Oracle® Fusion Middleware

Integration Overview for Oracle Identity Management Suite

11*g* Release 1 (11.1.1)

E15477-03

August 2012

Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite, 11*g* Release 1 (11.1.1)

E15477-03

Primary Author: Vinaye Misra

Contributors: Sidhartha Das, Ellen Desmond, Subbu Devulapalli, Sandy Lii, Kavya Muthanna, Sanjay Rallapalli, Vinay Shukla, Olaf Stullich, Lyju Vadassery, Mark Wilcox

Contents

5 Risk Management

6 User, Account, and Entitlement Provisioning

7 Identity Governance

8 Password Management

9 Database Security

10 Fine-Grained Access Control

11 Configuring an Identity Store with Multiple Directories

A Using the idmConfigTool Command

B Verifying Adapters for Multiple Directory Identity Stores by Using ODSM

Index

Preface

This document describes the Identity Management integration options in Oracle Fusion Middleware 11*g* Release 1 (11.1.1).

Audience

This document is intended for system administrators responsible for integrating identity management components and related third-party products for Oracle Fusion Middleware 11*g* Release 1 (11.1.1).

For specific interoperability details about the products mentioned in this guide, consult the certification matrix for Oracle Fusion Middleware 11g Release 1 (11.1.1.x), which is located at:

`http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html`

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 Oracle Fusion Middleware 11*g* documentation set:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*
- *Oracle Access Manager Integration Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*
- *Oracle Fusion Middleware Introduction to Oracle Entitlements Server*
- *Understanding WebLogic Security*
- *Oracle Fusion Middleware Securing Oracle WebLogic Server*
- *Programming WebLogic Security*

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.
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 in Security Integration

This chapter lists new integration features and updates.

New Features in 11g Release 1 (11.1.1.5.0)

New Integration Features

- A new integration tool is available in this release to help automate certain integration steps.

  For details, see Appendix A.

- Oracle Enterprise Single Sign-On Suite Plus (previously known as Oracle Enterprise Single Sign-On Suite) includes a new module and additional features.

  For details, see Chapter 3.

1 Introduction

This chapter introduces basic Oracle Fusion Middleware integration concepts. It contains these topics:

- About Oracle Identity Management
- Objectives of Integration
- Types of Integration
- Key Integration Scenarios
- How to Use this Book

1.1 About Oracle Identity Management

Oracle Identity Management provides customers with a path to meet compliance efficiently, secure critical applications and sensitive data, and lower operational costs. Using the most complete and best-in-class suite of IdM solutions, enterprises can manage the end-to-end lifecycle of user identities across all enterprise resources both within and beyond the firewall.

Through its foundation for service-oriented security, Oracle Identity Management 11*g* delivers enhanced security by automating provisioning of user accounts, dramatically reducing help desk calls, streamlining compliance audit and reporting, consolidating identity silos, enabling rapid integration with enterprise applications, and more.

Successful integration with identity management technologies is key to the secure operation of today's enterprise applications. This document will enable you to assess the tools and techniques that Oracle IdM provides to enable you to run secure enterprise operations.

1.2 Objectives of Integration

Components of Oracle Identity Management typically integrate with the existing infrastructure and applications in the enterprise. Some examples:

- A directory service may provide a centralized user store for existing applications that are LDAP-enabled.
- An access management solution may provide single sign-on and web authorization for existing Web applications in concert with the application servers deployed in the enterprise.
- A provisioning solution may streamline the onboarding procedure by orchestrating the various entities and accounts that need to be created across multiple systems when a new employee is hired.

- A role management solution may provide the necessary scoping to enforce audit rules.

Designed to help you respond and adapt to the needs of your enterprise, Oracle Identity Management presents a highly heterogeneous solution that gives you many different options to enhance security in your existing environment. Understanding the business requirements and implementing the right level of integration is the key to a successful identity management deployment.

Based on functional areas, this document provides a high-level guide to the types of integration available in each Oracle Identity Management product.

Its objective is to enable you to easily identify the capabilities and integrations available for your current enterprise deployment and to plan its future road map.

1.3 Types of Integration

This section explains the different types of possible IdM integrations:

- Integration Among Oracle Identity Management Components
- Integration for other Oracle products
- Integration for Third-Party products

1.3.1 Integration Among Oracle Identity Management Components

Many Oracle Identity Management components can integrate and interoperate with each other. For example, Oracle Access Manager can provide single sign-on for products such as Oracle Identity Manager and Oracle Identity Analytics.

This book covers the range of Oracle Identity Management component integrations.

1.3.2 Integration for other Oracle products

Oracle products cover a large spectrum of the technology stack, with products in all of these areas:

- operating systems
- virtual machines
- databases
- middleware
- applications

Oracle Identity Management is well equipped to handle many of the security requirements in each of these areas. Depending on your requirements, Oracle Identity Management can integrate with many products from the rest of the Oracle technology stack to provide additional security and identity management-related features to these products.

For example, Oracle Identity Manager provides user account management and provisioning support for Oracle E-Business Suite and Oracle PeopleSoft. This book will also cover those integration scenarios.

1.3.3 Integration for Third-Party products

For customers with non-Oracle products in their enterprise deployment, Oracle Identity Management can also integrate with many third-party products to strengthen and satisfy your business requirements.

For example, many of our LDAP-enabled products can be readily integrated with Microsoft Active Directory. You can use Oracle Access Manager, for example, to support Windows Native Authentication for web applications by integrating with a Microsoft Windows domain.

Where relevant, this book covers security integration scenarios between Oracle Identity Management and third-party products.

1.4 Key Integration Scenarios

Table 1–1 lists some key areas of integration in the identity management suite, and the components/products involved in each area.

Table 1–1 Key Integration Scenarios

Objective	Description	Components
Web Access Management	Centralized access management, single sign-on, fine-grained authentication and entitlement control.	Oracle Access Manager Oracle Identity Manager Oracle Adaptive Access Manager Oracle Entitlements Server
Federation	Authentication and single sign-on across security domains.	Oracle Identity Federation Oracle HTTP Server Oracle Access Manager Oracle Internet Directory Oracle Directory Server Enterprise Edition Third-party Directories
Enterprise Single Sign-On	Enable single sign-on in a distributed enterprise and through a variety of sign-on interfaces.	Oracle Access Manager Oracle Enterprise Single Sign-On Oracle Identity Manager Oracle Waveset IBM Tivoli Identity Manager
Risk Management	Protect your exposed Web applications, services, and end-users from online threats and insider fraud.	Oracle Adaptive Access Manager
User, Account, and Entitlement Provisioning	Provision users, accounts, and entitlements for your enterprise applications.	Oracle Identity Manager
Password Management	Options for integrating password management solutions into the enterprise.	Oracle Access Manager Oracle Adaptive Access Manager Oracle Identity Manager

Table 1–1 (Cont.) Key Integration Scenarios

Objective	Description	Components
Identity Governance	Intelligent controls to enable sustainable risk and compliance management.	Oracle E-Business Suite Oracle Application Access Controls Governor SAP GRC
Database Security	Advanced database security features and integration of IdM with Oracle and third-party directory environments.	Oracle Internet Directory Oracle Virtual Directory Oracle Directory Server Enterprise Edition Microsoft Active Directory
Fine-Grained Access Control	Fine-grained entitlement management solution to secure critical applications.	Oracle Entitlements Server

1.5 How to Use this Book

Use this book to understand the major integration options available to meet your site's requirements. Use the references provided with each topic to learn more about each option, including specific prerequisites, installation, and post-install configuration.

The book contains a comprehensive cross-product index that you can use to quickly locate a topic of interest. Each integration topic is indexed twice, once for each component/product in the integration. For example, the Oracle Identity Manager connector for Microsoft Exchange is indexed under both Microsoft Exchange and Oracle Identity Manager. This allows you to see what types of integration are available for any particular Oracle Identity Management component. It also allows you to see all the relevant integration options Oracle Identity Management supports for a particular Oracle product or third-party product from the reverse angle, that is, from the latter perspective.

2 Web Access Management

Oracle Access Manager provides Web single sign-on to enable secure access to multiple applications with one authentication step. It also provides flexible support for all popular authentication methods, including login forms, digital certificates, and smart cards.

This chapter explains how you can integrate Oracle Access Manager with other components to enable Web access management for your enterprise applications. It contains these sections:

- Oracle Access Manager for Oracle Identity Management
- Oracle Access Manager for Oracle Fusion Middleware
- Oracle Access Manager for Other Oracle Applications
- Oracle Access Manager for Third-Party Applications

2.1 Oracle Access Manager for Oracle Identity Management

Oracle Access Manager provides single sign-on support for many Oracle Identity Management components. It also integrates with some Oracle Identity Management components to support more advanced features for those components.

Oracle Access Manager with Oracle Security Token Service brokers trust between a Web Service Consumer (WSC) and a Web Service Provider (WSP).

Table 2–1 shows the supported integrations:

Table 2–1 Oracle Access Manager for Oracle Identity Management

Oracle Access Manager Integrated with	Additional Information
Oracle Identity Manager	Enabling Identity Administration with Oracle Identity Manager in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*
Oracle Adaptive Access Manager	Integrating Oracle Access Manager and Oracle Adaptive Access Manager in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager* Configuring OAM and OAAM with Other Oracle Identity Management Products in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*

Table 2–1 (Cont.) Oracle Access Manager for Oracle Identity Management

Oracle Access Manager Integrated with	Additional Information
Oracle Identity Navigator	Integrating with Oracle Identity Navigator in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*
Oracle Identity Federation	Chapter 4, "Federation"
Oracle Security Token Service	About Oracle Security Token Service with Oracle Access Manager in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*

2.2 Oracle Access Manager for Oracle Fusion Middleware

Oracle Access Manager integrates with various Oracle Fusion Middleware components to provide single sign-on support for applications running on Oracle WebLogic servers.

Oracle Access Manager with Oracle Security Token Service enables identity propagation for a Web Service Client.

Table 2–2 shows the supported integrations:

Table 2–2 Oracle Access Manager for Oracle Fusion Middleware

Oracle Access Manager Integrated with	Additional Information
Oracle WebLogic Server 11*g*	Configuring Oracle Access Manager (OAM) in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* Registering Partners (Agents and Applications) Remotely in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.
Oracle HTTP Server 11*g*	Configuring Oracle Access Manager (OAM) in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* Registering Partners (Agents and Applications) Remotely in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.
Oracle HTTP Server 10*g*	Platform-specific Oracle Application Server Installation Guide for 10*g*. In particular see the chapter Configuring the Apache v1.3 and Oracle HTTP Server Web Servers.
Oracle Business Intelligence	
Oracle WebCache	
Oracle Web Services Manager	About Oracle Security Token Service and Oracle Web Services Manager in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service* Typical Deployment Topology and Processing for Identity Propagation in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*
Oracle Application Server 10*g*	Platform-specific Oracle Application Server Installation Guide for 10*g*. Integrating with Oracle Application Servers in the Oracle Access Manager Integration Guide for 10*g*

2.3 Oracle Access Manager for Other Oracle Applications

Oracle Access Manager integrates with several enterprise applications from Oracle to support Web access management. Table 2–3 shows the supported integrations:

Table 2–3 Oracle Access Manager for Other Oracle Applications

Oracle Access Manager Integrated with	Additional Information
Oracle E-Business Suite	http://www.oracle.com/technology/products/id_mgmt/pdf/idm_tech_wp_11g_r1.pdf
Siebel	http://www.oracle.com/technology/products/id_mgmt/pdf/idm_tech_wp_11g_r1.pdf
PeopleSoft Enterprise	Deploying Oracle Access Manager 10g SSO Solutions in the *Oracle Fusion Middleware Application Security Guide*. Introduction to the OAM Policy Model, Single Sign-On, and Sign-Off in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*. *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*

2.4 Oracle Access Manager for Third-Party Applications

Oracle Access Manager supports integration with many third-party products to provide web access management in a heterogeneous enterprise environment. Table 2–4 shows the supported integrations:

Table 2–4 Oracle Access Manager for Third-Party Applications

Oracle Access Manager Integrated with	Additional Information
Apache Web servers	Configuring 10g WebGates for Apache v2-based Web Servers (OHS and IHS) in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*
SAP mySAP	
IBM Lotus Domino	Configuring Lotus Domino Web Servers for 10g WebGates in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*
IBM HTTP Server	Configuring 10g WebGates for Apache v2-based Web Servers (OHS and IHS) in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*
Microsoft SharePoint	See the white paper Securing Microsoft Office SharePoint Server (MOSS) Resources at: http://download.oracle.com/docs/cd/E12890_01/ales/docs32/integrateappenviron/moss.html
Microsoft Internet Information Server (IIS)	Configuring 10g WebGates for the IIS Web Server in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*
Microsoft Internet and Security Acceleration Server (ISA)	Configuring 10g WebGates for the ISA Server in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*
Windows Native Authentication	Configuring Oracle Access Manager to use Windows Native Authentication in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*

3

Enterprise Single Sign-On

Oracle Enterprise Single Sign-On Suite Plus provides users with unified sign-on and authentication across all their enterprise resources. Unlike Oracle Access Manager which focuses on web access management, Oracle Enterprise Single Sign-On Suite Plus also covers desktops, client-server, custom, and host-based mainframe applications.

Even if users travel or share workstations, they can enjoy the flexibility of a single log-on, eliminating the need for multiple user names and passwords and helping enforce strong password and authentication policies.

This chapter contains topics related to enterprise single sign-on:

- Enterprise Single Sign-On Logon Manager
- Enterprise Single Sign-On Synchronization
- Enterprise Single Sign-On Provisioning Gateway
- Enterprise Single Sign-On Authentication Manager

> **See Also:** For the latest information about the suite, see *Oracle Enterprise Single Sign-on Suite Plus Release Notes* (Release 11.1.1.5.0).

3.1 Enterprise Single Sign-On Logon Manager

Oracle Enterprise Single Sign-On Suite Logon Manager (ESSO-LM) provides interfaces to network and computer logons as well as sign-on to applications, enabling users to log in one time with a single password. ESSO-LM handles storage and retrieval of credentials and settings from an external repository such as an LDAP or RDBMS store.

The ESSO-LM administration console interacts with the Logon Manager and facilitates management and administration of ESSO attributes. For details, see the *ESSO-LMGlobal Agent Settings Reference Guide*.

3.2 Enterprise Single Sign-On Synchronization

ESSO Synchronization is a component of Oracle Enterprise Single Sign-On Suite Logon Manager (ESSO-LM). This feature lets you synchronize credentials between an end user's local store (on a workstation) and a store in a remote SSO repository (file system share, relational database, or directory server). You configure synchronization through the ESSO-LM administration console.

Table 3–1 shows the supported integrations:

Table 3–1 Oracle ESSO Synchronization Manager Integrations

ESSO Synchronization Manager Integrated with	Additional Information
Microsoft Active Directory	http://download.oracle.com/docs/cd/E15624_01/logon.11111/SSOAdmin.chm
Microsoft Active Directory Application Mode (ADAM)	http://download.oracle.com/docs/cd/E15624_01/logon.11111/SSOAdmin.chm
LDAP	http://download.oracle.com/docs/cd/E15624_01/logon.11111/SSOAdmin.chm
Database	http://download.oracle.com/docs/cd/E15624_01/logon.11111/SSOAdmin.chm

3.3 Enterprise Single Sign-On Provisioning Gateway

Oracle Enterprise Single Sign-On Suite Provisioning Gateway (ESSO-PG) enables system administrators to directly distribute, reset, remove, or delete user credentials in ESSO-LM without the need for any user involvement.

Here are some examples:

- An administrator can inject a new user's credentials directly into the user's ESSO-LM account.
- The administrator can update ESSO-LM simultaneously to reset a password and prevent an application from falling out of synchronization with ESSO-LM.
- When a user's access to an application is terminated, the administrator can use ESSO-PG to quickly remove the corresponding credentials from the user's ESSO-LM account.
- When a user leaves the company, the administrator can instantly delete all the user's credentials.

All these operations can be automatically initiated and controlled by industry-leading provisioning systems. ESSO-PG provides an open interface to integrate with other industry-standard or internally-developed provisioning systems, and also provides an interactive interface for administrators to manually provision credentials.

Table 3–2 shows the supported integrations:

Table 3–2 Oracle Enterprise Single Sign-On Suite Provisioning Gateway Integrations

ESSO-PG Integrated with	Additional Information
Oracle Identity Manager	http://download.oracle.com/docs/cd/E12472_01/provisioning_gateway/PGWOC.pdf
Oracle Waveset	http://download.oracle.com/docs/cd/E12472_01/provisioning_gateway/EPGSC.pdf
IBM Tivoli Identity Manager	http://download.oracle.com/docs/cd/E12472_01/provisioning_gateway/EPGSC.pdf
Novell Identity Manager	http://download.oracle.com/docs/cd/E15624_01/provisioning.11111/NIMIG.pdf

3.4 Enterprise Single Sign-On Authentication Manager

Oracle Enterprise Single Sign-On Suite Authentication Manager (ESSO-AM), an add-on module to Oracle Enterprise Single Sign-on Logon Manager (ESSO-LM), enables an organization to seamlessly provide a strong authentication bridge to all its applications, including smart cards and Entrust authenticators.

Users can employ different authenticators at different times, and application access can be controlled based upon the authenticator used for all authentication events: initial authentication, re-authentication, and forced authentication.

Table 3–3 shows the supported integrations:

Table 3–3 Oracle Enterprise Single Sign-On Suite Authentication Manager Integrations

ESSO-AM Integrated with	Additional Information
Entrust	`http://download.oracle.com/docs/cd/E15624_01/authentication.11111/ESAIG.pdf`
LDAP	`http://download.oracle.com/docs/cd/E12472_01/authentication_manager/ESAIG.pdf`
Microsoft Windows	`http://download.oracle.com/docs/cd/E12472_01/authentication_manager/ESAIG.pdf`
Proximity cards	`http://download.oracle.com/docs/cd/E12472_01/authentication_manager/ESAIG.pdf`
smart cards	`http://download.oracle.com/docs/cd/E12472_01/authentication_manager/ESAIG.pdf`
RSA SecurID	`http://download.oracle.com/docs/cd/E12472_01/authentication_manager/ESAIG.pdf`

3.5 Enterprise Single Sign-On Universal Authentication Manager

Universal Authentication Manager (ESSO-UAM) is a new component of Oracle Enterprise Single Sign-on Suite Plus Release 11.1.1.5.0. ESSO-UAM enables enterprises to implement stronger and easier-to-use authentication methods, including two-factor authentication methods.

ESSO-UAM supports integrations in these areas:

- Microsoft Windows and Active Directory networks
- smart cards for logon and authentication
- proximity cards that a card reader can detect
- biometric technologies compatible with the BioAPI standard.

For details, see *Oracle Enterprise Single Sign-on Suite Plus Release Notes* (Release 11.1.1.5.0).

4 Federation

Oracle Identity Federation provides a comprehensive implementation of federation standards delivered via Oracle Universal Federation Framework - the unified, extensible and customizable architecture for rapid deployment in any multi-vendor environment.

Oracle Identity Federation allows customers to quickly achieve cross-domain SSO by providing a complete end-to-end federation deployment package, including a simple and lightweight deployment option for Service Providers.

This chapter introduces the integrations for Oracle Identity Federation:

- Oracle Identity Federation for Oracle Identity Management
- Oracle Identity Federation for Oracle Fusion Middleware
- Oracle Identity Federation Authentication Engines
- Oracle Identity Federation Service Provider Integration Modules

4.1 Oracle Identity Federation for Oracle Identity Management

Oracle Identity Federation integrates with several Oracle Identity Management products to provide integrated federation solutions. Table 4–1 shows the supported integrations:

Table 4–1 Oracle Identity Federation for Oracle Identity Management

Oracle Identity Federation Integrated with	Additional Information
Oracle Access Manager	For 11g webgates, see Integrating Oracle Access Manager with Oracle Identity Federation in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager* For 10g webgates, see Oracle Access Manager in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
Oracle Single Sign-On 10g	See Oracle Single Sign-On in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*

4.2 Oracle Identity Federation for Oracle Fusion Middleware

Oracle Identity Federation integrates with Oracle Fusion Middleware products supporting a variety of federation use cases. Table 4–2 shows the supported integrations:

Table 4–2 Oracle Identity Federation for Oracle Fusion Middleware

Oracle Identity Federation Integrated with	Additional Information
Oracle HTTP Server for Oracle Access Manager integration	Deploying Oracle Identity Federation with Oracle Access Manager in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
Oracle HTTP Server to set up proxy for Oracle Identity Federation	Setting Up a Proxy for Oracle Identity Federation in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*

4.3 Oracle Identity Federation Authentication Engines

In Oracle Identity Federation, an authentication mechanism defines a method or policy for verifying an entity's claimed identity using submitted credentials. An authentication engine is a module implementing a particular authentication method.

Oracle Identity Federation provides several out-of-the-box authentication engines and supports custom authentication engines. Table 4–3 shows the supported integrations:

Table 4–3 Oracle Identity Federation Authentication Engines

Authentication Engine for	Additional Information
Oracle Access Manager	Authentication Engines - Oracle Access Manager in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
Oracle Single Sign-On 10g	Authentication Engines - Oracle Single Sign-On in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
LDAP Directory	Authentication Engines - LDAP Directory in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
Database Security	Authentication Engines - Database Security in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
Database Table	Authentication Engines - Database Table in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
Microsoft Windows CardSpace (InfoCard)	Authentication Engines - Infocard in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
JAAS	Authentication Engines - JAAS in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
Custom authentication engine	Authentication Engines - Custom in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*

4.4 Oracle Identity Federation Service Provider Integration Modules

A service provider (SP) integration module creates a user authenticated session at an identity and access management (IAM) system like Oracle Access Manager.

Oracle Identity Federation provides several out-of-the-box SP integration modules, and also supports custom service provider integration modules. Table 4–4 shows the supported integrations:

Table 4–4 Oracle Identity Federation SP Integration Modules

Oracle Identity Federation SP Integration Module for	Additional Information
Oracle Access Manager	SP Integration module - Oracle Access Manager in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
Oracle Single Sign-On 10*g*	SP Integration module - Oracle Single Sign-On in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
Custom SP Integration Module for third-party IAM system	SP Integration Module - Custom in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*

5 Risk Management

Oracle Adaptive Access Manager supports companies by protecting their exposed Web applications, services, and end-users from online threats and insider fraud. Oracle Adaptive Access Manager features include:

- risk-aware authentication,
- real-time behavior profiling,
- transaction and event risk analysis.

Oracle Adaptive Access Manager provides real-time or offline risk analysis by calculating the risk of an access request, an event or a transaction and determining proper outcomes to prevent fraud and misuse. A portion of the risk evaluation is dedicated to verifying a user's identity and determining if the activity is suspicious.

Oracle Adaptive Access Manager provides end-user-facing functionality to prevent fraud through its Virtual Authentication Devices to secure credential data at the entry point.

Oracle Adaptive Access Manager also provides interdiction methods including risk-based authentication, blocking, and configurable actions to interdict in other systems.

This chapter explains how you can integrate Oracle Adaptive Access Manager with other components to provide risk management for your enterprise applications. It contains these sections:

- Oracle Adaptive Access Manager for Oracle Identity Management
- Oracle Adaptive Access Manager for Custom Applications

5.1 Oracle Adaptive Access Manager for Oracle Identity Management

Oracle Adaptive Access Manager integrates with other Oracle Identity Management components to provide additional risk management support.

Table 5–1 shows the supported integrations:

Table 5–1 Oracle Adaptive Access Manager for Oracle Identity Management

Oracle Adaptive Access Manager Integrated with	Additional Information
Oracle Access Manager	Integrating Oracle Access Manager and Oracle Adaptive Access Manager in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*
Oracle Identity Manager for password flow	Deployment Options for Password Management in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*
Oracle Internet Directory as an authentication provider	Oracle Identity Management Suite-Level Installation Scenarios in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
Oracle Virtual Directory as an authentication provider	Oracle Identity Management Suite-Level Installation Scenarios in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*

5.2 Oracle Adaptive Access Manager for Custom Applications

Oracle Adaptive Access Manager provides a variety of mechanisms to integrate with custom applications.

Applications can integrate natively with Oracle Adaptive Access Manager using APIs. The Universal Installer reverse proxy deployment option offers login risk-based, multi-factor authentication to web applications without requiring any change to the application code.

Table 5–2 shows the supported integrations:

Table 5–2 Oracle Adaptive Access Manager with Custom Applications

Oracle Adaptive Access Manager Integration	Additional Information
using Web Services and SOAP API	Using Web Services and SOAP API in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
using Java API	Integrating Native Java Applications in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
using OAAM Proxy for Internet and Security Acceleration Server (ISA)	Installing Oracle Adaptive Access Manager Proxy for Microsoft ISA in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
using OAAM Proxy for Apache	Installing Oracle Adaptive Access Manager Proxy for Apache in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*

6 User, Account, and Entitlement Provisioning

Oracle Identity Manager provides a comprehensive provisioning solution for many enterprise resources. Predefined connectors and a flexible Adaptor Factory enable customers to easily establish connectivity with well-known targets and custom systems.

This connectivity forms the basis of Oracle Identity Manager, enabling you to provide support for self-service and delegated administration, password management, provisioning, and request and approval workflow across many enterprise targets.

This chapter explains how you can integrate Oracle Identity Manager with other components to provision users, accounts, and entitlements for your enterprise applications. It contains these sections:

- Oracle Identity Manager Connectors for Oracle Identity Management
- Oracle Identity Manager Connectors for Databases
- Oracle Identity Manager Connectors for Oracle Applications
- Oracle Identity Manager Connectors for Third-Party Applications

6.1 Oracle Identity Manager Connectors for Oracle Identity Management

Table 6–1 shows the Oracle Identity Manager connectors for Oracle Identity Management components:

Table 6–1 Oracle Identity Manager Connectors for Oracle Identity Management

Oracle Identity Manager Connector for	Additional Information
Oracle Internet Directory	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Oracle" connector group, select the Oracle Internet Directory document.
Oracle Directory Server Enterprise Edition[1]	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Sun" connector group, select the Sun Java System Directory document.

[1] formerly Sun Java System Directory Server

6.2 Oracle Identity Manager Connectors for Databases

Table 6–2 shows the Oracle Identity Manager connectors for databases:

Note: These are generic database connectors and support other databases in addition to Oracle RDBMS.

Table 6–2 Oracle Identity Manager Connectors for Databases

Oracle Identity Manager Connector for	Additional Information
Database User Management	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Databases" connector group, select the Database User Management document.
Database Application Tables	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Databases" connector group, select the Database Application Tables document.

6.3 Oracle Identity Manager Connectors for Oracle Applications

Table 6–3 shows the Oracle Identity Manager connectors for Oracle applications:

Table 6–3 Oracle Identity Manager Connectors for Oracle Applications

Oracle Identity Manager Connector for	Additional Information
JD Edwards EnterpriseOne User Management	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Oracle" connector group, select the JD Edwards EnterpriseOne User Management document.
Oracle E-Business Employee Reconciliation	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Oracle" connector group, select the Oracle E-Business Employee Reconciliation document.
Oracle E-Business User Management	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Oracle" connector group, select the Oracle E-Business User Management document.
Oracle Retail Warehouse Management System	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Oracle" connector group, select the Oracle Retail Warehouse Management System document.
PeopleSoft Employee Reconciliation	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Oracle" connector group, select PeopleSoft Employee Reconciliation document.
PeopleSoft User Management	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Oracle" connector group, select the PeopleSoft User Management document.
Siebel User Management	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Oracle" connector group, select the Siebel User Management document.

6.4 Oracle Identity Manager Connectors for Third-Party Applications

Table 6–4 shows the Oracle Identity Manager connectors for third-party applications:

Table 6–4 Oracle Identity Manager Connectors for Third-Party Applications

Oracle Identity Manager Connector for	Additional Information
BMC Remedy User Management	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "BMC" connector group, select the BMC Remedy User Management document.
BMC Remedy Ticket Management	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "BMC" connector group, select the BMC Remedy Ticket Management document.
Computer Associates ACF2 Advanced	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Computer Associates" connector group, select the CA ACF2 Advanced document.
Computer Associates Top Secret Advanced	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Computer Associates" connector group, select the CA Top Secret Advanced document.
Database User Management	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Databases" connector group, select the Database User Management document.
Database Application Tables	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Databases" connector group, select the Database Application Tables document.
IBM Resource Access Control Facility (RACF) Standard	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "IBM" connector group, select the IBM RACF Standard document.
IBM RACF Advanced	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "IBM" connector group, select the IBM RACF Advanced document.
IBM OS/400 Advanced	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "IBM" connector group, select the IBM OS/400 Advanced document.
IBM Lotus Notes and Domino	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "IBM" connector group, select IBM Lotus Notes and Domino documents.
Microsoft Active Directory User Management	http://download.oracle.com/docs/cd/E11223_01/index.htm Under the "Microsoft" connector group, select the Microsoft Active Directory User Management document.

Table 6–4 (Cont.) Oracle Identity Manager Connectors for Third-Party Applications

Oracle Identity Manager Connector for	Additional Information
Microsoft Active Directory Password Synchronization	`http://download.oracle.com/docs/cd/E11223_01/index.htm` Under the "Microsoft" connector group, select the Microsoft Active Directory Password Synchronization document.
Microsoft Exchange	`http://download.oracle.com/docs/cd/E11223_01/index.htm` Under the "Microsoft" connector group, select Microsoft Exchange documents.
Microsoft Windows	`http://download.oracle.com/docs/cd/E11223_01/index.htm` Under the "Microsoft" connector group, select the Microsoft Windows document.
Novell eDirectory	`http://download.oracle.com/docs/cd/E11223_01/index.htm` Under the "Novell" connector group, select the Novell eDirectory document.
Novell GroupWise	`http://download.oracle.com/docs/cd/E11223_01/index.htm` Under the "Novell" connector group, select the Novell GroupWise document.
RSA Authentication Manager	`http://download.oracle.com/docs/cd/E11223_01/index.htm` Under the "RSA" connector group, select the RSA Authentication Manager document.
RSA ClearTrust	`http://download.oracle.com/docs/cd/E11223_01/index.htm` Under the "RSA" connector group, select the RSA ClearTrust document.
SAP Employee Reconciliation	`http://download.oracle.com/docs/cd/E11223_01/index.htm` Under the "SAP" connector group, select the SAP Employee Reconciliation document.
SAP Enterprise Portal	`http://download.oracle.com/docs/cd/E11223_01/index.htm` Under the "SAP" connector group, select the SAP Enterprise Portal document.
SAP User Management	`http://download.oracle.com/docs/cd/E11223_01/index.htm` Under the "SAP" connector group, select the SAP User Management document.
Unix SSH	`http://download.oracle.com/docs/cd/E11223_01/index.htm` Under the "Unix" connector group, select the Unix SSH document.

Table 6–4 (Cont.) Oracle Identity Manager Connectors for Third-Party Applications

Oracle Identity Manager Connector for	**Additional Information**
Unix Telnet	`http://download.oracle.com/docs/cd/E11223_01/index.htm` Under the "Unix" connector group, select the Unix Telnet document.
Custom Connector with Adapter Factory	Developing Adapters in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
Custom Connector with Generic Technology Connectors	Creating and Managing Generic Technology Connectors in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

7

Identity Governance

Oracle Identity Analytics (formerly Sun Role Manager) provides enterprises with the ability to engineer and manage roles and automate critical identity-based controls.

By integrating with the various enterprise systems including applications, operating systems, LDAP directories, and custom applications, Oracle Identity Analytics provides a complete view of access-related data that includes:

- the user's access,
- the why and how of that access, and
- whether the access violates policies.

Oracle Identity Analytics enables you to automate the access certification process and removes inappropriate access by integrating with a provisioning solution. It also provides evidence that the access complies with established policies.

Sections include:

- Oracle Identity Analytics for Oracle Identity Management
- Oracle Identity Analytics for Third-Party Products

7.1 Oracle Identity Analytics for Oracle Identity Management

Oracle Identity Analytics integrates with Oracle Identity Management components to pull in user, account and entitlement data, and to provide closed-loop remediation.

Table 7–1 shows the Oracle Identity Analytics integrations supported for Oracle Identity Management components:

Note: Oracle Waveset was formerly known as Sun Identity Manager.

Table 7–1 Oracle Identity Analytics Integration for Oracle Identity Management

Oracle Identity Analytics Integration for	Additional Information
Oracle Identity Manager	Integrating with Oracle Identity Manager in the *Sun Role Manager 5.0.3 System Integrator's Guide* at: `http://wikis.sun.com/display/Srm503Docs/System+Integrator%27s+Guide`
Oracle WaveSet	Integrating with Sun Identity Manager in the *Sun Role Manager 5.0.3 System Integrator's Guide* at: `http://wikis.sun.com/display/Srm503Docs/System+Integrator%27s+Guide`

To integrate with Oracle Identity Manager and Oracle Waveset, Oracle Identity Analytics leverages the connectors in those components, thus indirectly integrating with the target systems supported by those components.

7.2 Oracle Identity Analytics for Third-Party Products

Oracle Identity Analytics integrates with third-party products to pull in user, account and entitlement data, and to provide closed-loop remediation.

Table 7–2 shows the Oracle Identity Analytics integrations supported for third-party products:

Table 7–2 Oracle Identity Analytics Integration for Third-Party Products

Oracle Identity Analytics Integration	Additional Information
for third-party provisioning servers	Integrating with Other Provisioning Servers in the *Sun Role Manager 5.0.3 System Integrator's Guide* at: `http://wikis.sun.com/display/Srm503Docs/System+Integrator%27s+Guide`
using ETL process	Role Manager ETL Process in the *Sun Role Manager 5.0.3 Business Administrator's Guide* at: `http://wikis.sun.com/display/Srm503Docs/Business+Administrator%27s+Guide`

8 Password Management

This chapter explains how you can integrate with Oracle Identity Manager for centralized password management features. Topics include:

- Oracle Identity Manager Password Management Support for Oracle Identity Management
- Oracle Identity Manager Password Management through Connectors
- Oracle Enterprise Single Sign-On Suite ESSO-PR for Password Reset

8.1 Oracle Identity Manager Password Management Support for Oracle Identity Management

Oracle Identity Manager's password management feature includes password policy support and self-service administration for password reset and password change. Oracle Identity Manager provides centralized password management for other Oracle Identity Management components where password management is needed.

Table 8–1 shows the supported integrations:

Table 8–1 Oracle Identity Manager Password Management Support for Oracle Identity Management

Oracle Identity Manager Integration with	Additional Information
Oracle Access Manager	Deployment Options for Password Management in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.
Oracle Adaptive Access Manager	Deployment Options for Password Management in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.
Oracle Access Manager and Oracle Adaptive Access Manager combined	Deployment Options for Password Management in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.

8.2 Oracle Identity Manager Password Management through Connectors

Oracle Identity Manager provides centralized password management for enterprise applications, a feature that you can leverage by provisioning through its connectors. In this way, you can configure a centralized password policy for the enterprise, allowing your users to specify a single password which can then be provisioned to the various targets where passwords are required.

Password reset, password change, and expiration can all be handled through Oracle Identity Manager's self-service support.

See Chapter 6, "User, Account, and Entitlement Provisioning" for more information on supported connectors.

8.3 Oracle Enterprise Single Sign-On Suite ESSO-PR for Password Reset

Oracle Enterprise Single Sign-on Password Reset (ESSO-PR) allows users to access their Windows user accounts in case they lose or forget their password, without requiring help desk or technical support, improving the operational efficiency of the enterprise.

For details, see the Oracle Enterprise Single Sign-on documentation library at:

http://download.oracle.com/docs/cd/E12472_01/index.htm

ESSO-PR documents are located in the Password Reset Documentation section.

9 Database Security

This chapter describes integrations that support database security. Topics include:

- Oracle Database Net Services LDAP Naming
- Oracle Database Enterprise User Security with LDAP

See Also:

- http://www.oracle.com/technology/deploy/security/database-security/enterprise-user-security/index.html
- http://www.oracle.com/technology/products/id_mgmt/odsee/ovd-dsee-eus.html

Note: DB aliases are not supported.

9.1 Oracle Database Net Services LDAP Naming

To manage large networking environments, administrators must be able to easily access a centralized repository to specify and modify the network configuration. To support this requirement, the Oracle Net Services configuration can be stored in an LDAP-compliant directory server.

Supporting LDAP-compliant directory servers provides the enterprise with a vehicle for centrally managing and configuring a distributed Oracle network. The directory can act as a central repository of information about database network components, user and corporate policies, and user authentication and security, thus replacing localized client-side and server-side configuration files.

Table 9–1 shows the supported integrations:

Table 9–1 Oracle Database Net Services LDAP Naming

Oracle Database Net Services for	Additional Information
Directory Naming with Oracle Internet Directory	Centralized Configuration and Management in the *Oracle Database Net Services Administrator's Guide*. Using a Directory Server for Centralized Management in the *Oracle Database Net Services Administrator's Guide*.
Directory Naming with Oracle Virtual Directory	
Directory Naming with Microsoft Active Directory using Oracle Virtual Directory	Managing Network Address Information in the *Oracle Database Net Services Administrator's Guide*. Using a Directory Server for Centralized Management in the *Oracle Database Net Services Administrator's Guide*.
Directory Naming with Oracle Directory Service Enterprise Edition (formerly Sun Java System Directory Server) using Oracle Virtual Directory	How to set up Enterprise User Security with Oracle Virtual Directory and Oracle Directory Server Enterprise Edition at: `http://www.oracle.com/technology/products/id_mgmt/odsee/ovd-dsee-eus.html`

9.2 Oracle Database Enterprise User Security with LDAP

Enterprise User Security (EUS), a feature of Oracle Database Enterprise Edition, leverages Oracle Directory Services (ODS) to centrally manage database users and role memberships in an enterprise LDAP directory. This provides a way to address the security and management problems posed by maintaining database users and privileges in individual databases.

Table 9–2 shows the supported integrations:

Table 9–2 Oracle Database Enterprise User Security with LDAP

Enterprise User Security Integration for	Additional Information
Oracle Internet Directory	`http://www.oracle.com/technology/products/aid/pdf/dirsrv_eus_integration.pdf`
Microsoft Active Directory using Oracle Virtual Directory	`http://www.oracle.com/technology/products/oid/pdf/dirsrv_eus_integration.pdf`
Oracle Directory Service Enterprise Edition (formerly Sun Java System Directory Server) using Oracle Virtual Directory	`http://www.oracle.com/technology/products/oid/pdf/dirsrv_eus_integration.pdf`

10

Fine-Grained Access Control

Oracle Entitlements Server provides a fine-grained entitlement management solution that secures critical applications with uncompromised performance and reliability. By combining centralized policy management with distributed policy decision-making and enforcement, it enables you to rapidly adapt to changing business requirements.

> **See Also:** Oracle Entitlements Server product page at http://www.oracle.com/technology/products/id_mgmt/oes/index.html

This chapter includes these topics:

- Oracle Entitlements Server for Oracle Identity Management
- Oracle Entitlements Server for Oracle Fusion Middleware and Oracle SOA
- Oracle Entitlements Server for Third-Party products

10.1 Oracle Entitlements Server for Oracle Identity Management

You can integrate Oracle Entitlements Server with Oracle Identity Management components. Table 10–1 shows the supported integrations:

Table 10–1 Oracle Entitlements Server for Oracle Identity Management

Oracle Entitlements Server Integrated with	Additional Information
Oracle Identity Manager	LDAPAuthenticator at: http://download.oracle.com/docs/cd/E12890_01/ales/docs32/adminref/blmconfigapi.html#wp1060276
Oracle Adaptive Access Manager	Custom Attribute Retrievers at: http://download.oracle.com/docs/cd/E12890_01/ales/docs32/adminref/plugins.html#wp1167025
Oracle Access Manager	Use OAM Authentication Provider or Identity Asserter

Table 10–1 (Cont.) Oracle Entitlements Server for Oracle Identity Management

Oracle Entitlements Server Integrated with	Additional Information
Oracle Identity Federation	Use OIF Authentication Provider or Identity Asserter
Oracle Virtual Directory	■ LDAPAuthenticator at: http://download.oracle.com/docs/cd/E12890_01/ales/docs32/adminref/blmconfigapi.html#wp1060276 ■ LDAP Attribute Retrievers at: http://download.oracle.com/docs/cd/E12890_01/ales/docs32/adminref/retrievers.html#wp1171979
Oracle Directory Server Enterprise Edition (ODSEE)	■ LDAPAuthenticator at: http://download.oracle.com/docs/cd/E12890_01/ales/docs32/adminref/blmconfigapi.html#wp1060276 ■ LDAP Attribute Retrievers at: http://download.oracle.com/docs/cd/E12890_01/ales/docs32/adminref/retrievers.html#wp1171979 ■ OES Adapter for ODSEE at: http://download.oracle.com/docs/cd/E12890_01/ales/docs32/integrateappenviron/ales_adapter_appen.html

10.2 Oracle Entitlements Server for Oracle Fusion Middleware and Oracle SOA

You can integrate Oracle Entitlements Server with Oracle Fusion Middleware components. Table 10–2 shows the supported integrations:

Table 10–2 Oracle Entitlements Server for Oracle Fusion Middleware

Oracle Entitlements Server Integrated with	Additional Information
Oracle WebLogic Server (WLS) 8.1.5, 8.1.6, 9.2.2, 10.0 MP1, 10.37, 10.3.1, 10.3.2	Securing WebLogic Servers at: http://download.oracle.com/docs/cd/E12890_01/ales/docs32/integrateappenviron/configWLS.html
Oracle Service Bus (OSB) 2.6, 3.09, 10gR3	Securing Oracle Service Bus Runtime Resources at: http://download.oracle.com/docs/cd/E12890_01/ales/docs32/integrateappenviron/servicebus.html
Oracle Data Service Integrator (ODSI) 2.5, 3.0, 3.18	Securing Oracle Data Service Integrator at: http://download.oracle.com/docs/cd/E12890_01/ales/docs32/integrateappenviron/dataservices.html
Oracle Enterprise Repository	Storing and Versioning Policy with Oracle Enterprise Repository at: http://download.oracle.com/docs/cd/E12890_01/ales/docs32/integrateappenviron/aler.html

10.3 Oracle Entitlements Server for Third-Party products

Oracle Entitlements Server integrates with several third-party products. Table 10–3 shows the supported integrations:

Table 10–3 Oracle Entitlements Server for Third-Party Products

Oracle Entitlements Server Integrated with	Additional Information
Websphere Application Server 6.1	Configuring the WebSphere SSM at: `http://download.oracle.com/docs/cd/E12890_01/ales/docs32/installssms/Config_WebSphereSSM.html`
Microsoft Active Directory 2000 and 2003	ActiveDirectoryAuthenticator at: `http://download.oracle.com/docs/cd/E12890_01/ales/docs32/adminref/blmconfigapi.html#wp1058658`
Microsoft ADAM	ActiveDirectoryAuthenticator at: `http://download.oracle.com/docs/cd/E12890_01/ales/docs32/adminref/blmconfigapi.html#wp1058658`
Microsoft .NET Framework 1.1 and 2.05	Programming Security for Web Services at: `http://download.oracle.com/docs/cd/E12890_01/ales/docs32/webservicesprogrammersguide/index.html`
Microsoft Office SharePoint Server 2007	Securing Microsoft Office SharePoint Server (MOSS) at: `http://download.oracle.com/docs/cd/E12890_01/ales/docs32/integrateappenviron/moss.html`
Open LDAP v2.2.24	OpenLDAPAuthenticator at: `http://download.oracle.com/docs/cd/E12890_01/ales/docs32/adminref/blmconfigapi.html#wp1060851`
Novell eDirectory v8.7.31	NovellAuthenticator at: `http://download.oracle.com/docs/cd/E12890_01/ales/docs32/adminref/blmconfigapi.html#wp1060696`

11 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:

11.1 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 11.4, "Configuring Multiple Directories as an Identity Store: Distinct User and Group Populations in Multiple Directories."
- **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 11.4, "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.

11.2 Using idmConfigTool configOVD to Configure Oracle Virtual Directory

To configure Oracle Virtual Directory adapters as described in this chapter, you must use the `-configOVD` option to the `idmConfigTool` command. Before attempting to use this option with Oracle Fusion Middleware 11*g*R1 (11.1.1.5), ensure that you have applied the latest patches for Oracle Identity Management.

The syntax and properties for this option are as follows:

Syntax

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

Properties

Table 11–1 lists the command properties (where *n*=1,2..).

Table 11–1 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

11.3 Configuring Multiple Directories as an Identity Store: Split Profile

This section describes how to configure multiple directories as an Identity Store. In cases where the Active Directory schema cannot be extended, you use Oracle Internet Directory as a shadow directory to store these attributes. Oracle Virtual Directory links them together to present a single consolidated DIT view to clients. This is called a split profile or split directory configuration. In this configuration, all the Oracle specific attributes and Oracle specific entities are created in Oracle Internet Directory.

This section contains the following topics:

- Section 11.3.1, "Prerequisites"
- Section 11.3.2, "Repository Descriptions"
- Section 11.3.3, "Setting Up Oracle Internet Directory as a Shadow Directory"

- Section 11.3.4, "Directory Structure Overview - Shadow Join"
- Section 11.3.5, "Configuring Oracle Virtual Directory Adapters for Split Profile"
- Section 11.3.6, "Configuring a Global Consolidated Changelog Plug-in"
- Section 11.3.7, "Validating the Oracle Virtual Directory Changelog"

11.3.1 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.

11.3.2 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.

11.3.3 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 11–1.
- 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.

11.3.4 Directory Structure Overview - Shadow Join

Figure 11–1 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 11–1 Directory Structure

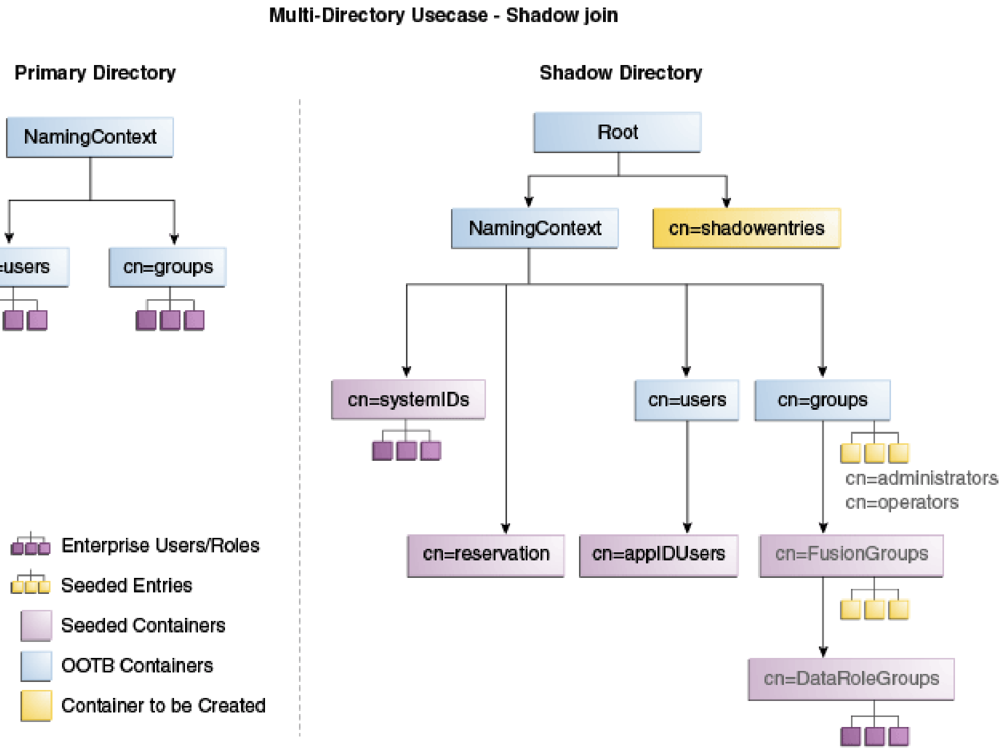


Figure 11–2 shows how the DIT appears to a user or client application. The containers `cn=appIDUsers`, `cn=FusionGroups`, and `cn=DataRoleGroups` are speciric to Fusion Applications.

Figure 11–2 Client View of the DIT

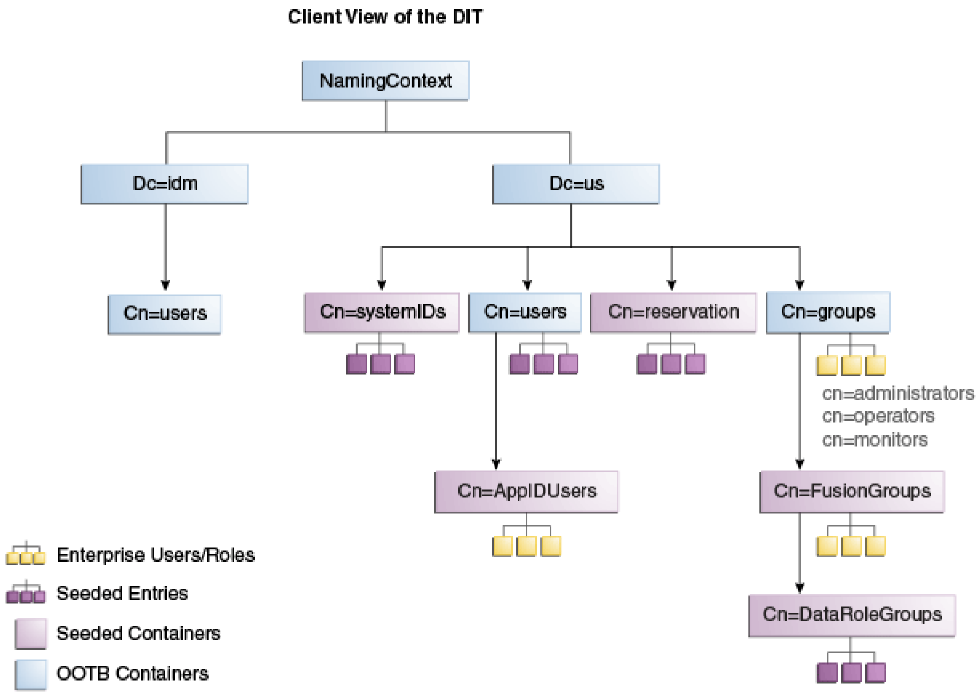
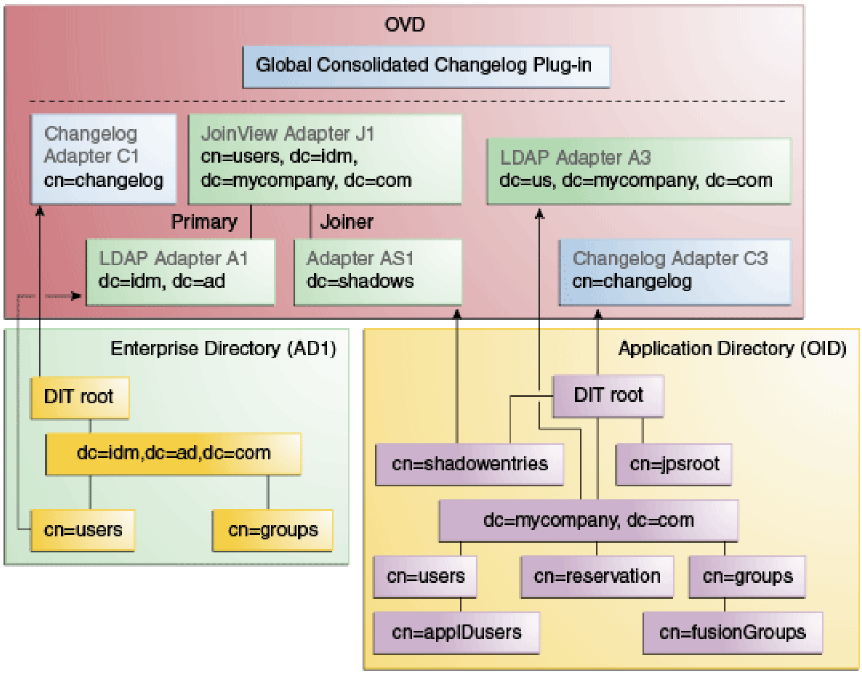


Figure 11–3 summarizes the adapters and plug-ins. The containers `cn=appIDUsers`, and `cn=FusionGroups` are speciric to Fusion Applications.

Figure 11–3 Adapter and Plug-in Configuration



11.3.5 Configuring Oracle Virtual Directory Adapters for Split Profile

In order to produce the client side view of the data shown in Figure 11–2, 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 B.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.

11.3.6 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**.

11.3.7 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.

11.4 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,

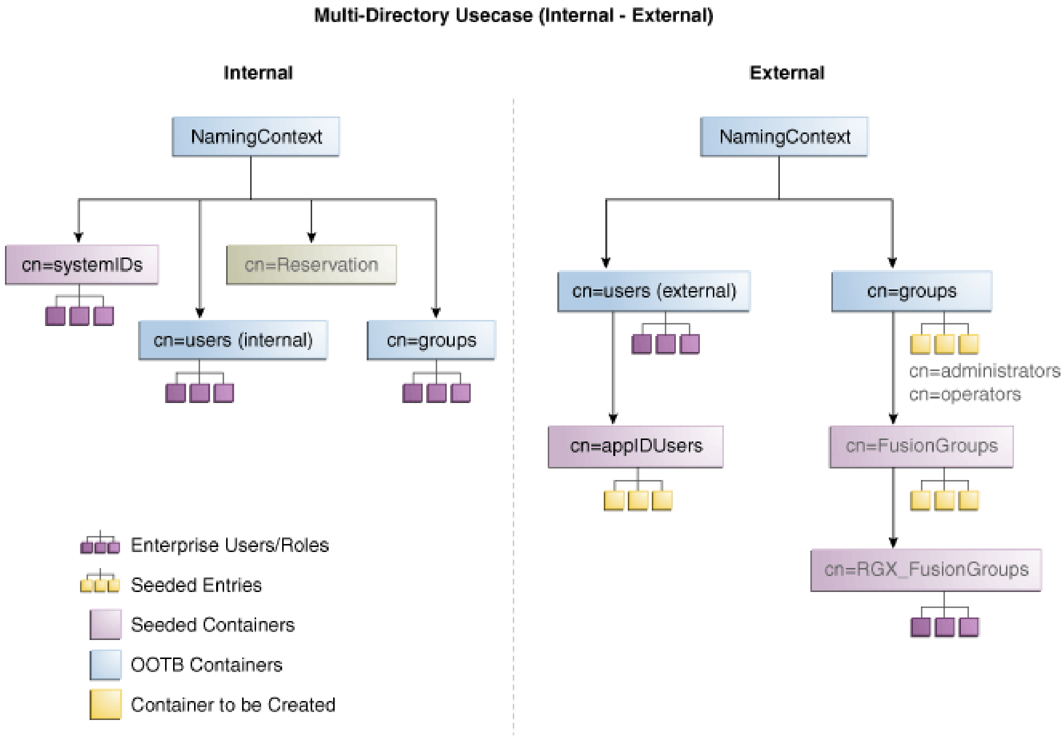
This section contains the following topics:

- Section 11.4.1, "Directory Structure Overview for Distinct User and Group Populations in Multiple Directories"
- Section 11.4.2, "Configuring Oracle Virtual Directory Adapters for Distinct User and Group Populations in Multiple Directories"
- Section 11.4.3, "Creating a Global Plug-in"

11.4.1 Directory Structure Overview for Distinct User and Group Populations in Multiple Directories

Figure 11–4 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 11–4 Directory Structure



Oracle Virtual Directory makes multiple directories look like a single DIT to a user or client application, as shown in Figure 11–5. The containers cn=appIDUsers, cn=FusionGroups, and cn=RGX_FusionGroups are Fusion Applications-specific.

Figure 11–5 Client View of the DIT

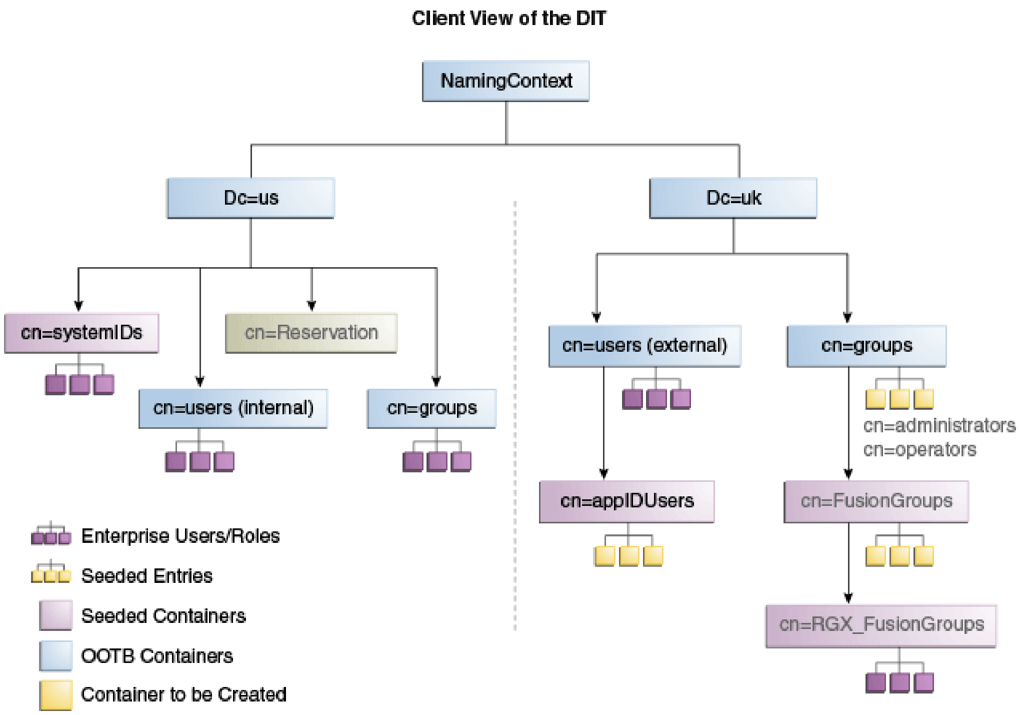
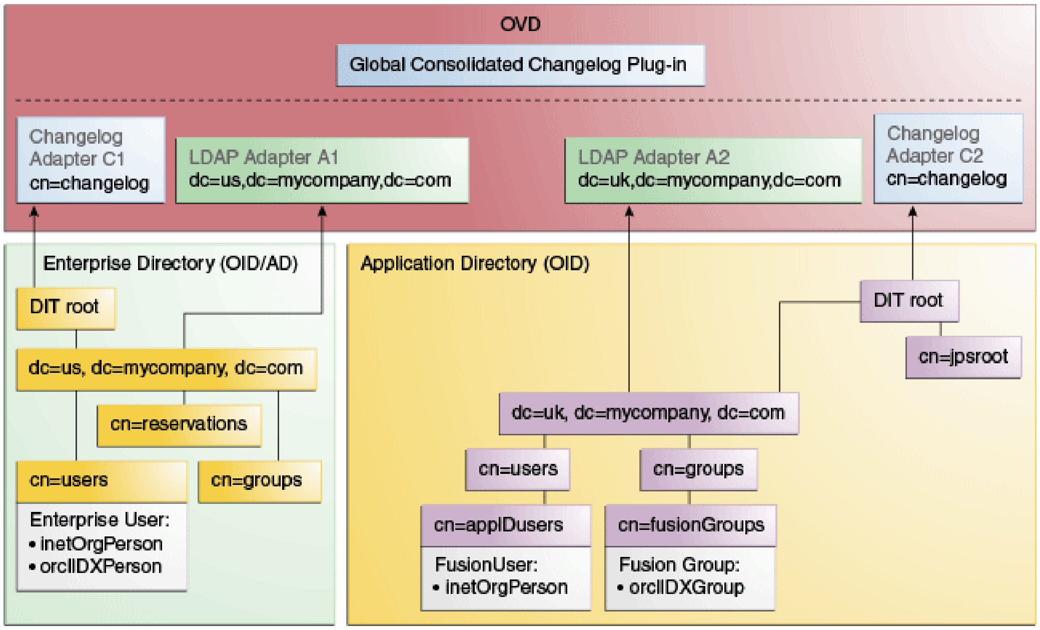


Figure 11–6 provides an overview of the adapter configuration. The classes `inetOrgPerson`, `orclIDXPerson`, and `orclIDXGroup` and the containers `cn=appIDusers` and `cn=fusionGroups` are required only for Fusion Applications.

Figure 11–6 Configuration Overview


OVD
Global Consolidated Changelog Plug-in
Changelog Adapter C1 cn=changelog
LDAP Adapter A1 dc=us,dc=mycompany,dc=com
LDAP Adapter A2 dc=uk,dc=mycompany,dc=com
Changelog Adapter C2 cn=changelog
Enterprise Directory (OID/AD)
DIT root
dc=us, dc=mycompany, dc=com
cn=reservations
cn=users
cn=groups
Enterprise User:
• inetOrgPerson
• orclIDXPerson
Application Directory (OID)
DIT root
cn=jpsroot
dc=uk, dc=mycompany, dc=com
cn=users
cn=groups
cn=appIDusers
cn=fusionGroups
FusionUser:
• inetOrgPerson
Fusion Group:
• orclIDXGroup

11.4.2 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

11.4.2.1 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 B.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.us.oracle.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.us.oracle.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.

11.4.2.2 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.us.oracle.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.

11.4.3 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.

11.5 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.

A

Using the idmConfigTool Command

The idmConfigTool is located at:

IAM_ORACLE_HOME/idmtools/bin

You use the idmConfigTool to automate the following tasks:

- Preconfiguring the Identity Store components (Oracle Internet Directory and Oracle Virtual Directory) for installing the other Identity Management components, including Oracle Access Manager and Oracle Identity Manager
- Postconfiguring the Identity Store components Oracle Access Manager, Oracle Identity Manager and wiring of Oracle Access Manager and Oracle Identity Manager
- Extracting the configuration of the Identity Management components Oracle Internet Directory, Oracle Virtual Directory, Oracle Access Manager and Oracle Identity Manager
- Validating the configuration parameters representing the Identity Management components Oracle Internet Directory, Oracle Virtual Directory, Oracle Access Manager and Oracle Identity Manager.

A.1 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		Configure the Identity Store and Policy store by creating the groups and setting ACIs to the various containers.
prepareIDStore		Configure the identity store by adding necessary users and associating users with groups. Modes are available to enable you to configure for a specific component.

Command	Component name	Description
configPolicyStore		Configures policy store by creating read-write user and associates them to the groups.
configOAM		Prepares Oracle Access Manager for integration with Oracle Identity Manager.
configOIM		Sets up wiring between Oracle Access Manager and Oracle Identity Manager.
validate	IDSTORE POLICYSTORE OAM10g OIM	Validates the set of input parameters.

The `validate` command requires a component name.

You must run this tool as a user with `orcladmin` privileges on Oracle Internet Directory.

A.2 Parameters

The following sections list the parameters for the commands.

A.2.1 preConfigIDStore

Parameter	Value
IDSTORE_HOST	identity store hostname, for example mynode.us.mycompany.com
IDSTORE_PORT	identity store port, for example 1234
IDSTORE_BINDDN	cn:orcladmin
IDSTORE_USERNAMEATTRIBUTE	cn
IDSTORE_USERSEARCHBASE	cn:Users, dc:test
IDSTORE_GROUPSEARCHBASE	cn:Groups, dc:test
IDSTORE_SEARCHBASE	dc:test
IDSTORE_SYSTEMIDBASE	cn:system, dc:test
IDSTORE_READONLYUSER	readOnlyUser
IDSTORE_READWRITEUSER	readWriteUser
IDSTORE_SUPERUSER	FAAdmin
IDSTORE_OAMSOFTWAREUSER	oamSoftwareUser
IDSTORE_OAMADMINUSER	oamAdminUser
IDSTORE_OIMADMINUSER	oimAdminUser
IDSTORE_OIMADMINGROUP	oimAdminGroup
POLICYSTORE_SHARES_IDSTORE	true

A.2.2 prepareIDStore Parameters

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

```
prepareIDStore mode=mode
input_file=filename_with_ConfigParameters
```

where mode must be one of:

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

prepareIDStore mode=fusion

The following are created 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

Table A–1 prepareIDStore mode=fusion Parameters

Parameter	Value
IDSTORE_HOST	identity store hostname
IDSTORE_PORT	identity store port
IDSTORE_BINDDN	cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE	cn
IDSTORE_LOGINATTRIBUTE	uid
IDSTORE_USERSEARCHBASE	cn=Users, dc=us,dc=oracle,dc=com
IDSTORE_GROUPSEARCHBASE	cn=Groups, dc=us,dc=oracle,dc=com
IDSTORE_SEARCHBASE	dc=us,dc=oracle,dc=com
IDSTORE_READONLYUSER	readOnlyUser
IDSTORE_READWRITEUSER	readWriteUser
IDSTORE_SUPERUSER	superUser

prepareIDStore mode=OAM

The following are created in this mode:

- Perform schema extensions as required by the OAM component
- Add the oblix schema
- Create the OAMSoftware User
- Create OblixAnonymous User
- Optionally create the OAM Admin User
- Associate these users to their respective groups
- Create the group "orclFAOAMUserWritePrivilegeGroup"

Table A–2 prepareIDStore mode=OAM Parameters

Parameter	Value
IDSTORE_HOST	identity store hostname
IDSTORE_PORT	identity store port
IDSTORE_BINDDN	cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE	cn
IDSTORE_LOGINATTRIBUTE	uid
IDSTORE_USERSEARCHBASE	cn=Users, dc=us,dc=oracle,dc=com
IDSTORE_GROUPSEARCHBASE	cn=Groups, dc=us,dc=oracle,dc=com
IDSTORE_SEARCHBASE	dc=us,dc=oracle,dc=com
IDSTORE_OAMSOFTWAREUSER	oamSoftwareUser
IDSTORE_OAMADMINUSER	oamAdminUser

prepareIDStore mode=OIM

The following are created in this mode:

- Create OIM Admin User under SystemID container
- Create OIM Admin Group
- Add OIM Admin User to OIM Admin Group
- Add ACIs to OIM Admin Group
- Create reserve container
- Create xelsysadmin user

Table A–3 prepareIDStore mode=OIM Parameters

Parameter	Value
IDSTORE_HOST	identity store hostname
IDSTORE_PORT	identity store port
IDSTORE_BINDDN	cn=orcladmin

Table A–3 (Cont.) prepareIDStore mode=OIM Parameters

Parameter	Value
IDSTORE_ USERNAMEATTRIBUTE	cn
IDSTORE_ LOGINATTRIBUTE	uid
IDSTORE_ USERSEARCHBASE	cn=Users, dc=us,dc=oracle,dc=com
IDSTORE_ GROUPSEARCHBASE	cn=Groups, dc=us,dc=oracle,dc=com
IDSTORE_SEARCHBASE	dc=us,dc=oracle,dc=com
IDSTORE_ OIMADMINUSER	oimAdminUser
IDSTORE_ OIMADMINGROUP	oimAdminGroup
IDSTORE_SYSTEMIDBASE	cn=system,dc=us,dc=oracle,dc=com

prepareIDStore mode=OAAM

The following are created in this mode:

- Create OAAM Admin User
- Create OAAM Groups
- Add the OAAM Admin User as a member of OAAM Groups

Table A–4 prepareIDStore mode=OAAM Parameters

Parameter	Value
IDSTORE_HOST	identity store hostname
IDSTORE_PORT	identity store port
IDSTORE_BINDDN	cn=orcladmin
IDSTORE_ USERNAMEATTRIBUTE	cn
IDSTORE_ LOGINATTRIBUTE	uid
IDSTORE_ USERSEARCHBASE	cn=Users, dc=us,dc=oracle,dc=com
IDSTORE_ GROUPSEARCHBASE	cn=Groups, dc=us,dc=oracle,dc=com
IDSTORE_SEARCHBASE	dc=us,dc=oracle,dc=com

prepareIDStore mode=WLS

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

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

Table A–5 prepareIDStore mode=WLS Parameters

Parameter	Value
IDSTORE_HOST	identity store hostname
IDSTORE_PORT	identity store port
IDSTORE_BINDDN	cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE	cn
IDSTORE_LOGINATTRIBUTE	uid
IDSTORE_USERSEARCHBASE	cn=Users, dc=us,dc=oracle,dc=com
IDSTORE_GROUPSEARCHBASE	cn=Groups, dc=us,dc=oracle,dc=com
IDSTORE_SEARCHBASE	dc=us,dc=oracle,dc=com

prepareIDStore mode=all

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

Table A–6 prepareIDStore mode=WLS Parameters

Parameter	Value
IDSTORE_HOST	identity store hostname
IDSTORE_PORT	identity store port
IDSTORE_BINDDN	cn=orcladmin
IDSTORE_USERSEARCHBASE	cn=Users, dc=us,dc=oracle,dc=com
IDSTORE_GROUPSEARCHBASE	cn=Groups, dc=us,dc=oracle,dc=com
IDSTORE_SEARCHBASE	dc=us,dc=oracle,dc=com
IDSTORE_SYSTEMIDBASE	cn=system,dc=us,dc=oracle,dc=test
IDSTORE_READONLYUSER	readOnlyUser
IDSTORE_READWRITEUSER	readWriteUser
IDSTORE_SUPERUSER	superUser
IDSTORE_OAMSOFTWAREUSER	oamSoftwareUser
IDSTORE_OAMADMINUSER	oamAdminUser
IDSTORE_OIMADMINUSER	oimAdminUser
IDSTORE_OIMADMINGROUP	oimAdminGroup

A.2.3 configPolicyStore Parameters

Parameter	Value
POLICYSTORE_HOST	policy store hostname, for example mynode.us.mycompany.com
POLICYSTORE_PORT	policy store port, for example 1234
POLICYSTORE_BINDDN	cn:orcladmin
POLICYSTORE_SEARCHBASE	dc:test
POLICYSTORE_READONLYUSER	PolStoreROUser
POLICYSTORE_READWRITEUSER	PolStoreRWUser
POLICYSTORE_CONTAINER	cn:jpsroot

A.2.4 configOAM Parameters

Parameter	Value
IDSTORE_HOST	identity store hostname, for example mynode.us.mycompany.com
IDSTORE_PORT	identity store port, for example 1234
POLICYSTORE_HOST	policy store hostname, for example abc
POLICYSTORE_PORT	policy store port, for example 1110
POLICYSTORE_OAMDN	cn:oamsoftware,cn:users,dc:us,dc:oracle,dc:com
POLICYSTORE_PWD	password
OAM_POLICYSEARCHBASE	(required only for non-OID directory)
OAM_POLICYSEARCHBASE	dc:us,dc:oracle,dc:com
OAM_WEBGATE_URL	WebGate URL, for example http://mynode.us.mycompany.com:1010
OAM_CONSENTFORM_URL	/cgi-bin/consentredirect.pl
OAM_IMPERSONATION_PATH	impersonation path, for example /mydir/lib/authz_impersonate.so
OIM_OHS_URL	OHS URL, for example http://mynode.us.mycompany.com:1234
App_agent_password	*password*
Oam_aaa_mode	open
Oam_aaa_passphrase	*password*
Primary_oam_servers	ACCSERVEROAS
MAX_OAM_CONNECTIONS	4

A.2.5 configOIM Parameters

Parameter	Value
ACCESS_SERVER_HOST	Access Server hostname, for example mynode.us.mycompany.com

Parameter	Value
ACCESS_GATE_ID	IdentityManagerAccessGate
ACCESS_SERVER_PORT	5575
COOKIE_DOMAIN	.us.oracle.com
COOKIE_EXPIRY_INTERVAL	120
WEBGATE_TYPE	javaWebgate | ohsWebgate10g | ohsWebgate11g
SSO_ENABLED_FLAG	true | false
IDSTORE_PORT	
IDSTORE_HOST	
IDSTORE_ADMIN_USER	
IDSTORE_USERSEARCHBASE	
IDSTORE_GROUPSEARCHBASE	
MDS_DB_URL	
MDS_DB_URL	
MDS_DB_SCHEMA_USERNAME	
WLSHOST	
WLSPORT	
WLSADMIN	
DOMAIN_NAME	
OIM_MANAGED_SERVER_NAME	
DOMAIN_LOCATION	
OIM_MANAGED_SERVER_HOST	
OIM_MANAGED_SERVER_PORT	

A.2.6 postProv Parameters

Same as preConfigIDStore parameters.

A.2.7 Validate IDStore parameters

Parameter	Value
IDSTORE_TYPE	OID | OVD
IDSTORE_HOST	adcxyx
IDSTORE_PORT	3060
IDSTORE_SSLPORT	3031
IDSTORE_SSL_ENABLED	true
IDSTORE_SUPER_USER	faadmin
IDSTORE_READ_WRITE_USER	cn=rou,cn=users,dc=mycompany,dc=com
IDSTORE_READ_WRITE_PASSWORD	*password*

Parameter	Value
IDSTORE_READ_ONLY_USER	cn=rwu,cn=users,dc=mycompany,dc=com
IDSTORE_READ_ONLY_PASSWORD	*password*
IDSTORE_USER_CONTAINER	cn=users,dc=mycompany,dc=com
IDSTORE_GROUP_CONTAINER	cn=users,dc=mycompany,dc=com
IDSTORE_SEEDING	true
IDSTORE_ADMIN_GROUP	cn=administrators,cn=groups,dc=mycompany,dc=com
IDSTORE_ADMIN_GROUP_EXISTS	true

A.2.8 PolicyStore parameters

Parameter	Value
POLICYSTORE_HOST	POLICYSTORE.host
POLICYSTORE_PORT	POLICYSTORE.port
POLICYSTORE_SECURE_PORT	POLICYSTORE.sslport
POLICYSTORE_IS_SSL_ENABLED	POLICYSTORE.ssl.enabled
POLICYSTORE_READ_WRITE_USERNAME	POLICYSTORE.username
POLICYSTORE_PASSWORD	POLICYSTORE.password
POLICYSTORE_SEEDING	POLICYSTORE.seeding
POLICYSTORE_JPS_ROOT_NODE	POLICYSTORE.jps.root
POLICYSTORE_DOMAIN_NAME	POLICYSTORE.domain.name
POLICYSTORE_CREATED_BY_CUSTOMER	POLICYSTORE.created.by.customer
POLICYSTORE_JPS_CONFIG_DIR	idm.jpsconfig.filesdir
POLICYSTORE_CRED_MAPPING_FILE_LOCATION	idm.credentials.mapping.filelocation
POLICYSTORE_ADF_CRED_FILE_LOCATION	idm.common.adfcreds.file
POLICYSTORE_STRIPE_FSCM	fscm
POLICYSTORE_STRIPE_CRM	crm
POLICYSTORE_STRIPE_HCM	hcm
POLICYSTORE_STRIPE_SOA_INFRA	soa-infra
POLICYSTORE_STRIPE_APM	oracle.security.apm
POLICYSTORE_STRIPE_ESSAPP	ESSAPP
POLICYSTORE_STRIPE_B2BUI	b2bui
POLICYSTORE_STRIPE_OBI	obi
POLICYSTORE_STRIPE_WEBCENTER	webcenter
POLICYSTORE_STRIPE_IDCCS	IDCCS
POLICYSTORE_CRED_STORE	POLICYSTORE.credential.store
IDM_KEYSTORE_FILE	idm.keystore.file

Parameter	Value
IDM_KEYSTORE_PASSWORD	idm.keystore.password

A.2.9 Validate OAM Configuration

Parameter	Value	Notes
OAM10g_MODE		
OAM10g_NOPROMPT		Query for password is suppressed when true.
OAM10g_POLICY_HOST		
OAM10g_POLICY_PORT		
OAM10g_POLICY_USERDN	ldap_userdn	
OAM10g_POLICY_USERPWD	ldap_userpassword	
OAM10g_AAA_MODE	oam_aaa_mode	
OAM10g_AAA_PASSPHRASE	oam_aaa_passphrase	
OAM10g_PRIMARY_SERVERS	primary_oam_servers	
OAM10g_SECONDARY_SERVERS	secondary_oam_servers	
OAM10g_RUNTIME_USER	oam_runtime_user	User used to configure Oracle Access Manager 10*g* components. This user has read/write privileges to the Oracle Access Manager Policy store, for example: cn=OAMSoftware

A.2.10 Validate OIM

Parameter	Value	Notes
ADMIN_SERVER_HOST	admin_server_host	Domain Admin Server Constant
ADMIN_SERVER_PORT	admin_server_port	Domain Admin Server Constant
ADMIN_SERVER_USER	admin_server_user	Domain Admin Server Constant
ADMIN_SERVER_USER_PASSWORD	admin_server_user_password	Domain Admin Server Constant
ACCESS_SERVER_HOST		
ACCESS_SERVER_PORT		
ACCESS_SERVER_ID		

A.3 Examples

The following reference contains examples of idmConfigTool usage:

- "Integrating Oracle Access Manager and Oracle Identity Manager" in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.

B

Verifying Adapters for Multiple Directory Identity Stores by Using ODSM

After you have configured your Oracle Virtual Directory adapters as described in Chapter 11, "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 B.1, "Verifying Oracle Virtual Directory Adapters for Split Profile by Using ODSM"
- Section B.2, "Verifying Adapters for Distinct User and Group Populations in Multiple Directories by Using ODSM"

B.1 Verifying Oracle Virtual Directory Adapters for Split Profile by Using ODSM

This section describes how to validate the adapters created in Chapter 11.3.5, "Configuring Oracle Virtual Directory Adapters for Split Profile."

This section contains the following topics:

- Section B.1.1, "Verifying User Adapter for Active Directory Server"
- Section B.1.2, "Verifying Shadowjoiner User Adapter"
- Section B.1.3, "Verifying JoinView Adapter"
- Section B.1.4, "Verifying User/Role Adapter for Oracle Internet Directory"
- Section B.1.5, "Verifying Changelog adapter for Active Directory Server"
- Section B.1.6, "Verifying Changelog Adapter for Oracle Internet Directory"
- Section B.1.7, "Configuring a Global Consolidated Changelog Plug-in"
- Section B.1.8, "Validate Oracle Virtual Directory Changelog"

B.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.

B.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'	

B.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**.

B.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**.

B.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

B.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)

B.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.

B.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.

B.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 11.4.2, "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 B.2.1, "User/Role Adapter A1"
- Section B.2.2, "User/Role Adapter A2"

- Section B.2.3, "Changelog Adapter C1"
- Section B.2.4, "Changelog Adapter for Active Directory"
- Section B.2.5, "Changelog Adapter C2"
- Section B.2.6, "Verifying Oracle Virtual Directory Global Plug-in"
- Section B.2.7, "Configuring a Global Consolidated Changelog Plug-in"

B.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.

B.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.

B.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 B–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

B.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`.

B.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 B–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 B–2 (Cont.) Values in Parameters Table

Parameter	Value	Comments
virtualDITAdapterName	The adapter name of User/Role adapter A2: `User_Adapter_A2`	Create

B.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.

B.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.

Index