identity Self service application as 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`.

7.13.5 Miscellaneous Issues

This provides solutions for the following miscellaneous issues:

- Client Based Login to Oracle Identity Manager Fails
- Logout Throws 404 Error

7.13.5.1 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 7.11.2.

7.13.5.2 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 7.11.5.

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="/oamsso/logout.html", autologinuri="/obrar.cgi")`
5. `exit`
6. Restart all servers in the domain

8

Integrating Access Manager and Oracle Adaptive Access Manager

Integrating Oracle Access Management Access Manager (Access Manager) and Oracle Adaptive Access Manager (OAAM) 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 explains how to integrate Oracle Adaptive Access Manager with Oracle Access Management Access Manager (Access Manager) to secure resources via risk-based authentication.

This chapter contains these sections:

> **Note:** Integration with Oracle Identity Manager provides additional features related to password collection. See Chapter 9, "Integrating Access Manager, OAAM, and OIM".

8.1 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 11*g* 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 Access Manager and Oracle Adaptive Access Manager in one of two ways:

- OAAM Basic integration with Access Manager
- OAAM Advanced integration with Access Manager

OAAM Basic integration with Access Manager, which is a native integration, requires the OAM Server and OAAM Admin Server in the Identity Management Middleware WebLogic Server Domain and a functional OAAM database. 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.

The Oracle Adaptive Access Manager libraries are bundled with the OAM server. Access Manager is integrated with Oracle Adaptive Access Manager through the extension libraries and uses them directly. 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. The OAAM Server is not needed in this deployment since the Oracle Adaptive Access Manager runtime functionalities are available through the libraries. Knowledge-based Authentication (KBA) is the only challenge mechanism available in this integration.

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".

Table 8–1 summarizes the Access Manager and Oracle Adaptive Access Manager integrations types.

Table 8–1 Types of Access Manager-Oracle Adaptive Access Manager Integration

Details	Basic	Advanced	Advanced Using TAP
Available	11.1.1.3.0 and above	11.1.1.3.0 and OAAM prior to 11.1.1.5 Refer to the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager* 11g Release 1 (11.1.1) for this version of OAAM Advanced integration with Access Manager.	11.1.1.5.0 and above Access Manager and OAAM integration using TAP is supported OAAM Advanced integration with Access Manager.
Features	Authentication schemes, device fingerprinting, risk analysis, and the Knowledge-based Authentication (KBA) challenge mechanism KBA is the only challenge mechanism available in this integration. Libraries and configuration interface for different flows (challenge, registration, and so on). Many of the login security use cases available from OAAM	Authentication schemes, device fingerprinting, risk analysis, KBA challenge mechanisms Advanced features and extensibility such as OTP Anywhere, challenge processor framework, shared library framework, and secure self-service password management flows. OAAM can also be integrated with third party single sign-on products via systems integrators if required.	Authentication schemes, device fingerprinting, risk analysis, KBA challenge mechanisms, and additional advanced security access features, such as step up authentication Advanced features and extensibility such as OTP Anywhere, challenge processor framework, shared library framework, and secure self-service password management flows. OAAM can also be integrated with third party single sign-on products via systems integrators if required.

Table 8–1 (Cont.) Types of Access Manager-Oracle Adaptive Access Manager Integration

Details	Basic	Advanced	Advanced Using TAP
OAAM Server	Embedded OAAM Server into Access Manager; therefore smaller footprint The Oracle Adaptive Access Manager extension libraries are bundled with the embedded OAM Server and used directly. A separate OAAM Server is not needed in this deployment since the Oracle Adaptive Access Manager runtime functionalities are available through the libraries. Libraries provide rules engine and the runtime functionality of Oracle Adaptive Access Manager. 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.	Complete integration with OAAM is required Requires a separate managed server for OAAM Server	Complete integration with OAAM is required Requires a separate managed server for OAAM Server
OAAM Admin Server	Required 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.	Required	Required
OAAM Database	Required	Required	Required

Table 8–1 (Cont.) Types of Access Manager-Oracle Adaptive Access Manager Integration

Details	Basic	Advanced	Advanced Using TAP
Supported Agents	10*g* WebGate and Single Sign-On (OSSO) Agent	10g WebGate	10*g* and 11*g* WebGates
Authentication Scheme	OAAMBasic Challenge Parameters: ■ oaamPostAuth=true ■ oaamPreAuth=true Specifications: ■ Authentication Level: 2 ■ Challenge Method: Form ■ Authentication Module: LDAP ■ Context Type: default ■ Context Value: /oam For information about the scheme, see "Managing Authentication Schemes" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.	OAAMAdvanced Specifications: ■ Authentication Level: 2 ■ Challenge Method: Form ■ Authentication Module: LDAP ■ Context Type: External For information about the scheme, see "Managing Authentication Schemes" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.	TAPScheme Challenge Parameters: ■ TAPPartnerId=TAPPartnerName ■ MatchLDAPAttribute=*user_name_attribute* ■ SERVER_HOST_ALIAS=HOST_ALIAS_1 Specifications: ■ Authentication Level: 2 ■ Challenge Method: DAP ■ Authentication Module: DAP ■ Context Type: External For information about the scheme, see "Managing Authentication Schemes" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
Where information is located	Section 8.3, "OAAM Basic Integration with Access Manager"	Refer to the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager* 11g Release 1 (11.1.1)	Chapter 9, "Integrating Access Manager, OAAM, and OIM"

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

8.2 Definitions, Acronyms, and Abbreviations

This section provides key definitions, acronyms, and abbreviations that are related to this integration.

Table 8–2 Advanced Integration Terms

Term	Definition
Action	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. For information, see "Managing Policies, Rules, and Conditions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Alert	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. Alert groups are used as results within rules so that when a rule is triggered all of the alerts within the groups are created. For information, see "Managing Policies, Rules, and Conditions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Authentication	The process of verifying a person's, device's, application's identity. Authentication deals with the question "Who is trying to access my services?"
Authentication Level	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. 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. The trust level is expressed as an integer value between 0 (no trust) and 99 (highest level of trust). 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. Current Authentication level is the current authentication level of the user. Target Authentication level is the authentication level required to access the protected resource.
Authorization	Authorization regards the question "Who can access what resources offered by which components?"
Authentication Scheme	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. 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.
Authentipad Checkpoint	The Authentipad checkpoint determines the type of device to use based on the purpose of the device.
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."

Table 8–2 (Cont.) Advanced Integration Terms

Term	Definition
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 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." 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 pads, 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: ■ Pre-authentication - Rules are run before a user completes the authentication process. ■ Post-authentication - Rules are run after a user is successfully authenticated. For information, see "Managing Policies, Rules, and Conditions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
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 computer, PDA, cell phone, kiosk, and other web-enabled device used by a user
Device fingerprinting	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. A customer typically uses these devices to log in: PC, notebook, mobile phone, smart phone, or other web-enabled machines.
Knowledge Based Authentication (KBA)	Knowledge-based authentication (KBA) is a secondary authentication method that provides an infrastructure based on registered challenge questions. Enables end-users to select questions and provide answers which are used to challenge them later on. Security administration include: ■ 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 For information, see "Managing Knowledge-Based Authentication" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

Table 8–2 (Cont.) Advanced Integration Terms

Term	Definition
KeyPad	Virtual keyboard for entry of passwords, credit card number, and so on. The KeyPad protects against Trojan or keylogging.
LDAPScheme	Authentication scheme used to protect Access Manager-related resources (URLs) for most directory types based on a form challenge method.
Multi-Level Authentication	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. 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". For information, see "Managing Authentication and Shared Policy Components" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
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)	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. For information, see "Setting Up OTP Anywhere" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Access Manager-OAAM TAP Integration	In Access Manager-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 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.
OAMAdminConsoleScheme	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 with 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 8–2 (Cont.) Advanced Integration Terms

Term	Definition
Policies	Policies contain security rules and configurations used to evaluate the level of risk at each checkpoint. For information, see "Managing Policies, Rules, and Conditions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Post-authentication rules	Post-authentication - Rules are run after a user is successfully authenticated. For information, see "Managing Policies, Rules, and Conditions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Pre-authentication rules	Pre-authentication - Rules are run before a user completes the authentication process. For information, see "Managing Policies, Rules, and Conditions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Profile	The customer's registration information including security phrase, image, challenge questions, challenge (question and OTP) counters, and OTP.
Protection level	There are three protection levels in which to choose from: ■ 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	Registration is the enrollment process, the opening of a new account, or other event where information is obtained from the user. 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.
Risk score	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.

Table 8–2 (Cont.) Advanced Integration Terms

Term	Definition
Rules	Fraud rules are used to evaluate the level of risk at each checkpoint. For information on policies and rules, see "OAAM Security and Autolearning Policies" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.
Step Up Authentication	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. Access Manager resources are graded by authentication level, which defines the relative sensitivity of a resource. 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.
Strong Authentication	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. Using more than one factor is sometimes called strong authentication or multi-factor authentication.
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	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. 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.
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 8–2 (Cont.) Advanced Integration Terms

Term	Definition
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 "Using Virtual Authentication Devices" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.
Web Agent	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. 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. 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.
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

8.3 OAAM Basic Integration with Access Manager

This section explains how to configure OAAM Basic integration with Access Manager.

> **See Also:** Section 9.1.1, "Deployment Options for Strong Authentication".

The following topics explain how this type of integration is implemented:

- Prerequisites
- Configuring OAAM Basic Integration with Access Manager

8.3.1 Prerequisites

Prior to configuring Access Manager with Oracle Adaptive 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 *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

The following are the required components that must be installed and configured before the integration tasks are performed.

Table 8–3 Required Components for Integration

Component	Information
Oracle Database	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 component. For more information, see "Database Requirements" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
WebLogic Servers	For more information, see *Installing Oracle WebLogic Server* and *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
Access Manager and Oracle Adaptive Access Manager schemas	Run RCU to create the schemas for Access Manager and OAAM. Oracle Fusion Middleware Repository Creation Utility is available on the Oracle Technology Network (OTN) Web site. For more information about using RCU, see *Oracle Fusion Middleware Repository Creation Utility User's Guide*.
Access Manager and Oracle Adaptive Access Manager	Install Access Manager and OAAM. 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 *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. 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 *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. Run the Oracle Identity Management 11*g* Fusion Middleware Configuration Wizard to configure Oracle Adaptive Access Manager and Access Manager in a new WebLogic administration domain or in an existing one. They can be on the same domain or different domains. Patch the software to the latest version. For information, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

8.3.2 Start WebLogic Server

Start the WebLogic Administration Server for the WebLogic Server domain.

```
DOMAIN_HOME/bin/startWeblogic.sh
```

8.3.3 Configuring OAAM Basic Integration with Access Manager

Follow the steps in this section to implement the Access Manager and Oracle Adaptive Access Manager integration.

Create a Policy to Protect Application

1. Log in to the Oracle Access Management Console:

   ```
   http://oam_adminserver_host:oam_adminserver_port/oamconsole
   ```

2. Select **Resources** under **IDMDomainAgent**.
3. Add the protected resource.

   For example, provide the following information for the resource:

   - **Host Identifier**: `IDMDomain`

- **Resource URL**: */resource/. . . /**

Create a New Authentication Policy

Create a new Authentication Policy under **IDMDomainAgent** 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 left pane, double-click **Application Domains**, then click **Search**, and in the search results, click **IAM Suite**.
2. Click the **Authentication** Policies tab and then the **Create Authentication Policy** button.
3. Add general policy details:

   Name: A unique name used as an identifier in the left pane. For example, `HighPolicy`.

   Authentication Scheme: `OAAMBasic`
4. Add global policy elements and specifications:

   Description (optional): Optional unique text that describes this authentication policy.

   Success URL: The redirect URL to be used upon successful authentication.

   Failure URL: The redirect URL to be used if authentication fails.
5. Add Resources:

   Choose the URL of a resource from those listed. 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.

   a. Click the Resources tab on the Authentication Policy page.

   b. Click the **Add** button on the tab.

   c. Choose the URL from the list. For example, `/higherriskresource`.
6. Click **Apply** to save changes and close the Confirmation window.
7. Add policy responses.

   Responses are the obligations (post authentication actions) to be carried out by the Web agent. After a successful authentication, the application server hosting the protected application should be able to assert the User Identity based on these responses.After a failed authentication, the browser redirects the request to a pre-configured URL
8. Close the page when you finish.

Create a New Authorization Policy

Create a new Authorization Policy.

1. In the left pane, double-click **Authorization Policies** and then the **Create** button.
2. Enter a unique name for this authorization policy.
3. On the Resource tab, click the **Add** button.
4. From the list provided, click a resource URL.

Resource URL: `IDMDomain:/<resource>/.../*`

5. Click **Apply** to save changes and close the Confirmation window.

Create User with Privileges to Log into the OAAM Administration Console

By default there is not a user that has the correct privileges to log in to the OAAM Administration console. You must create a user that has the correct privileges to log in to the OAAM Administration Console and then grant the necessary groups to the user.

1. Log in to the Oracle WebLogic Administration Console for your WebLogic administration domain.
2. Under Domain Structure in the left pane, select **Security Realms**.
3. On the Summary of Security Realms page, select the realm that you are configuring (for example, `myrealm`).
4. On the Settings for Realm Name page select **Users and Groups** and then **Users**.
5. 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/Confirmation
6. Click the newly created user, `user1`.
7. Click the **Groups** tab.
8. Assign any of the groups with the `OAAM` keyword to the user, `user1`.

   Move those groups from the left (available) to the right (chosen).
9. Click **Save**.

Modify oam-config.xml

Locate and modify the `oam-config.xml` file manually.

The `oam-config.xml` file contains all Access Manager-related system configuration data and is located in the *DOMAIN_HOME*`/config/fmwconfig` directory.

Set the `OAAMEnabled` property to `true` as shown in the following example:

```
<Setting Name="OAAM" Type="htf:map">
<Setting Name="OAAMEnabled" Type="xsd:boolean">true</Setting>
<Setting Name="passwordPage" Type="xsd:string">/pages/oaam/password.jsp</Setting>
<Setting Name="challengePage"
Type="xsd:string">/pages/oaam/challenge.jsp</Setting>
<Setting Name="registerImagePhrasePage"
Type="xsd:string">/pages/oaam/registerImagePhrase.jsp</Setting>
<Setting Name="registerQuestionsPage"
Type="xsd:string">/pages/oaam/registerQuestions.jsp</Setting>
```

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 to Create the Datasource in OAAM Basic Integration with Access Manager".

Start the OAAM Admin Server

Start the OAAM Admin Server, `oaam_admin_server1`, to register the newly created managed servers with the domain.

```
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 these instructions:

1. Log in to the OAAM Administration Console.

   `http://oaam_managed_server_host:oaam_admin_managed_server_port/oaam_admin`

2. Load the snapshot file from the *MW_HOME*/*IDM_ORACLE_HOME*/oaam/init directory into the system by following these instructions:

   a. In the left pane, open **System Snapshot** under the **Environment** node.

   b. Click the **Load from File** button.

      A Load and Restore Snapshot screen appears.

   c. Deselect **Back up current system now** and click **Continue**.

   d. 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**.

      The Load and Restore Snapshot page appears for you to choose a snapshot to load.

   e. Browse for `oaam_base_snapshot.zip` and click the **Load** button to load the snapshot into the system database.

      The default `oaam_base_snapshot.zip` is located in the *OAAM_HOME*`/oaam/init` directory.

   f. Click **OK** and then **Restore**.

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. For details, see Setting Up the Oracle Adaptive Access Manager Environment in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

You may encounter a non-working URL if policies and challenge questions are not available as expected in your Oracle Adaptive Access Manager environment.

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 Datasource

1. Access the Oracle WebLogic Administration Console:

   `http://weblogic_admin_server:7001/console`

2. If Oracle Adaptive Access Manager is not configured to be in the same WebLogic domain as Access Manager, perform the following steps for Access Manager:

- Create a datasource with the following JNDI name:

  `jdbc/OAAM_SERVER_DB_DS`

  Note: The name of the datasource 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 Oracle Adaptive Access Manager 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 **oam_server1** as targets with the datasource.
7. Click the **Activate** button in the upper left corner of the Oracle WebLogic Administration Console.

Test the Configuration

1. Access the protected resource configured in earlier to verify the configuration.

   At this point the configuration of Oracle Adaptive Access Manager is completed.

   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.
2. For verify the configuration, remote-register two agents, each protecting a resource.
3. 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 *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

8.4 OAAM Advanced Integration with Access Manager

Integrating Oracle Adaptive Access Manager with Oracle 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 Access Management Access Manager (Access Manager) 11g and Oracle Adaptive Access Manager (OAAM) 11g as an Advanced integration.

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 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 9, "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.

8.4.1 Integration Roadmap

Table 8–4 lists the high-level tasks for integrating Access Manager and Oracle Adaptive Access Manager.

The configuration instructions assume Access Manager and Oracle Adaptive Access Manager are integrated using the out-of-the box integration.

Table 8–4 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 users. Before you can access the OAAM Administration Console, you must create administration users.	For information, see "Creating the OAAM Admin 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 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	Validate that OAAM was set up correctly.	For information, see "Validating Initial Configuration of Oracle Adaptive Access Manager".
7	Register the WebGate agent. The WebGate is an out-of-the-box access client. This Web server access client intercepts HTTP requests for Web resources and forwards these to the OAM Server 11g.	For information, see "Registering WebGate Using the Oracle Access Management Console"

Table 8–4 (Cont.) Integration Flow for Access Manager and Oracle Adaptive Access Manager

Number	Task	Information
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	Add 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 a Password to the IAMSuiteAgent Profile in the Oracle Access Management Console"
10	Update the IAMSuiteAgent.	For information, see "Updating the IAMSuiteAgent in the WebLogic Administration Console".
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".

8.4.2 Integration Prerequisites

Prior to configuring Access Manager with Oracle Adaptive Access Manager, you must have installed all the required components, including any dependencies, and configure 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 *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

The following are the required components that must be installed and configured before the integration tasks are performed.

Table 8–5 Required Components for Integration

Component	Information
Oracle HTTP Server	For more information on installing the HTTP Server, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management.*
Oracle Access Manager 10g or Access Manager 11g agent (WebGate)	For information on installing the Oracle Access Management 11g WebGate, see "Installing and Configuring Oracle HTTP Server 11g WebGate" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. For information on installing the OAM 10g WebGate, see "Registering and Managing 10g Webgates with Access Manager 11g" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
Oracle Database	Ensure that you have an Oracle Database installed on your system before installing Access Manager and OAAM. The database must be up and running to install the products. For more information, see "Database Requirements" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
Repository Creation Utility (RCU)	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 *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* and *Oracle Fusion Middleware Repository Creation Utility User's Guide*. You will need to install and run RCU to create database schemas for Access Manager and OAAM.
Oracle Access Management Access Manager and Oracle Adaptive Access Manager schemas	Execute the Oracle Fusion Middleware Repository Creation Utility (RCU) to load the Access Manager and OAAM schemas into the database. **Note**: Ensure that the database and listener are running before creating the schemas.
Oracle WebLogic Servers	Install WebLogic servers. In this chapter, `OAM_HOME` is `OAM_WL_HOME/Oracle_IDM1`, and `OAAM_HOME` is `OAAM_WL_HOME/Oracle_IDM1`. For more information, see "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
Access Manager	You must install and configure Access Manager. 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. 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 *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
Oracle Adaptive Access Manager	You must install and configure Oracle Adaptive Access Manager: 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 *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

If so preferred, Oracle 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 "Oracle Adaptive Access Manager Command-Line Interface Scripts" in

the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager* for information on setting this parameter.

During the integration steps below, for reference we will refer to the WLS Domain which contains Oracle Access Manager as `OAM_DOMAIN_HOME`, and the WLS Domain which contains OAAM as `OAAM_DOMAIN_HOME`.

For information on installing the Identity Management Suite, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

8.4.3 Restarting the Servers

Before you can perform tasks in this section, ensure that the Access Manager and OAAM Administration Consoles and managed servers are running. To restart the servers, perform these steps:

1. Start the WebLogic Administration Server.

   OAM_DOMAIN_HOME/bin/startWeblogic.sh

   If OAAM is in a different domain, you must also start the WebLogic Administration Server located in `OAAM_Domain_Home`:

   OAAM_DOMAIN_HOME/bin/startWeblogic.sh

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*

8.4.4 Creating the OAAM Admin Users and OAAM Groups

Before integrating Access Manager and OAAM, 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 protecting the OAAM Administration Console, you must take care of user and group creation in the external LDAP store. For details, see Chapter 2, "Using the idmConfigTool Command."

  OR

- If not protecting the OAAM Administration Console, then the administration user must be created in the WebLogic Administration Console.

  To disable OAAM Administration Console protection, refer to Section 8.5.5, "Disabling OAAM Administration Console Protection."

The following are instructions to create administration users in the WebLogic Administration Console:

1. Log in to the Oracle WebLogic Administration Console for your WebLogic administration domain.
2. In the Domain Structure tab in the left pane, select **Security Realms**.

3. On the Summary of Security Realms page, select the realm that you are configuring (for example, `myrealm`).
4. On the Settings for Realm Name page select **Users and Groups** and then **Users**.
5. 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/Confirmation
6. Click the newly created user, `user1`.
7. Click the **Groups** tab.
8. Assign all the groups with the `OAAM` keyword to the user, `user1`.

   Move those groups from the left (available) to the right (chosen).
9. Click **Save** to save the changes.

8.4.5 Importing Oracle Adaptive Access Manager 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 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 on 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**.

   So far, you have loaded the snapshot into memory. 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. For details, see Setting Up the Oracle Adaptive Access Manager Environment in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

You may encounter a non-working URL if policies and challenge questions are not available as expected in your Oracle Adaptive Access Manager environment.

8.4.6 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 administrator user name and password.

   If the login is successful, the Welcome to Oracle Access Management page is displayed.

8.4.7 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. Click the **Enter** button on the virtual authentication device.
5. Click **Continue** to register the new user.
6. Click **Continue** to accept the security device.
7. Choose questions and provide answers to register for Knowledge Based Authentication (KBA).

   A successful login indicates that you have configured the initial configuration correctly.

8.4.8 Registering WebGate Using the Oracle Access Management Console

This section describes how to create and register the 11*g* WebGate. Oracle HTTP Server WebGate is a Web server extension that is available with Oracle Access Manager. The Oracle HTTP Server WebGate intercepts HTTP requests from users for Web resources and forwards them to the Access Server for authentication and

authorization. Oracle HTTP Server WebGate installation packages are found on media and virtual media that is separate from the core components. For information on installing the Oracle HTTP Server WebGate, see "Installing and Configuring Oracle HTTP Server 11g Webgate for Oracle Access Manager" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

8.4.8.1 Pre-requisites for WebGate Registration

Ensure that the following are installed before configuring and registering the Oracle Web Gate:

- WebLogic Server for Oracle HTTP Server (`WLS_FOR_OHS`)
- Oracle HTTP Server (`WLS_FOR_OHS/Oracle_WT1`, call this `OHS_HOME`)
- WebGate (`WLS_FOR_OHS/Oracle_OAMWebGate1`, call this `WG_HOME`)

For information, see "Preparing to Install Oracle HTTP Server 11g Webgate for Oracle Access Manager" in Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management

8.4.8.2 Configure the 11*g* WebGate

After installing WebGate, perform the post-installation steps. For information, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

8.4.8.3 Register the 11*g* WebGate as a Partner Using the Oracle Access Management Console

You must register the Access Manager Agent that resides on the computer hosting the application to be protected.

Registering an agent sets up the required trust mechanism between the agent and the Access Manager engine. Registered agents delegate authentication tasks to the OAM Server.

For information, see *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

1. Go to the Oracle Access Management Console.

   `http://`*`oam_adminserver_host`*`:`*`oam_adminserver_port`*`/oamconsole`

2. Register the 11*g* WebGate partner using the Oracle Access Management Console.
3. Click the **Edit** button in the tool bar to display the configuration page.
4. Set the **Access Client Password** and click **Apply** to save the changes. Note the Artifacts Location in the confirmation message.
5. In the Artifacts Location, locate the `ObAccessClient.xml` configuration file and `cwallet.sso` and copy them to the *OHS_HOME*`/instances/`*instance*`/config/OHS/`*component*`/webgate/config` directory.

8.4.8.4 Restarting the OHS WebGate

Restart the Web server (OHS) for the changes to take effect.

1. Navigate to the *OHS_HOME*`/instances/`*instance*`/bin` directory.
2. Restart the OHS instance by using the following command:

```
opmnctl stopall
opmnctl startall
```

8.4.8.5 Validating the WebGate Setup

Once the setup of WebGate is complete, validate the registration:

1. Verify the WebGate configuration by accessing the protected URL.

   `http://ohs_host:ohs_port/`

   You should be redirected to Access Manager SSO login page for authentication.

2. Enter user name and password.

   The Oracle HTTP Server Welcome page should be displayed.

   This is the partner that will be protected using Oracle Adaptive Access Manager.

8.4.9 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. If OAAM is registered with Access Manager as a partner application, OAAM will then be able to communicate with Access Manager via 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 the OAM Server owns the responsibility for redirecting to the protected resource.

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.

To register the OAAM Server as a trusted partner application to Access Manager, follow these steps:

1. Ensure that the Access Manager Administration Server is running.
2. Set up the environment for WLST.
3. Go to *IAM_ORACLE_HOME*`/common/bin`.

   `cd IAM_ORACLE_HOME/common/bin`

4. Execute the `wlst.sh` to enter the WLST shell.

   `./wlst.sh`

5. Type `Connect` to connect to the WebLogic Administration Server.
6. Enter username. For example, `admin_username`.
7. Enter password. For example, `admin_password`.
8. Enter t3://*hostname:port*

   For example

   `t3://AdminHostname:7001`

9. In another terminal window, create the `keystore` directory by executing the following:

   `mkdir IAM_ORACLE_HOME/TAP/TapKeyStore`

10. 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")
```

The command registers any third party as a Trusted Authentication Protocol (TAP) Partner.

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 8–6 TAP Partner Example

Parameter	Details
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 `IAM_ORACLE_HOME/TAP/TapKeyStore/mykeystore.jks`. Another example is `keystoreLocation="/scratch/jsmith/dwps1tap/TapKeyStore/mykeystore.jks"`. When you run the command `registerThirdPartyTAPPartner`, the keystore file is created in that location specified. On Windows, the path must be escaped. For example: `"C:\\oam-oaam\\tap\\tapkeystore\\mykeystore.jks"`
password	The keystore password used to encrypt the keystore. The keystore is created by running command "registerThirdPartyTAPPartner" in the location as specified for parameter "keystoreLocation". Make a note of the password as you will need it later.
tapTokenVersion	Version of the Trusted Authentication Protocol. `tapTokenVersion` is always `v2.0` for 11.1.1.5.0 and 11.1.2.0. If using IDContext Claims, it is `v2.1`.
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 tapRedirectUrls, 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 `registerThirdPartyTAPPartner` command in the instructions above. The name of `TAPScheme` will be passed as parameter to that command. The example command has `tapScheme="TAPScheme"`.
tapRedirectUrl	Third party access URL. The TAP redirect URL should be accessible. If it is not, registration of the partner fails with the message: `Error! Hyperlink reference not valid`. `tapRedirectUrl` is constructed as follows: `http://`*oaamserver_host*`:`*oaamserver_port*`/oaam_server/oamLoginPage.jsp` 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 `registerThirdPartyTAPPartner` (TAPScheme) points to the OAAM Server credential collector page as the redirectURL.

11. Type `exit ()` to quit the WebLogic shell.

8.4.10 Setting the Agent Password

You will need to specify the Agent password in multiple places. OAAM needs this agent password in order to use the agent profile for integration.

8.4.10.1 Adding a Password to the IAMSuiteAgent Profile in the Oracle Access Management Console

When Access Manager is installed, a default agent profile called IAMSuiteAgent is created. This profile is used by OAAM 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 OAAM for integration. To do this, proceed as follows:

1. Log in to the Oracle Access Management Console.

   `http://oam_adminserver_host:oam_adminserver_port/oamconsole`

2. Enter username and password.
3. Select the **System Configuration** tab.
4. Expand **Access Manager Settings**, and then **SSO Agents**.
5. Double-click **OAM Agent**.

   The WebGate page opens in the right hand pane.
6. Click **Search** to list all WebGate agents including **IAMSuiteAgent**.
7. Double-click **IAMSuiteAgent** to edit the properties.
8. Specify the password in the **Access Client Password** field and click **Apply** to save the changes.

   This is a required step.

8.4.10.2 Updating the IAMSuiteAgent in the WebLogic Administration Console

Note: The IAMSuiteAgent is now in **Open Mode** with password authentication. If you are using the domain agent in the IDM Domain for another console, update the domain agent definition so that you can continue using the domain agent.

1. Log in to WebLogic Administration Console.

   `http:oam_adminserver_host:port/console`

2. Enter credentials.
3. Select **Security Realms** from the Domain Structure menu.
4. Click **myrealm**.
5. Click the **Providers** tab.
6. Select **IAMSuiteAgent** from the list of authentication providers.
7. Click **Provider Specific**.
8. Enter the agent password and confirm the password.

   This is a required step.
9. Click **Save**.
10. Click **Activate Change** on the top left corner.
11. Restart the WebLogic Administration Server, OAAM Admin and managed servers, and OAM Server.

8.4.11 Verifying TAP Partner Registration

To verify the TAP partner registration, follow the instructions below.

8.4.11.1 Verifying the Challenge URL

To validate the Access Manager configuration, perform the following steps:

1. Log in to the Oracle Access Management Console.
2. Enter credentials.
3. Click the **Policy Configuration** tab in the left pane of the console.
4. In the left pane, expand the **Authentication Schemes** node.
5. Double-click the **TAPScheme** authentication scheme.
6. Verify that the **Challenge Method** is `DAP` and the **Authentication Module** is `DAP`.
7. Verify that **Challenge URL** shows part of the value of the tapRedirectUrl that had been specified when OAAM was registered with Access Manager as a partner application. For example, if the `tapRedirectUrl` is `http://OAAM_Managed_server_host:14300/oaam_server/oamLoginPage.jsp`, then **Challenge URL** should show `/oaam_server/oamLoginPage.jsp`. The host and port part of the URL is parameterized in Challenge Parameter. In the Challenge Parameters field, you will see both `TAPPartnerId=OAAMPartner` and `SERVER_HOST_ALIAS=HOST_ALIAS_1`.
8. Check the challenge parameters are set correctly.

8.4.11.2 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. Log in to the Oracle Access Management Console.

   `http://oam_adminserver_host:oam_adminserver_port/oamconsole`

2. Enter credentials.
3. Click the **Policy Configuration** tab to the left of the screen.
4. Expand the **Authentication Schemes** node.
5. Double-click **TAPScheme** authentication scheme.
6. To add another parameter to an existing parameter, position your cursor in the **Challenge Parameter** field and press **Enter** using your keyboard.
7. 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 *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
8. Click **Apply** to submit the change.
9. Dismiss the Confirmation window.

8.4.11.3 Validating the IAMSuiteAgent Setup

To validate the IAMSuiteAgent setup, 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. Launch Oracle Access Management tester.

   IAM_ORACLE_HOME/../*jdk_version*/bin/java -jar *IAM_ORACLE_HOME*/oam/server/tester/oamtest.jar

   The Oracle Access Management Tester Console appears.

3. In the Server Connection section provide server connection details:
   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 Adding a Password to the IAMSuiteAgent Profile in the Oracle Access Management Console

   The Server Connection section provides fields for the information required to establish a connection to the OAM Server.

4. Click **Connect**.

   If you can connect to the server, the next section, **Protected Resource URI**, will be enabled.

5. 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`.

6. 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.

7. In the User Identity section, provide `User Identity` and click **Authenticate**. If the authentication is successful, the setup is successful.

   This section provides information about a user whose credentials need to be authenticated. The Authenticate button is used to submit the Authenticate User server request.

8.4.12 Setting Up Access Manager TAP Integration Properties 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. Create a working directory.

```
mkdir temp
cd temp
mkdir oaam_cli
cd..
```

3. Copy the OAAM `cli` folder to the working directory.

```
cp -r OAAM_HOME/oaam/cli/. temp/oaam_cli
```

4. Open `oaam_cli.properties` located in `temp/oaam_cli/conf/bharosa_properties with` a text editor.

```
gedit temp/oaam_cli/conf/bharosa_properties/oaam_cli.properties
```

5. Set the properties described in Table 8–7.

Table 8–7 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: jdbc:oracle:thin:@*db_host*:*db_port*:*db_sid*
oaam.uio.oam.tap.keystoreFile	This is the location of keystore file generated by `registerThirdPartyTAPPartner` WLST. Copy the file from the location specified in the above WLST for parameter "`keystoreLocation`". 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: "`C:\\oam-oaam\\tap\\keystore\\store.jks`"
oaam.uio.oam.tap.partnername	This is the "partnerName" used in the WLST registerThirdPartyTAPPartner command. For example, OAAMPartner.
oaam.uio.oam.host	This is the Access Manager Primary Host.

Table 8–7 (Cont.) OAAM CLI Properties

Parameter	Details
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 `IAMSuiteAgent` 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).
oam.uio.oam.rootcertificate.keystore.filepath	The location of the Keystore file generated for the root certificate: DOMAIN_HOME/output/webgate-ssl/oamclient-truststore.jks. This is required only for security modes 2 (Simple) and 3 (Cert).
oam.uio.oam.privatekeycertificate.keystore.filepath	The location of the Keystore file generated for private key: DOMAIN_HOME/output/webgate-ssl/oamclient-keystore.jks. Private key is only required if you set up Access Manager and OAAM in Simple and Cert mode.
oaam.csf.useMBeans	For a multiple domain installation, the oaam.csf.useMBeans property must be set to true. For information on setting this parameter, see "Oracle Adaptive Access Manager Command-Line Interface Scripts" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

6. Save the changes and quit the editor.
7. 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
   ```

8. Change directory to `temp/oaam_cli/`.
9. Enable execute permissions.

   ```
   chmod 777 setupOAMTapIntegration.sh
   ```

10. 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.

11. 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 (usually weblogic).
    - OAAM Admin server password: This is the password for the Admin Server user.
    - 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.

    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 *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

8.4.13 Configuring a Resource to be Protected with TAPScheme

To protect a resource with the OAAM TAPScheme, proceed as follows:

8.4.13.1 Creating a New Resource under the Application Domain

To create a new resource to protect, proceed as follows:

1. Log in to the Oracle Access Management Console.

   `http://oam_host:port/oamconsole`

2. Click the **Policy Configuration** tab in the Oracle Access Management Console.
3. Double-click **Application Domains** in the left panel.
4. In the Application Domains page, click **Search**, and in the search results, click **IAM Suite**
5. Click **Resources** tab.
6. Click the **New Resource** button to create a resource.

   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`

7. Click **Apply** to add this resource to the application domain.

8.4.13.2 Create 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. Double-click **Application Domains** in the left panel.
2. In the Application Domains page, click **Search**, and in the search results, click **IAM Suite**
3. Click the **Authentication** Policies tab and then the **Create Authentication Policy** button.
4. Add general policy details:

   Name: A unique name used as an identifier in the left pane. For example, HighPolicy.

   Authentication Scheme: **TAPScheme**
5. Add global policy elements and specifications:

   Description (optional): Optional unique text that describes this authentication policy.

   Success URL: The redirect URL to be used upon successful authentication.

   Failure URL: The redirect URL to be used if authentication fails.
6. Add Resources:

   Choose the URL of a resource from those listed. 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.

   a. Click the **Resources** tab on the Authentication Policy page.

   b. Click the **Add** button on the tab.

   c. Choose the URL from the list. For example, `/higherriskresource`.
7. Click **Apply** to save changes and close the Confirmation window.
8. Add policy responses.

   Responses are the obligations (post authentication actions) to be carried out by the Web agent. After a successful authentication, the application server hosting the protected application should be able to assert the User Identity based on these responses.After a failed authentication, the browser redirects the request to a pre-configured URL

9. Close the page when you finish.

8.4.14 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.

8.5 Other Access Manager and OAAM Integration Configuration Tasks

This section describes other configuration procedures that you may need depending on your deployment.

8.5.1 Configuring Integration to Use TAPScheme to Protect IDM Product Resources in the IAM Suite Application Domain

Note: The instructions in this section should only be performed if you want to use TAPscheme in the IAMSuiteAgent application domain.

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 navigation tree, double-click **Application Domains**, then click **Search**, and in the search results, click **IAM Suite**.
3. Click the **Authentication Policies** tab.
4. Click **Protected Higher Level Policy**.
5. In the Resources window click **/oamTAPAuthenticate**.
6. Click **Delete**, and then **Apply**.
7. Create a new Authentication Policy in the IAMSuite application domain.
8. For authentication scheme, choose **LDAP Scheme**.
9. In the Resources window, click **Add**.
10. Select the resource **/oamTAPAuthenticate.**
11. Click **Apply**.

8.5.2 Changing the Authentication Level of the TAPScheme Authentication Scheme

To change the authentication level of the TAPScheme authentication scheme, proceed as follows:

1. Select the **Policy Configuration** tab in the Oracle Access Management Console.
2. Expand the **Shared Components** node.
3. Expand the **Authentication Schemes** node.

4. Double-click **TAPScheme**.
5. On the Authentication Scheme page, change the authentication level.
6. Click **Apply** to submit the changes.
7. Dismiss the Confirmation window.
8. Close the page when you finish.

8.5.3 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.

8.5.3.1 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 *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

8.5.3.2 Setting OAAM Properties for Access Manager for Simple Mode

Follow the steps in Section 8.4.12, "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 8–7.

Table 8–8 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).
oam.uio.oam.rootcertificate.keystore.filepath	The location of the Keystore file generated for the root certificate: DOMAIN_HOME/output/webgate-ssl/oamclient-truststore.jks. This is required only for security modes 2 (Simple) and 3 (Cert).
oam.uio.oam.privatekeycertificate.keystore.filepath	The location of the Keystore file generated for private key: DOMAIN_HOME/output/webgate-ssl/oamclient-keystore.jks. This is required for security modes 2 (Simple) and 3 (Cert)

8.5.4 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/oam-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 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.
3. In 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. Click the **Policy Configuration** tab to the left of the screen.
   c. Expand the **Authentication Schemes** node.
   d. Double-click **TAPScheme** authentication scheme.
   e. To add another parameter to an existing parameter, position your cursor in the **Challenge Parameter** field and press **Enter** using your keyboard.
   f. In the new line, add TAPOverrideResource=http://IAMSuiteAgent:80/oamTAPAuthenticate for a challenge parameter of TAPScheme.

8.5.5 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 *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

8.5.6 Disabling Step Up Authentication

If you want to disable the Step Up Authentication scenario, the following property has to be set to `false` through the OAAM Properties Editor:

```
oaam.uio.oam.integration.stepup.enabled
```

By default this property is set to `true`. 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.

8.6 Resource Protection Use Case

This use case illustrates how to set up the login and step up authentication flows.

8.6.1 Changing Authentication Level of TAPScheme

To change the authentication level, proceed as follows:

1. Log in to the Oracle Access Management Console.

   ```
   http://oam_host:port/oamconsole
   ```

2. Click the **Policy Configuration** tab.
3. Click **TAPScheme** in the left panel.
4. In the TAPScheme Authentication Schemes page, 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.
5. Click **Apply** to save the changes.
6. In the left pane, click **OAMAdminConsoleScheme**.
7. Ensure that the Authentication Level value is lower than that of TAPScheme.

   OAMAdminConsoleScheme will be protecting the lower protected resource.

8.6.2 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. Click **Application Domains** in the left pane.
2. In the Application Domains page, click **Search**, and in the search results, click **IAM Suite**
3. Click the **Authentication Policies** tab.
4. Click **Protected Higher Level Policy.**
5. In the Resources tab, remove **/oaam_admin/**** and click **Apply** to apply the change.

8.6.3 Creating a New Policy that Uses TAPScheme to Protect the Resource

Create a new policy with TAPScheme and protect OAAM as a higher protected resource.

1. Click the **Create Authentication Policy** button in the Authentication Policies tab.

2. In the Authentication Policy page, specify a policy name in the name field. For example, `TestPolicy`.
3. In Authentication Scheme, select **TAPScheme** from the pulldown.
4. Click **Resources** tab.
5. Click the **Add** icon to create a new resource.
6. Click **Search** in the Search window.
7. Select **/oaam_admin/**** as the resource.
8. 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 Oracle Access Management Console protected by **OAMAdminConsoleScheme**.

8.6.4 Creating an New OAAM User

For information on creating a user, see Section 8.4.4, "Creating the OAAM Admin Users and OAAM Groups."

8.6.5 Login Flow Example

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 8.6.1, "Changing Authentication Level of TAPScheme" through Section 8.6.4, "Creating an New OAAM User."

The Login flow is as follows:

1. Access the protected resource, the OAAM Administration Console, by entering its URL in a web browser.

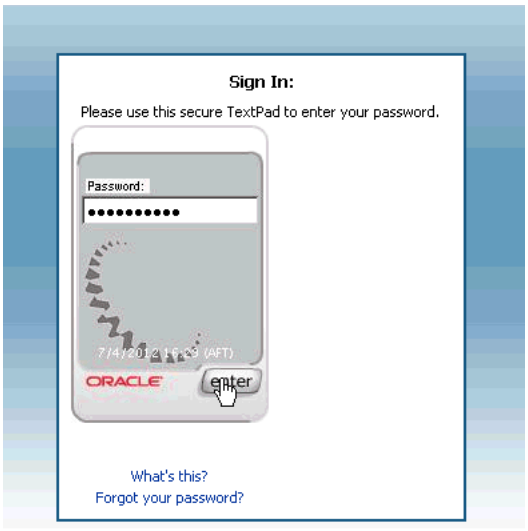
   The Access Manager user name page appears.

   You are redirected to OAAM Server.
2. In the Access Manager user name page, enter the user name and click **Continue**.

Figure 8–1 Access Management Username Page

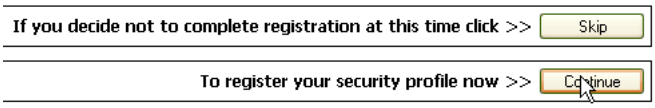
3. The Password page appears with the textpad for you to enter the password.

Figure 8–2 Password Page with TextPad



4. Enter the password and click **Enter**.
5. Click **Continue** to begin registering a profile for the user.

Figure 8–3 Register Profile

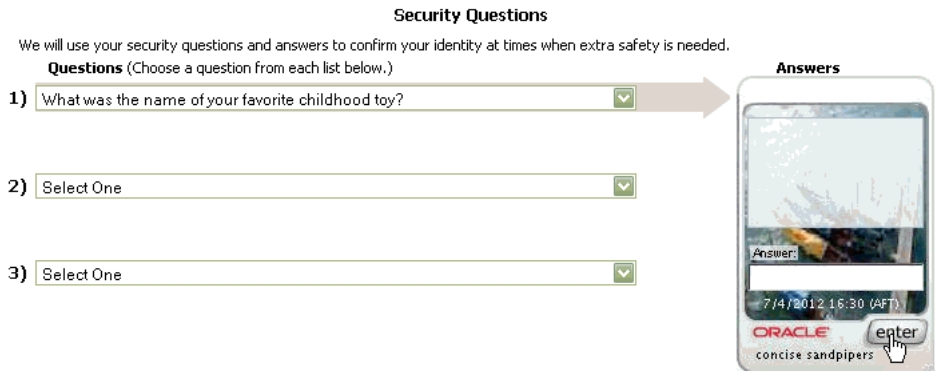


6. Select your security device and click **Continue**.

Figure 8–4 Security Device Selection

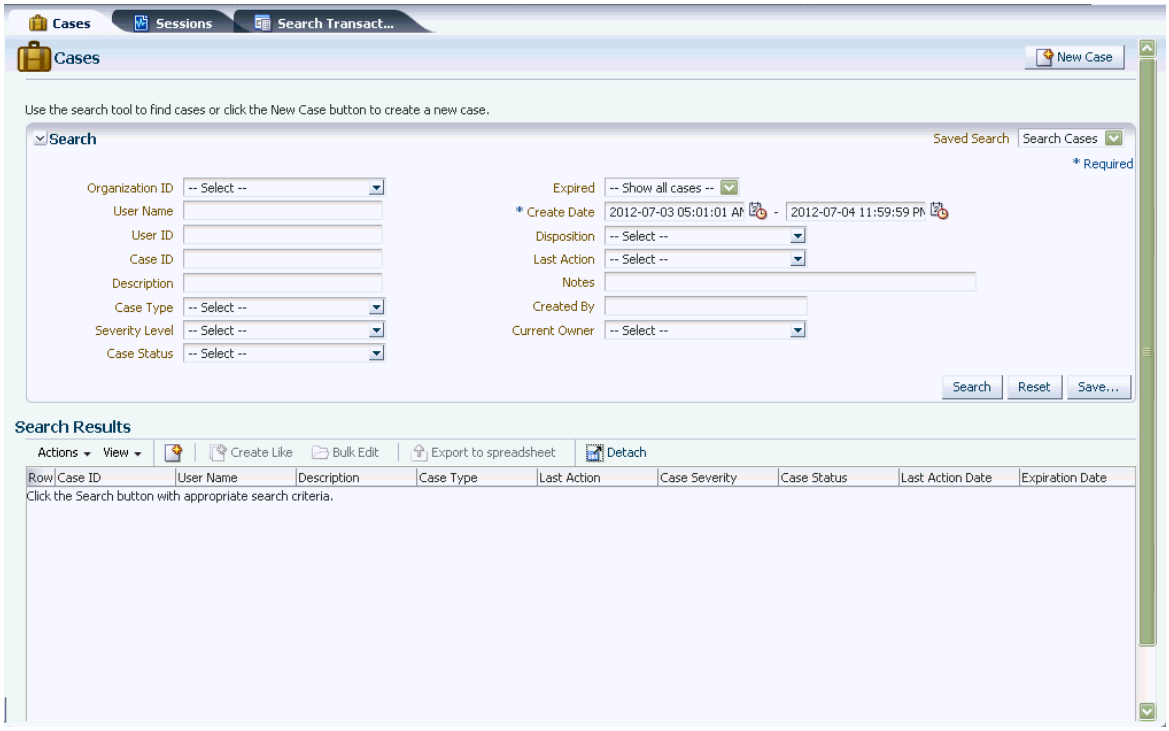
7. Register challenge questions.

Figure 8–5 Challenge Question Registration



8. You are allowed to access the protected resource, the OAAM Administration Console.

Figure 8–6 OAAM Administration Console Cases Page



8.6.6 Step Up Authentication Flow

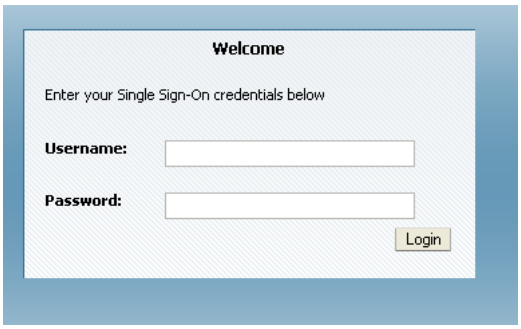
This section presents an example of the Step Up Authentication flow for the user who registered his profile and was allowed access to the higher protected resource in Section 8.6.5, "Login Flow Example." The example is based on the setup performed in Section 8.6.1, "Changing Authentication Level of TAPScheme" through Section 8.6.4, "Creating an New OAAM User."

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.

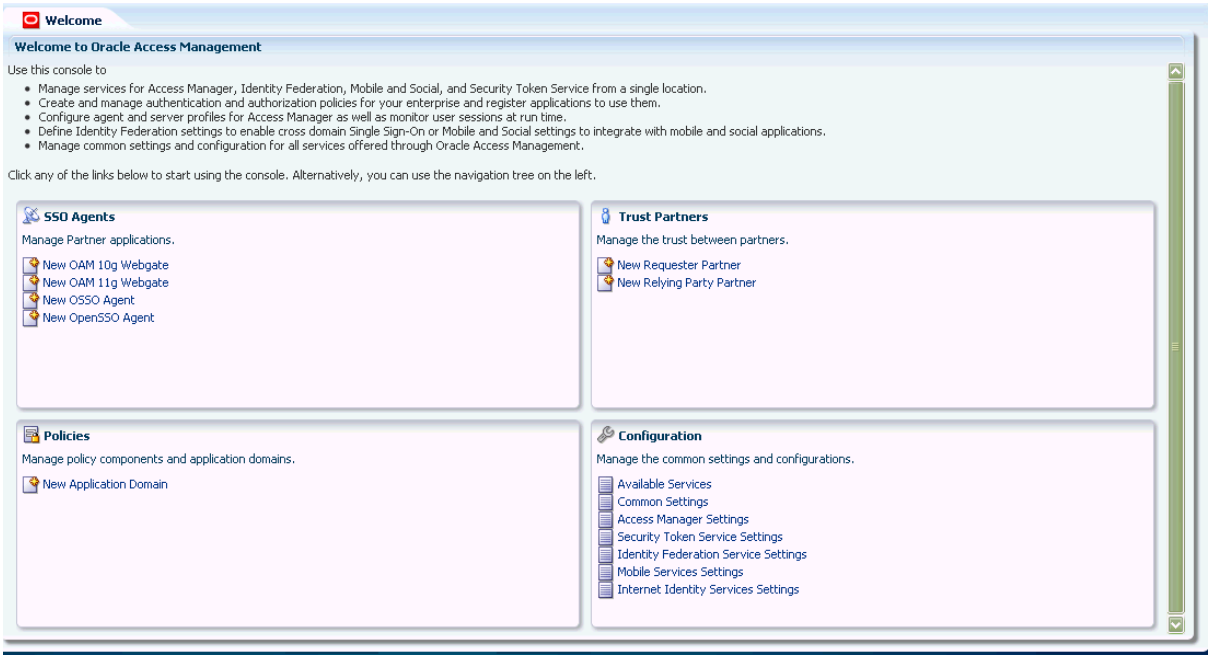
   When you access the lower risk resource, you are shown the Oracle Access Management login page, which has the username and password on the same page.

Figure 8–7 Access Management Login



2. Enter the credentials of the user who has registered a profile (see Section 8.6.5, "Login Flow Example") 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.

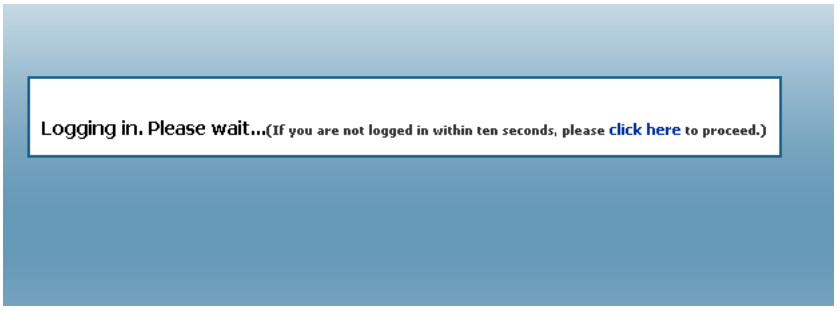
Figure 8–8 Access Management Console



4. Access the higher protected resource, the OAAM Administration Console, by entering the URL in a web browser.

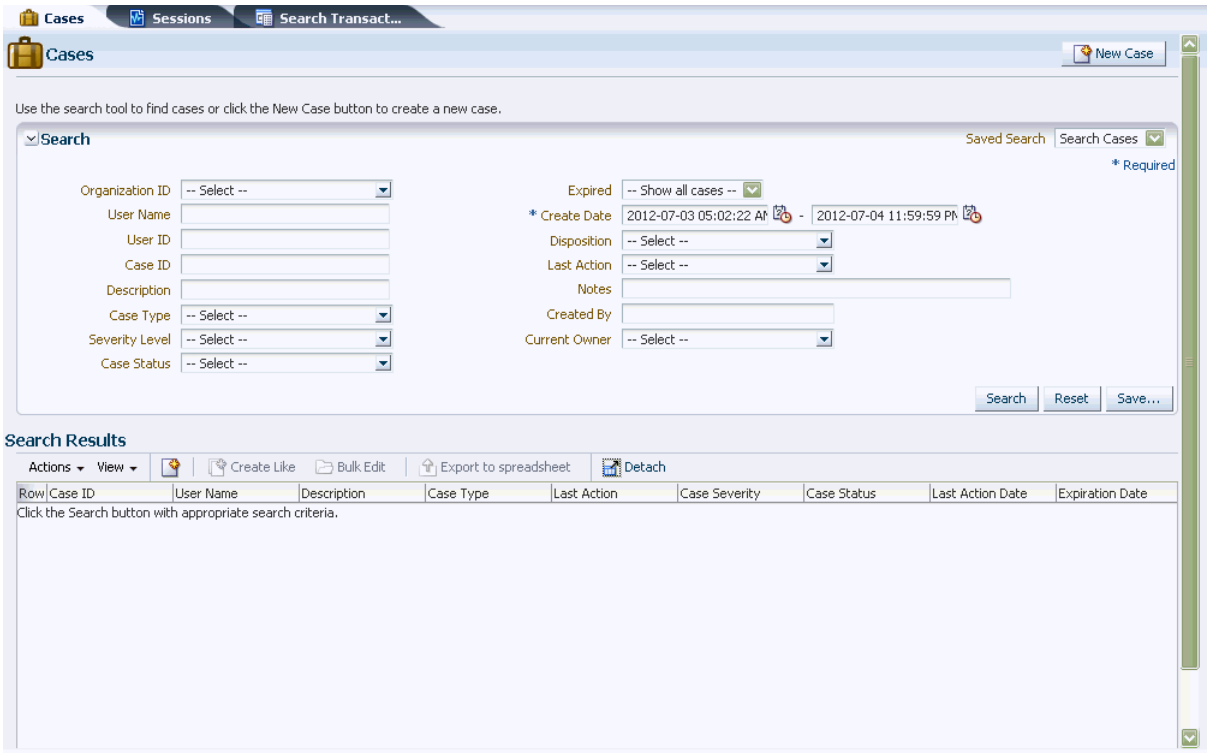
   OAM Server does not present the Login page since you are already authenticated. However, OAAM will run its fraud detection policies.

Figure 8–9 Step Up Authentication



5. After OAAM determines that the risk is low, you now have access to the higher protected resource, the OAAM Administration Console.

Figure 8–10 Higher Protected Resource



8.7 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."

8.7.1 OAAM Basic Integration with Access Manager

This provides solutions for integration issues pertaining to OAAM Basic integration with Access Manager.

8.7.1.1 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 username 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.

8.7.1.2 Access Manager and OAAM Integration and Changes in the Console

A 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`.

8.7.1.3 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.

8.7.1.4 Using ConfigureOAAM WLST to Create the Datasource 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 datasource 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` - maximum connection reserve time out size
  - `maxPoolSize` - maximum size of connection pool

For example:

```
configureOAAM(dataSourceName = "MyOAAMDS", hostName = "host.us.co.com",
port = "1521", sid = "sid", userName = "username", passWord = "password",
maxConnectionSize = None, maxPoolSize = None, serverName = "oam_server1")
```

Note: `SID =` requires the service name.

8.7.2 Login Failure

This provides solutions for login issues.

8.7.2.1 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`.

8.7.2.2 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 and OAAM servers, 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
```

For information on setting properties in Oracle Adaptive Access Manager, see "Using the Property Editor" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

8.7.2.3 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.

8.7.3 Identity Store

This provides solutions for identity store issues.

8.7.3.1 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 left panel, click **TAPScheme**.
3. Double-click **TAPScheme** authentication scheme.
4. In the TAPScheme page, 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.

5. Click **Apply** to submit the change.

8.7.3.2 In the Access Manager and OAAM 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 OAAM 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.

8.7.3.3 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 synched.

8.7.4 Miscellaneous

This section provides solutions and tips for miscellaneous issues.

8.7.4.1 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 left panel, click **TAPScheme**.
3. In the TAPScheme page, 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 enter 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 8–11

4. Click **Apply** to apply the changes.

8.7.4.2 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`.

Figure 8–12 TAP Token Version

4. Save the changes.

   `:wq!`

5. Log in to the OAAM Administration Console.

   `http://`*`oaam_managed_server_host`*`:`*`oaam_admin_managed_server_port`*`/oaam_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: `oaam.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 left pane, double-click the **TAPScheme** authentication scheme.
12. In the TAPScheme page, 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.

13. Click **Apply** to apply the changes.

8.7.4.3 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`.

8.7.4.4 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 Release 1 (11.1.1) and earlier:

  ```
  oaam.uio.oam.authenticate.withoutsession = false
  ```

- For Access Management 11g and 10g:

  ```
  oracle.oaam.httputil.usecookieapi = true
  ```

8.7.4.5 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.

9

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.

This chapter contains these sections:

9.1 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

In 11*g* Release 2 (11.1.2), 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 9–1 Responsibilities for Each Component in Integration

Component	Responsibilities
Oracle Adaptive Access Manager	Responsible for: ■ 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: ■ Provisioning users to add, modify, or delete users ■ Managing passwords through Reset Password or Change Password flows
Access Manager	Responsible for: ■ Authenticating and authorizing users ■ Providing advanced status flags such as Reset Password, Password Expired, User Locked, and others

9.1.1 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 the 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 wishing to add login security, including Knowledge Based Authentication (KBA), may use OAAM Basic integration with Access Manager. This option will still require an OAAM Admin Server, but it does not require the deployment of a separate OAAM Server. The functionality is accessed through

native OAAM calls. The "OAAM Basic Integration" option has a smaller footprint than the "OAAM Advanced Integration" option.

The "OAAM Basic Integration" differs from the "OAAM Advanced Integration" in that it does not provide access to more advanced features such as One-Time Password (OTP) through SMS, email, or IM. In addition, this native integration is not customizable beyond basic screen branding.

- OAAM Advanced Integration with Access Manager

  This option provides advanced features and customizations beyond that available with native integration. 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 Chapter 8, "Integrating Access Manager and Oracle Adaptive Access Manager".

9.1.2 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 9.3, "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 *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

9.2 Definitions, Acronyms, and Abbreviations

This section provides key definitions, acronyms, and abbreviations that are related to this integration.

Table 9–2 Advanced Integration Terms

Term	Definition
Action	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. For information, see "Managing Policies, Rules, and Conditions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Advanced integration with Access Manager	The "Advanced" option is an integration of Access Manager and full deployment of Oracle Adaptive Access Manager. ■ An Access Manager and Oracle Adaptive Access Manager integration with a full OAAM deployment. 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	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. Alert groups are used as results within rules so that when a rule is triggered all of the alerts within the groups are created. For information, see "Managing Policies, Rules, and Conditions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Authentication	The process of verifying a person's, device's, application's identity. Authentication deals with the question "Who is trying to access my services?"
Authentication Level	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. The trust level of the authentication scheme reflects the challenge method and degree of trust used to protect transport of credentials from the user. The trust level is expressed as an integer value between 0 (no trust) and 99 (highest level of trust). 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. Current Authentication level is the current authentication level of the user. Target Authentication level is the authentication level required to access the protected resource.
Authorization	Authorization regards the question "Who can access what resources offered by which components?"

Table 9–2 (Cont.) Advanced Integration Terms

Term	Definition
Authentication Scheme	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. 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.
Authentipad Checkpoint	The Authentipad checkpoint determines the type of device to use based on the purpose of the device.
Basic Integration of Access Manager and OAAM	Access Manager users wishing to add login security, including Knowledge Based Authentication (KBA), may use the Basic (native) integration option. This option will still require an OAAM Admin Server, but it does not require you to deploy a separate OAAM Server (the functionality is accessed through native OAAM calls), so the footprint is reduced. 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.
Blocked	If 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. 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 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." 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 pads, 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: ■ Pre-authentication - Rules are run before a user completes the authentication process. ■ Post-authentication - Rules are run after a user is successfully authenticated. For information, see "Managing Policies, Rules, and Conditions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Management*.
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.

Table 9–2 (Cont.) Advanced Integration Terms

Term	Definition
Device	A computer, PDA, cell phone, kiosk, and other web-enabled device used by a user
Device fingerprinting	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. A customer typically uses these devices to log in: PC, notebook, mobile phone, smart phone, or other web-enabled machines.
Knowledge Based Authentication (KBA)	Knowledge-based authentication (KBA) is a secondary authentication method that provides an infrastructure based on registered challenge questions. It enables end-users to select questions and provide answers which are used to challenge them later on. Security administration include: ■ 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 For information, see "Managing Knowledge-Based Authentication" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
KeyPad	Virtual keyboard for entry of passwords, credit card number, and so on. The KeyPad protects against Trojan or keylogging.
LDAPScheme	Authentication scheme used to protect Access Manager-related resources (URLs) for most directory types based on a form challenge method.
Multi-Level Authentication	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. 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". For information, see "Managing Authentication and Shared Policy Components" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
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.

Table 9–2 (Cont.) Advanced Integration Terms

Term	Definition
One-time Password (OTP)	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. For information, see "Setting Up OTP Anywhere" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Access Manager and Oracle Adaptive Access Manager TAP Integration	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.
OAAM Admin	Administration Web application for all environment and Adaptive Risk Manager and Adaptive Strong Authenticator features.
OAMAdminConsoleScheme	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 with 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 Authenticator features, Web services, LDAP integration and user Web application used in all deployment types except native integration
Policies	Policies contain security rules and configurations used to evaluate the level of risk at each checkpoint. For information, see "Managing Policies, Rules, and Conditions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Post-authentication rules	Post-authentication - Rules are run after a user is successfully authenticated. For information, see "Managing Policies, Rules, and Conditions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Pre-authentication rules	Pre-authentication - Rules are run before a user completes the authentication process. For information, see "Managing Policies, Rules, and Conditions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Profile	The customer's registration information including security phrase, image, challenge questions, challenge (question and OTP) counters, and OTP.

Table 9–2 (Cont.) Advanced Integration Terms

Term	Definition
Protection level	There are three protection levels in which to choose from: ■ 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	Registration is the enrollment process, the opening of a new account, or other event where information is obtained from the user. 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.
Risk score	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.
Rules	Fraud rules are used to evaluate the level of risk at each checkpoint. For information on policies and rules, see "OAAM Security and Autolearning Policies" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.
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.

Table 9–2 (Cont.) Advanced Integration Terms

Term	Definition
Step Up Authentication	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. 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.
Strong Authentication	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. Using more than one factor is sometimes called strong authentication or multi-factor authentication.
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	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. 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.
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 9–2 (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	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. 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. 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.
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

9.3 Integration Roadmap

Table 9–3 lists the high-level tasks for integrating Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager.

Table 9–3 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	Install Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager on different WebLogic servers.	For information, see "Install Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager".
3	Integrate Access Manager and Oracle Identity Manager.	For information, see "Integrate Access Manager and Oracle Identity Manager".
4	Enable 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 "Enable LDAP Synchronization for Oracle Identity Manager".
5	Integrate Access Manager and Oracle Adaptive Access Manager.	For information, see "Integrate Access Manager and Oracle Adaptive Access Manager".
6	Set up the integration between OAAM and OIM.	For information, see "Integrate Oracle Identity Manager and Oracle Adaptive Access Manager".
7	Perform additional configuration that you may need depending on your requirements.	For information, see "Other Configuration Tasks".

9.4 Integration Prerequisites

Prior to integrating 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 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 *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Table 9–4 lists the required components that must be installed and configured before the Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager integration tasks are performed.

Table 9–4 Access Manager, OAAM, and OIM Integration Required Components

Component	Information
Oracle Database	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. For more information, see "Database Requirements" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
Repository Creation Utility (RCU)	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. 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 *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* and *Oracle Fusion Middleware Repository Creation Utility User's Guide*.
Oracle Virtual Directory	The instructions in this chapter assumes that the Oracle Internet Directory is configured as the Identity Store and is front-ended by Oracle Virtual Directory. For more information on configuring the OVD, see Chapter 6, "Configuring Oracle Virtual Directory for Integration with Oracle Access Management Access Manager" and Chapter 4, "Configuring Oracle Virtual Directory for Integration with Oracle Identity Manager."
Oracle Internet Directory	The instructions in this chapter assumes the that Oracle Internet Directory is configured as the Identity Store and is front-ended by Oracle Virtual Directory. For more information, see Chapter 5, "Integrating Oracle Internet Directory with Access Manager."

Table 9–4 (Cont.) Access Manager, OAAM, and OIM Integration Required Components

Component	Information
Oracle WebLogic Servers for Access Manager, Oracle Adaptive Access Manager, Oracle Identity Manager, and Oracle HTTP Server	Prior to installing the WebLogic Server, ensure that your machines meet the system, patch, kernel, and other requirements that the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* specifies. 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. For more information on installing WebLogic Servers, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* and *Installing Oracle WebLogic Server*.
Oracle SOA Suite and patches	For more information on installing and configuring the SOA Suite, see *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*
Oracle HTTP Server	For more information on installing the HTTP Server, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management.*
Oracle Access Manager 10g or Access Manager 11g agent (WebGate) for Oracle HTTP Server 11g on the Oracle HTTP Server 11g instance.	For information on installing the Oracle HTTP Server WebGate, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
IdentityManagerAccessGate 10gWebGate profile	The integration of Access Manager and Oracle Adaptive Access Manager requires that the IdentityManagerAccessGate 10gWebGate profile exist. You can validate this through the Oracle Access Management Console by navigating to **System Configuration**, then **Agents**, then **10gWebGates**.

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 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 "Oracle Adaptive Access Manager Command-Line Interface Scripts" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager* for information on setting this parameter.

During the integration steps below, for reference we will refer to the WLS Domain which contains Oracle Access Manager as `OAM_DOMAIN_HOME`, and the WLS Domain which contains OAAM as `OAAM_DOMAIN_HOME`.

9.5 Install Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager

Install Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager on different WebLogic servers with Oracle Access Manager and Oracle Adaptive Access Manager configured in the same or separate WebLogic domains.

Table 9–5 Required Components for Integration

Component	Information
Access Manager	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 *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. 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. Oracle Adaptive Access Manager and Access Manager can be in a new WebLogic administration domain or in an existing one. They can be on the same domain or separate domains.
OAAM	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 *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
OIM	For more information, see "Installing and Configuring Oracle Identity and Access Management" and "Configuring Oracle Identity Manager" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. **Note**: When configuring Oracle Identity Manager, the LDAP directory must be preconfigured before you can use it as an Identity Store. Ensure that all installation instructions are followed, including any prerequisites for enabling LDAP synchronization. For more information, see: ■ "Configuring OIM Server", ■ "Completing the Prerequisites for Enabling LDAP Synchronization", and ■ "Creating Adapters in Oracle Virtual Directory" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. **Note**: You must create wlfullclient.jar when installing Oracle Identity Manager. This file must be present before performing the integration steps.

9.6 Integrate 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 7, "Integrating Access Manager and Oracle Identity Manager."

9.7 Enable 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 will be working 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 Chapter 3, "Enabling LDAP Synchronization in Oracle Identity Manager."

9.8 Integrate 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.

> **Note:** In the integration of Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager, the IdentityManagerAccessGate profile should already exist since it is configured during the Access Manager and Oracle Identity Manager integration (see Section 9.6, "Integrate Access Manager and Oracle Identity Manager").

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 Chapter 8, "Integrating Access Manager and Oracle Adaptive Access Manager."

Table 9–6 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 9–6 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 Admin 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 Oracle Adaptive Access Manager Snapshot".
5	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".

Table 9–6 (Cont.) Integration Flow for Access Manager and Oracle Adaptive Access Manager

Number	Task	Information
6	Register the WebGate agent. The WebGate is an out-of-the-box access client. This Web server access client intercepts HTTP requests for Web resources and forwards these to the OAM 11g Server.	For information, see "Registering WebGate Using the Oracle Access Management Console"
7	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"
8	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 "Setting the Agent Password"
9	Verify TAP partner registration using the Oracle Access Management tester.	For information, see "Verifying TAP Partner Registration".
10	Set up TAP integration properties in OAAM.	For information, see "Setting Up Access Manager TAP Integration Properties in OAAM".

9.9 Integrate 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:

- Set Oracle Identity Manager Properties for Oracle Adaptive Access Manager
- Update OAAM Properties to Enable Integration Between Oracle Identity Manager and OAAM
- Configure Oracle Identity Manager Credentials in the Credential Store Framework
- Configure Cross Domain Trust Between Oracle Identity Manager and Oracle Adaptive Access Manager

9.9.1 Set Oracle Identity Manager Properties for Oracle Adaptive Access Manager

In Oracle Identity Manager, the `OIM.ChangePasswordURL` and `OIM.ChangePasswordURL` 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.

To modify Oracle Identity Manager properties, take these steps:

1. Log in to the Oracle Identity Manager System Administrative Console.
2. Click **Configuration** in **System Management** and under **System Management**, click the **System Configuration** link.
3. In the pop-up window, click on **Advanced Search**.
4. Set the following properties and click **Save**.

Note: For the URLs, use the hostnames as they were configured in Access Manager. For example, if a complete hostname (with domain name) was provided during Access Manager configuration, use the complete hostname for the URLs.

Table 9–7 Oracle Identity Manager Redirection

Keyword	Property Name and Value
OIM.DisableChallengeQuestions	TRUE
OIM.ChangePasswordURL	URL for change password page in Oracle Adaptive Access Manager (http://*oaam_server_managed_server_host*:*oaam_server_managed_server_port*/oaam_server/`oimChangePassword.jsp` In a high availability (HA) environment, set this property to point to the virtual IP URL for the OAAM server.
OIM.ChallengeQuestionModificationURL	URL for challenge questions modification page in Oracle Adaptive Access Manager (http://*oaam_server_managed_server_host*:*oaam_server_managed_server_port*/`oaam_server/oimResetChallengeQuestions.jsp`)

5. Restart the Oracle Identity Manager managed server.

9.9.2 Update 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**.

For the following properties, set the values according to your deployment:

Table 9–8 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	`${oracle.oaam.home}/../designconsole/config/authwl.conf`
oaam.oim.url	t3://*OIM-Managed-Server*:*OIM-Managed-Port* For example, `t3://host.mycorp.com:14000`
oaam.oim.xl.homedir	${oracle.oaam.home}/../designconsole

Table 9–8 (Cont.) Configuring Oracle Identity Manager Property Values

Property Name	Property Values
bharosa.uio.default.signon.links.enum.selfregistration.url	The URL for Self Registrations is as follows: http://*OIM-Managed-Server-Host*:*OIM-Managed-Server-Port*/identity/faces/register?&backUrl=*back-URL*
bharosa.uio.default.signon.links.enum.trackregistration.url	`The URL for Track Registrations is as follows:` http://*OIM-Managed-Server-Host*:*OIM-Managed-Server-Port*/identity/faces/trackregistration?&backUrl=*back-URL*
bharosa.uio.default.signon.links.enum.trackregistration.enabled	true
bharosa.uio.default.signon.links.enum.selfregistration.enabled	true
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.
oaam.oim.passwordflow.unlockuser	true This property enables automatic unlocking of the user in the Forgot Password flow.

9.9.3 Configure 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* icon 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 sub menu.
4. Click **Create Map**.
5. Click **oaam** to select the map, 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 9–9 Oracle Identity Manager Credentials

Name	Value
Map Name	`oaam`
Key Name	`oim.credentials`

Table 9–9 (Cont.) Oracle Identity Manager Credentials

Name	Value
Key Type	Password
UserName	User name of Oracle Identity Manager Administrator
Password	Password of Oracle Identity Manager Administrator

9.9.4 Configure Cross Domain Trust Between Oracle Identity Manager and Oracle Adaptive Access Manager

If Oracle Identity Manager and Oracle Adaptive Access Manager are in separate domains, you must configure cross domain trust.

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.

9.10 Other Configuration Tasks

This section contains additional topics pertaining to Access Manager, OAAM, and OIM integration configuration and management. 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 8.5, "Other Access Manager and OAAM Integration Configuration Tasks."

9.11 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

- Two User Sessions are Created upon Successful Authentication

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."

9.11.1 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 *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

9.11.2 User is Redirected in a Loop After User Enters Wrong Password

A user is re-directed 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 *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

9.11.3 Two User Sessions are Created upon Successful Authentication

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 (which is configured in OAAM as the java agent as part of the OAAM-OAM configuration); and the other session is created by the actual WebGate (within the OHS web tier).

Solution

Check the value of the property `oaam.uio.oam.authenticate.withoutsession`.

Part III

External SSO Solutions

You can integrate federation partners into the Oracle IdM environment.

This part contains the following chapters:

- Chapter 10, "Integrating with Identity Federation"

10 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:

10.1 Background and Integration Overview

This section provides background about federation with Access Manager. Topics include:

10.1.1 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).

10.1.2 Deployment Options for Identity Federation

See Also: Introduction to Oracle Access Management in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management* for details about naming conventions and name changes in 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 11*g* Release 2 (11.1.2). In this initial release Identity Federation is limited to Service Provider mode. Identity Provider mode still requires an Oracle Identity Federation 11gR1 installation.

- Separate Oracle Identity Federation and OAM 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 11*g* Release 1 (11.1.1).

  Under this approach, Oracle Identity Federation provides two deployment scenarios for Oracle Access Manager:

  – Oracle Identity Federation 11*g* Release 1 (11.1.1) integrated with Oracle Access Manager 10*g*.

  – Oracle Identity Federation 11*g* Release 1 (11.1.1) integrated with Access Manager 11*g*.

Table 10–1 summarizes the options available to integrate the identity federation products with Oracle Access Management Access Manager and provides links to deployment procedures:

Table 10–1 Deployment Options involving Oracle Access Manager

Access Manager Version	Description	Additional Information
Oracle Access Management Access Manager 11*g*R2	Access Manager contains a built-in federation engine that provides SP mode functionality configurable through the Access Manager administration console.	Introduction to Federation within Oracle Access Suite Console in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
	For IdP functionality, Access Manager integrates with Oracle Identity Federation 11g Release 1.	Section 10.2
Access Manager 11*g*R1	The stand-alone Oracle Identity Federation 11g Release 1 server integrates with the Access Manager 11*g* OAM server.	Integrating Oracle Identity Federation in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.
Oracle Access Manager 10*g*	The stand-alone Oracle Identity Federation 11g Release 1 server integrates with the Oracle Access Manager 10*g* server.	*Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

10.1.3 References

Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation.

10.2 Integration with Access Manager 11gR2

This section describes how to integrate Access Manager 11*g* Release 2 (11.1.2) with Oracle Identity Federation 11*g* Release 1 (11.1.1) (also referred to as Access Manager 11*g*R2 with Oracle Identity Federation 11*g*R1).

- Architecture

10.2.1 Architecture

Two integration modes are described in this chapter:

- SP Mode

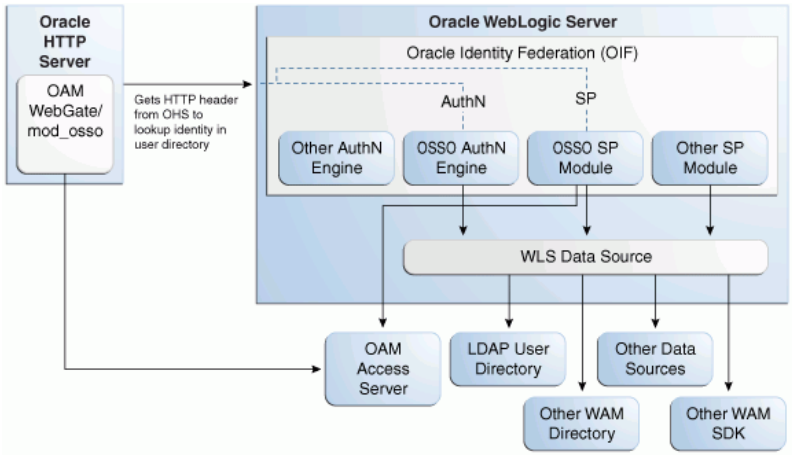
  This mode enables Oracle Identity Federation to authenticate the user via Federation SSO and propagate the authentication state to Access Manager, which maintains the session information.

- Authentication Mode

  This mode enables Access Manager to authenticate the user on behalf of Oracle Identity Federation.

Figure 10–1 describes the processing flow in each mode:

Figure 10–1 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.

10.2.2 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 10.2.4.
- Register Oracle HTTP Server as a partner with Access Manager to protect a resource. For details, see Section 10.2.5.
- 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 10.2.6.
- 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 10.2.7.

10.2.3 Prerequisites

You must install the following components prior to undertaking the integration tasks:

- Oracle WebLogic Server
- Oracle HTTP Server 11g
- Oracle 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

10.2.4 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.

10.2.5 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:

   ```
   https://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
   ```

10.2.6 Configure Oracle Identity Federation

This section describes how to configure Oracle Identity Federation to be integrated with Access Manager:

- In SP mode, where Access Manager will delegate authentication to Oracle Identity Federation for Federation SSO.
- In Authentication mode, where 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

10.2.6.1 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

10.2.6.2 Configure Oracle Identity Federation Authentication Engine

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 Oracle 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. Logout configuration:
   - If Oracle Identity Federation is also going to be integrated with Access Manager in SP mode, 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://oam_host:oam_port/oam/server/logout
       ```
8. Click **Apply**.

10.2.6.3 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.

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://oam_host:oam_port/oam/server/dap/cred_submit
     Logout URL:  http://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.

10.2.7 Configure Access Manager

This section describes how to configure Access Manager to integrate with Oracle Identity Federation:

- In SP mode, where Access Manager will delegate authentication to Oracle Identity Federation for Federation SSO.
- In Authentication mode, where Oracle Identity Federation will delegate authentication to Access Manager.

This section contains these topics:

10.2.7.1 Configure OIFScheme

This task configures Access Manager to redirect the user to Oracle Identity Federation for authentication when the OIFScheme is used to protect a resource via Federation SSO. The steps needed to achieve this are as follows:

1. Log in to the Access Manager Administration Console.
2. Select the Policy Configuration tab.
3. Select and open the OIFScheme.
4. In the Challenge URL field, modify the value of OIFHost and port.

5. Confirm that the value of the Context Type drop-down is set to "external".
6. Click **Apply** to save the changes.

10.2.7.2 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 10.2.7.2.1.

If Oracle Identity Federation is used in authentication mode only, refer to Section 10.2.7.2.2.

10.2.7.2.1 Register Oracle Identity Federation for Use in SP Mode

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 to invoke 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/spslooam11g?doneURL=ht
   tp://abc1234567.in.mycorp.com:6001/oam/pages/logout.jsp")
   ```

10.2.7.2.2 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 to invoke when the Access Manager server logs out the user.

For example:

```
registerOIFDAPPartnerIDPMode(logoutURL="http://abcdef0123.in.mycorp.com:1200/fed/user/authnslooam11g?doneURL=http://abc1234567.in.mycorp.com:6001/oam/pages/logout.jsp")
```

10.2.8 Protecting a Resource with OIFScheme

After the integration of Access Manager and Oracle Identity Federation in SP mode, a resource can now be protected via OIFScheme, which will trigger a Federation SSO 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.

10.2.9 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

10.2.9.1 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.
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`

10.2.9.2 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 SSO 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.

Part IV

Monitoring

You can monitor the Oracle IdM environment using Oracle Identity Navigator.

This part contains the following chapters:

- Chapter 11, "Integrating with Oracle Identity Navigator"

11

Integrating with Oracle Identity Navigator

This chapter explains how Oracle Access Management Access Manager (Access Manager) integrates with Oracle Identity Navigator. Using this integration scenario, you can protect Oracle Identity Navigator with Access Manager using a Webgate agent. The instructions in this chapter assume that Oracle Internet Directory is configured as the Identity Store. Other component configurations are possible. Refer to the system requirements and certification documentation on Oracle Technology Network for more information about supported configurations

Note: This is a specific example of Access Manager used to protect URLs. Although it outlines the general approach for this type of configuration, you are not limited to using the exact steps and components used here. For example, Oracle Internet Directory is one of several identity stores certified with Access Manager 11*g*.

Note: Beginning with release 11.1.1.5.0, Oracle Identity Navigator is protected by the domain agent out-of-the-box. In earlier releases, this was not the case; manual configuration was required to protected the URLs.

This chapter contains this section:

11.1 Enabling Single Sign-On

You can use Access Manager to SSO-enable the Oracle Identity Navigator Administration Console using any Access Manager authentication scheme as the challenge method.

The prerequisites are as follows:

- Oracle HTTP Server has been installed.

  When installing Oracle HTTP Server, deselect Oracle WebCache and associated selected components with WebLogic domain.

- Access Manager 11*g* has been installed and configured properly.
- Oracle HTTP Server 11*g* has been installed and configured as a front-ending proxy web server for Oracle Identity Navigator.

- Access Manager 11*g* Webgate for Oracle HTTP Server 11*g* has been installed on the Oracle HTTP Server 11*g*.

  See Also: *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* for details about installation of the listed components.

The high-level SSO-enablement steps are as follows:

- Use the Oracle Access Management Administration Console to configure a new resource for the agent under which the Oracle Identity Navigator URL is to be protected. For information, see Configure a New Resource for the Agent.
- Configure Oracle HTTP Server to point to the Access Manager domain which has the resources and policies configured. For information, see Configure Oracle HTTP Server for the Access Manager Domain.
- Use the Oracle WebLogic Server Administration Console to add the two new identity providers, namely OAMIdentityAsserter and the OIDAuthenticator. For information, see Add New Identity Providers.
- Use Oracle Directory Services Manager (ODSM) to grant administrator privileges to the login user. For information, see Add New Identity Providers.
- Use a WLST command to enable access to more than one application using multiple tabs in a browser session. For information, see Configure Access to Multiple Applications

11.1.1 Configure a New Resource for the Agent

Perform these steps in the Oracle Access Management administration console:

1. Select the **Policy Configuration** tab.
2. Under **Application Domains**, select the agent under which the Oracle Identity Navigator URL is to be protected (for example, -OIMDomain).
3. Choose **Resources** and click the **create** icon to add a new resource. Enter the type, host identifier and value, (/oinav/…/*) and click the **Apply** button.
4. Choose Protected Policy or the policy whose authentication schema is the LDAP schema. In the resources table, click the **add** icon and choose the Oracle Identity Navigator URL (/oinav/…/*) from the drop-down list.
5. Repeat the step for Authorization Policy.

11.1.2 Configure Oracle HTTP Server for the Access Manager Domain

Perform these steps to ensure that Oracle HTTP Server front ends the Oracle WebLogic Server container where Oracle Identity Navigator is installed.

1. Navigate to the Oracle HTTP Server server `config` directory, for example, `/scratch/mydir1/oracle/product/11.1.1/as_1/instances/instance1/config/OHS/ohs1`), and find the `mod_wl_ohs.conf` file.
2. In the `<IfModule mod_weblogic.c>` block, add the host and the port number of the Oracle Identity Navigator URL to be protected. For example:

   ```
   MatchExpression /oinav* WebLogicHost=host WebLogicPort=port
   ```

3. Restart the Oracle HTTP Server server in the Oracle HTTP Server install `bin` directory, for example, `/scratch/mydir1/oracle/product/11.1.1/as_1/instances/instance1/bin`) by executing the following command:

   ```
   -./opmnctl restartproc ias=component=ohs1
   ```

11.1.3 Add New Identity Providers

Perform these steps to add two new identity providers and grant administrator privileges to the login user:

1. Using the Oracle WebLogic Server Administration Console, navigate to **Security Realms**, then **myreleam**, then **Providers**.
2. Add these two providers: OAMIdentityAsserter and OIDAuthenticator.
3. Set the Control Flag of the OAMIdentityAsserter to `Required`
4. Update the following settings in the OIDAuthenticator:
   - Set the Control Flag to `Sufficient`
   - Select the **Provider specific** tab and make the necessary changes, supplying the host, port, and other credentials of the Oracle Internet Directory server. Configure the correct LDAP setting in the OID Authenticator.

   The users and Groups in the LDAP will be reflected in the console.
5. Use Oracle Directory Services Manager (ODSM) to give the administrator privilege to the login user:
   a. Create a user in the LDAP server that is associated with Access Manager, for example: `uid=testuser,cn=users,dc=us,dc=oracle,dc=com`
   b. Create an Administrators group in the LDAP directory, namely `cn=Administrators,cn=groups,dc=us,dc=oracle,dc=com`
   c. Assign the Administrators role to the user, `testuser`, by adding the user to the Administrator group.
   d. You can now test an SSO by this user to Oracle Identity Navigator.
6. Re-order the providers as follows:
   a. OAMIdentityAsserter
   b. Authenticator
   c. Default Authenticator
   d. Default Identity Asserter
7. Restart Oracle WebLogic Server.
8. Enter the protected Oracle Identity Navigator URL, which will have the host and port from the Oracle HTTP Server install:

   `http://`*`OHSHost:OHSPort`*`/oinav/faces/idmNag.jspx`

11.1.4 Configure Access to Multiple Applications

The following applies when SSO protection is provided by an 11*g* OAM Server. Perform these steps to configure access to applications using multiple tabs in a single browser session by changing to FORM cache mode.

1. Stop the Access Manager Managed Servers.

2. Execute the following online Access Manager WLST command:

   ```
   configRequestCacheType(type='FORM')
   ```

3. Restart the Access Manager Managed Servers.

Part V

Additional Identity Store Configuration

This part contains topics related to additional configuration of the identity store.

This part contains the following chapter:

12

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:

12.1 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 12.3, "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 7.4.1, "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 12.3, "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.

12.2 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:

12.2.1 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.

12.2.2 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.

12.2.3 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 12–1.
- 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.

12.2.4 Directory Structure Overview - Shadow Join

Figure 12–1 shows the directory structure in the primary and shadow directories. The containers `cn=reservation`, `cn=appIDUsers`, `cn=FusionGroups`, and `cn=DataRoleGroups` are speciric to Fusion Applications.

Figure 12–1 Directory Structure

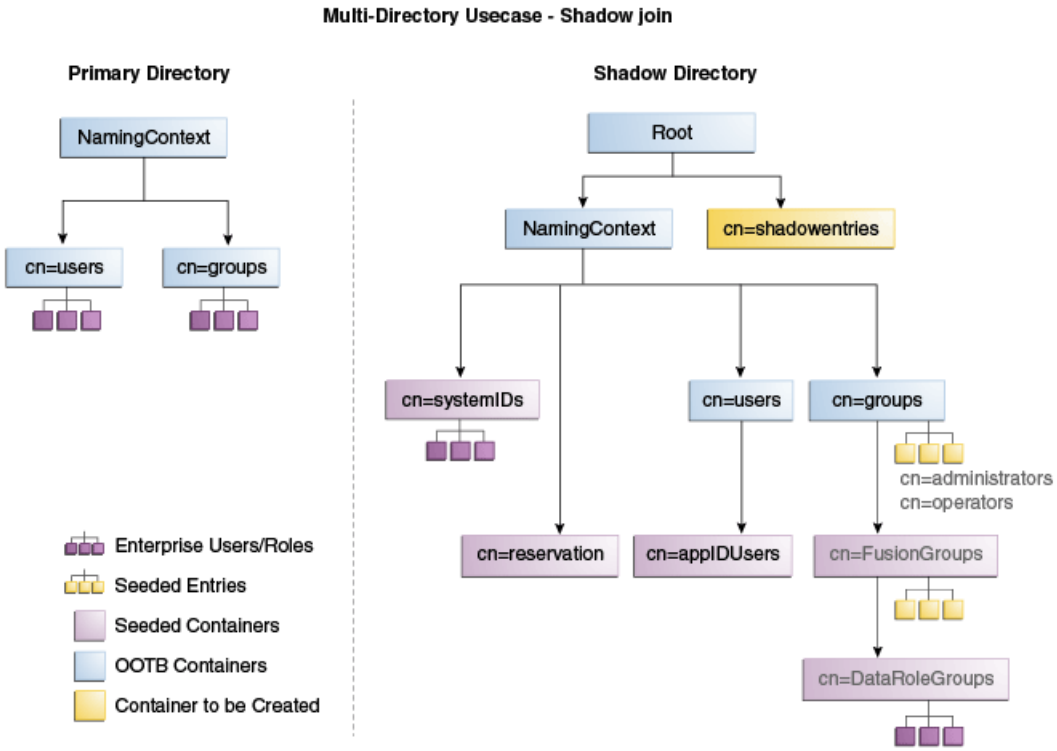


Figure 12–2 shows how the DIT appears to a user or client application. The containers `cn=appIDUsers`, `cn=FusionGroups`, and `cn=DataRoleGroups` are speciric to Fusion Applications.

Figure 12–2 Client View of the DIT

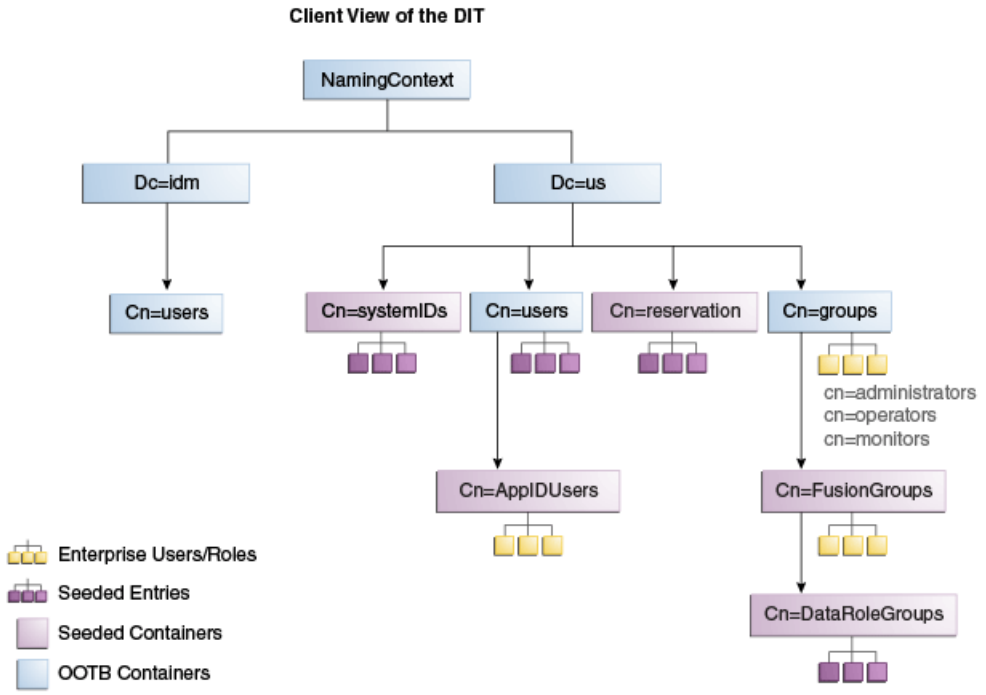
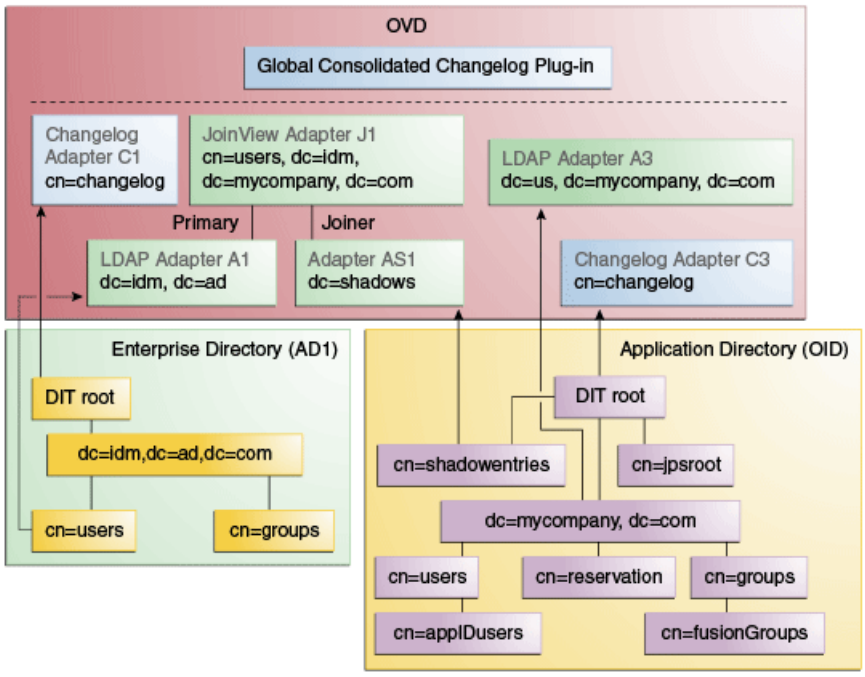


Figure 12–3 summarizes the adapters and plug-ins. The containers `cn=appIDUsers`, and `cn=FusionGroups` are speciric to Fusion Applications.

Figure 12–3 Adapter and Plug-in Configuration



12.2.5 Configuring Oracle Virtual Directory Adapters for Split Profile

In order to produce the client side view of the data shown in Figure 12–2, 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.

12.2.6 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**.

12.2.7 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.

12.3 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 *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity 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:

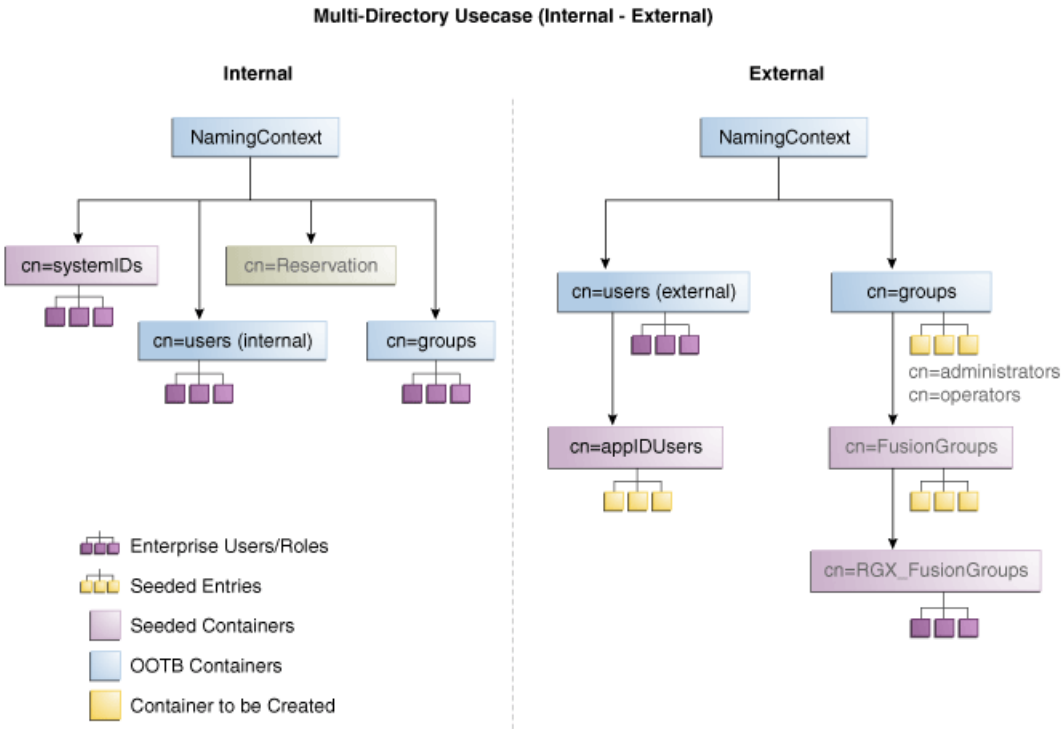
- Enterprise Directory Identity data is in one or more directories. Application-specific attributes of users and groups are stored in the Enterprise Directory.
- Application-specific entries are in the Application Directory. AppIDs and Enterprise Roles are stored in the Application Directory,

This section contains the following topics:

12.3.1 Directory Structure Overview for Distinct User and Group Populations in Multiple Directories

Figure 12–4 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 12–4 Directory Structure



Oracle Virtual Directory makes multiple directories look like a single DIT to a user or client application, as shown in Figure 12–5. The containers cn=appIDUsers, cn=FusionGroups, and cn=RGX_FusionGroups are Fusion Applications-specific.

Figure 12–5 Client View of the DIT

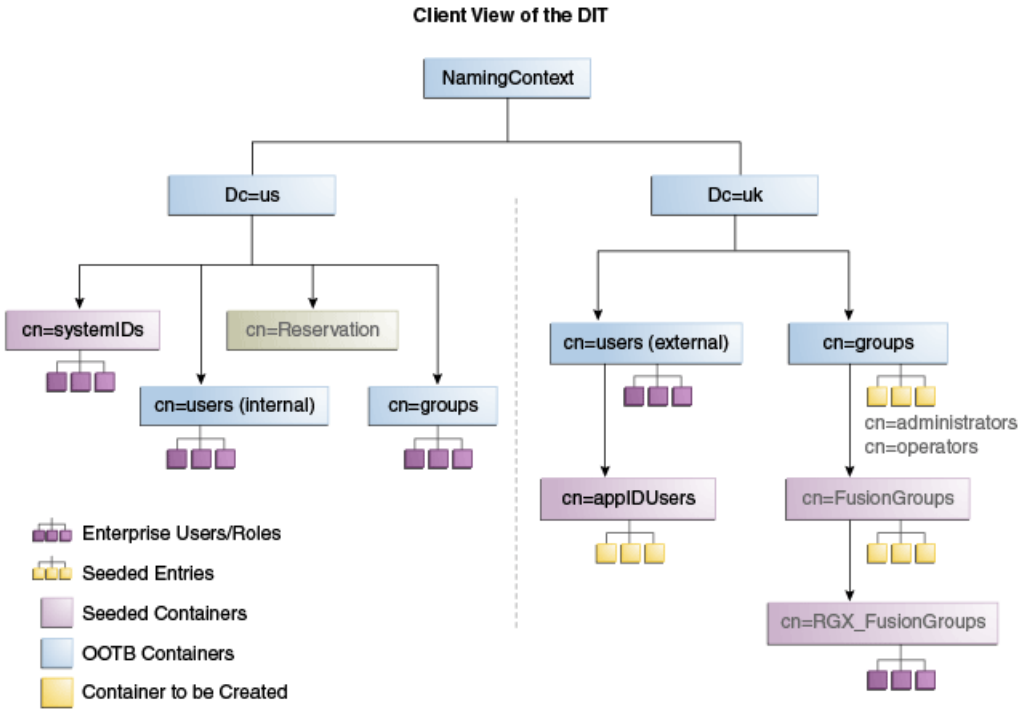
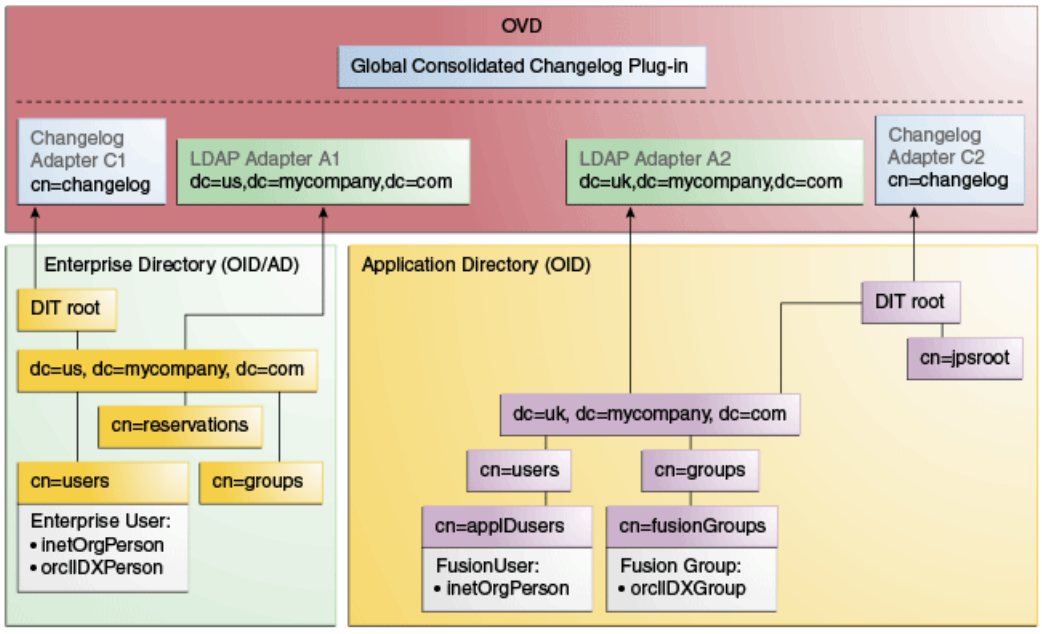


Figure 12–6 provides an overview of the adapter configuration. The classes `inetOrgPerson`, `orclIDXPerson`, and `orclIDXGroup` and the containers `cn=appIDusers` and `cn=fusionGroups` are required only for Fusion Applications.

Figure 12–6 Configuration Overview



12.3.2 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

12.3.2.1 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 `idmconfgTool` 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 `idmconfgTool`, 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 depends on whether you are configuring the Oracle Internet Directory adapter or the Active Directory Adapter.

   - **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
     ```

   - **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.password:adpassword
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.

12.3.2.2 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 `idmconfgTool` 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.

12.3.3 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.

12.4 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 VI

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"

A

Verifying Adapters for Multiple Directory Identity Stores by Using ODSM

After you have configured your Oracle Virtual Directory adapters as described in Chapter 12, "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 12.2.5, "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 as 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%,%orclshortuid%`	
mapAttribute	`mail=userPrincipalName`	
mapAttribute	`ntgrouptype=grouptype`	
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.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=orclContainer`	`Yes`
oimDateFormat	yyyyMMddHHmmss'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=orclContainer`	`Yes`
oimDateFormat	yyyyMMddHHmmss'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`
virtualDITAdapterName	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 12.3.2, "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%,%orclshortuid%`	
mapAttribute	`mail=userPrincipalName`	
mapAttribute	`ntgrouptype=grouptype`	
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.

B

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 self and advanced admin webapp consoles(canonic webapp)

   <Location /oim>
      SetHandler weblogic-handler
      WLCookieName    oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

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

# oim admin console(idmshell based)
   <Location /admin>
      SetHandler weblogic-handler
      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

    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>

## 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 "/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

# 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 self and advanced admin webapp consoles(canonic 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>

# oim admin console(idmshell based)
   <Location /admin>
      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>

# spml xsd profile
   <Location /spml-xsd>
      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>

# used for FA Callback service.
   <Location /callbackResponseService>
      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>

## 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 "/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

# 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 self and advanced admin webapp consoles(canonic webapp)

   <Location /oim>
      SetHandler weblogic-handler
      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

    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 "/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
      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 self and advanced admin webapp consoles(canonic 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>

# oim admin console(idmshell based)
   <Location /admin>
      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>
```

Index

K

L

N

O

P

S

T

U

W