

Oracle® Fusion Middleware

Integration Overview for Oracle Identity Management Suite

11g Release 1 (11.1.1)

E15477-02

June 2011

E15477-02

Copyright © 2010, 2011, Oracle and/or its affiliates. All rights reserved.

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

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	vii
Audience	vii
Documentation Accessibility	vii
Related Documents	viii
Conventions	viii
What's New in Security Integration	ix
New Features in 11g Release 1 (11.1.1.5.0)	ix
1 Introduction	
1.1 About Oracle Identity Management	1-1
1.2 Objectives of Integration	1-1
1.3 Types of Integration	1-2
1.3.1 Integration Among Oracle Identity Management Components	1-2
1.3.2 Integration for other Oracle products	1-2
1.3.3 Integration for Third-Party products	1-3
1.4 Key Integration Scenarios	1-3
1.5 How to Use this Book	1-4
2 Web Access Management	
2.1 Oracle Access Manager for Oracle Identity Management	2-1
2.2 Oracle Access Manager for Oracle Fusion Middleware	2-2
2.3 Oracle Access Manager for Other Oracle Applications	2-3
2.4 Oracle Access Manager for Third-Party Applications	2-3
3 Enterprise Single Sign-On	
3.1 Enterprise Single Sign-On Logon Manager	3-1
3.2 Enterprise Single Sign-On Synchronization	3-1
3.3 Enterprise Single Sign-On Provisioning Gateway	3-2
3.4 Enterprise Single Sign-On Authentication Manager	3-2
3.5 Enterprise Single Sign-On Universal Authentication Manager	3-3
4 Federation	
4.1 Oracle Identity Federation for Oracle Identity Management	4-1

4.2	Oracle Identity Federation for Oracle Fusion Middleware	4-1
4.3	Oracle Identity Federation Authentication Engines	4-2
4.4	Oracle Identity Federation Service Provider Integration Modules	4-2
5	Risk Management	
5.1	Oracle Adaptive Access Manager for Oracle Identity Management	5-1
5.2	Oracle Adaptive Access Manager for Custom Applications.....	5-2
6	User, Account, and Entitlement Provisioning	
6.1	Oracle Identity Manager Connectors for Oracle Identity Management.....	6-1
6.2	Oracle Identity Manager Connectors for Databases	6-1
6.3	Oracle Identity Manager Connectors for Oracle Applications.....	6-2
6.4	Oracle Identity Manager Connectors for Third-Party Applications	6-3
7	Identity Governance	
7.1	Oracle Identity Analytics for Oracle Identity Management	7-1
7.2	Oracle Identity Analytics for Third-Party Products	7-2
8	Password Management	
8.1	Oracle Identity Manager Password Management Support for Oracle Identity Management	8-1
8.2	Oracle Identity Manager Password Management through Connectors.....	8-1
8.3	Oracle Enterprise Single Sign-On Suite ESSO-PR for Password Reset.....	8-2
9	Database Security	
9.1	Oracle Database Net Services LDAP Naming	9-1
9.2	Oracle Database Enterprise User Security with LDAP	9-2
10	Fine-Grained Access Control	
10.1	Oracle Entitlements Server for Oracle Identity Management.....	10-1
10.2	Oracle Entitlements Server for Oracle Fusion Middleware and Oracle SOA.....	10-2
10.3	Oracle Entitlements Server for Third-Party products	10-3
A	Using the idmConfigTool Command	
A.1	Syntax	A-1
A.2	Parameters.....	A-2
A.2.1	preConfigIDStore	A-2
A.2.2	prepareIDStore Parameters	A-3
A.2.3	configPolicyStore Parameters	A-7
A.2.4	configOAM Parameters	A-7
A.2.5	configOIM Parameters	A-7
A.2.6	postProv Parameters	A-8
A.2.7	Validate IDStore parameters.....	A-8
A.2.8	PolicyStore parameters	A-9
A.2.9	Validate OAM Configuration	A-10

A.2.10	Validate OIM	A-10
A.3	Examples	A-10

Index

Preface

This document describes the Identity Management integration options in Oracle Fusion Middleware 11g 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 11g 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

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/support/contact.html> or visit <http://www.oracle.com/accessibility/support.html> if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Fusion Middleware 11g 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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New 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](#).

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 11g 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.

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 <i>Oracle Fusion Middleware Integration Guide for Oracle Access Manager</i>
Oracle Adaptive Access Manager	Integrating Oracle Access Manager and Oracle Adaptive Access Manager in the <i>Oracle Fusion Middleware Integration Guide for Oracle Access Manager</i>
	Configuring OAM and OAAM with Other Oracle Identity Management Products in the <i>Oracle Fusion Middleware Installation Guide for Oracle Identity Management</i>

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 <i>Oracle Fusion Middleware Integration Guide for Oracle Access Manager</i>
Oracle Identity Federation	Chapter 4, "Federation"
Oracle Security Token Service	About Oracle Security Token Service with Oracle Access Manager in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service</i>

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 11g	Configuring Oracle Access Manager (OAM) in the <i>Oracle Fusion Middleware Installation Guide for Oracle Identity Management</i> Registering Partners (Agents and Applications) Remotely in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager</i> .
Oracle HTTP Server 11g	Configuring Oracle Access Manager (OAM) in the <i>Oracle Fusion Middleware Installation Guide for Oracle Identity Management</i> Registering Partners (Agents and Applications) Remotely in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager</i> .
Oracle HTTP Server 10g	Platform-specific Oracle Application Server Installation Guide for 10g. 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 <i>Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service</i> Typical Deployment Topology and Processing for Identity Propagation in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service</i>
Oracle Application Server 10g	Platform-specific Oracle Application Server Installation Guide for 10g. Integrating with Oracle Application Servers in the Oracle Access Manager Integration Guide for 10g

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 <i>Oracle Fusion Middleware Application Security Guide</i> . Introduction to the OAM Policy Model, Single Sign-On, and Sign-Off in <i>Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager</i> . <i>Oracle Fusion Middleware Integration Guide for Oracle Access Manager</i>

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 <i>Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager</i>
SAP mySAP	
IBM Lotus Domino	Configuring Lotus Domino Web Servers for 10g WebGates in <i>Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager</i>
IBM HTTP Server	Configuring 10g WebGates for Apache v2-based Web Servers (OHS and IHS) in <i>Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager</i>
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 <i>Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager</i>
Microsoft Internet and Security Acceleration Server (ISA)	Configuring 10g WebGates for the ISA Server in <i>Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager</i>
Windows Native Authentication	Configuring Oracle Access Manager to use Windows Native Authentication in the <i>Oracle Fusion Middleware Integration Guide for Oracle Access Manager</i>

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-LM Global 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).

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 <i>Integrating Oracle Access Manager with Oracle Identity Federation in the Oracle Fusion Middleware Integration Guide for Oracle Access Manager</i> For 10g webgates, see <i>Oracle Access Manager in the Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>
Oracle Single Sign-On 10g	See <i>Oracle Single Sign-On in the Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>

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 <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>
Oracle HTTP Server to set up proxy for Oracle Identity Federation	Setting Up a Proxy for Oracle Identity Federation in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>

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 <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>
Oracle Single Sign-On 10g	Authentication Engines - Oracle Single Sign-On in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>
LDAP Directory	Authentication Engines - LDAP Directory in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>
Database Security	Authentication Engines - Database Security in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>
Database Table	Authentication Engines - Database Table in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>
Microsoft Windows CardSpace (InfoCard)	Authentication Engines - Infocard in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>
JAAS	Authentication Engines - JAAS in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>
Custom authentication engine	Authentication Engines - Custom in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>

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 <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>
Oracle Single Sign-On 10g	SP Integration module - Oracle Single Sign-On in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>
Custom SP Integration Module for third-party IAM system	SP Integration Module - Custom in the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation</i>

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 <i>Oracle Fusion Middleware Integration Guide for Oracle Access Manager</i>
Oracle Identity Manager for password flow	Deployment Options for Password Management in the <i>Oracle Fusion Middleware Integration Guide for Oracle Access Manager</i>
Oracle Internet Directory as an authentication provider	Oracle Identity Management Suite-Level Installation Scenarios in the <i>Oracle Fusion Middleware Installation Guide for Oracle Identity Management</i>
Oracle Virtual Directory as an authentication provider	Oracle Identity Management Suite-Level Installation Scenarios in the <i>Oracle Fusion Middleware Installation Guide for Oracle Identity Management</i>

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 <i>Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager</i>
using Java API	Integrating Native Java Applications in the <i>Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager</i>
using OAAM Proxy for Internet and Security Acceleration Server (ISA)	Installing Oracle Adaptive Access Manager Proxy for Microsoft ISA in the <i>Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager</i>
using OAAM Proxy for Apache	Installing Oracle Adaptive Access Manager Proxy for Apache in the <i>Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager</i>

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 <i>Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager</i> .
Custom Connector with Generic Technology Connectors	Creating and Managing Generic Technology Connectors in the <i>Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager</i>

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 <i>Sun Role Manager 5.0.3 System Integrator's Guide</i> at: http://wikis.sun.com/display/Srm503Docs/System+Integrator%27s+Guide
Oracle WaveSet	Integrating with Sun Identity Manager in the <i>Sun Role Manager 5.0.3 System Integrator's Guide</i> 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 <i>Sun Role Manager 5.0.3 System Integrator's Guide</i> at: http://wikis.sun.com/display/Srm503Docs/System+Integrator%27s+Guide
using ETL process	Role Manager ETL Process in the <i>Sun Role Manager 5.0.3 Business Administrator's Guide</i> at: http://wikis.sun.com/display/Srm503Docs/Business+Administrator%27s+Guide

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 <i>Oracle Fusion Middleware Integration Guide for Oracle Access Manager</i> .
Oracle Adaptive Access Manager	Deployment Options for Password Management in the <i>Oracle Fusion Middleware Integration Guide for Oracle Access Manager</i> .
Oracle Access Manager and Oracle Adaptive Access Manager combined	Deployment Options for Password Management in the <i>Oracle Fusion Middleware Integration Guide for Oracle Access Manager</i> .

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.

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 <i>Oracle Database Net Services Administrator's Guide</i> . Using a Directory Server for Centralized Management in the <i>Oracle Database Net Services Administrator's Guide</i> .
Directory Naming with Oracle Virtual Directory	
Directory Naming with Microsoft Active Directory using Oracle Virtual Directory	Managing Network Address Information in the <i>Oracle Database Net Services Administrator's Guide</i> . Using a Directory Server for Centralized Management in the <i>Oracle Database Net Services Administrator's Guide</i> .
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

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	<ul style="list-style-type: none"> ■ 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)	<ul style="list-style-type: none"> ■ 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

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

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	ACCSEVEROAS
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 10g 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*.

Index

A

- AD Password Synchronization
 - Oracle Identity Manager Connector, 6-4
- AD User Management
 - Oracle Identity Manager Connector, 6-3
- Adapter Factory
 - Oracle Identity Manager Connector, 6-5
- Apache proxy
 - Oracle Adaptive Access Manager, 5-2
- Apache Webservers
 - and Oracle Access Manager, 2-3

B

- BMC Remedy Ticket Management
 - Oracle Identity Manager Connector, 6-3
- BMC Remedy User Management
 - Oracle Identity Manager Connector, 6-3

C

- CA ACF2 Advanced
 - Oracle Identity Manager Connector, 6-3
- CA Top Secret Advanced
 - Oracle Identity Manager Connector, 6-3

D

- Database Application Tables
 - Oracle Identity Manager Connector, 6-2, 6-3
- database security, 1-4
- Database User Management
 - Oracle Identity Manager Connector, 6-2, 6-3
- Databases
 - and ESSO Synchronization Manager, 3-2
 - Oracle Identity Manager Connectors, 6-1
- Directory Naming with LDAP
 - Oracle Database Net Services, 9-1

E

- Enterprise Single Sign-On, 1-3
 - Authentication Manager, 3-2
 - ESSO Synchronization, 3-1
 - Logon Manager, 3-1
 - Provisioning Gateway, 3-2

- Universal Authentication Manager, 3-3
- Enterprise Single Sign-On Logon Manager, 3-1
- Enterprise User Security
 - for Microsoft Active Directory using Oracle Virtual Directory, 9-2
 - for Oracle Internet Directory, 9-2
 - with Oracle Directory Service Enterprise Edition using Oracle Virtual Directory, 9-2
- Entrust
 - and ESSO Authentication Manager, 3-3
- ESSO Authentication Manager
 - and Entrust, 3-3
 - and LDAP directories, 3-3
 - and Microsoft Windows, 3-3
 - and Proximity cards, 3-3
 - and RSA SecurID, 3-3
 - and smart cards, 3-3
- ESSO Provisioning Gateway, 3-2
 - and IBM Tivoli Identity Manager, 3-2
 - and Novell Identity Manager, 3-2
 - and Oracle Identity Manager, 3-2
 - and Oracle Waveset, 3-2
- ESSO Synchronization Manager
 - and Databases, 3-2
 - and LDAP directories, 3-2
 - and Microsoft Active Directory, 3-2
 - and Microsoft ADAM, 3-2
- ESSO Universal Authentication Manager, 3-3
- ESSO-PR
 - for password reset, 8-2
- ETL process
 - and Oracle Identity Analytics, 7-2

F

- Federation, 1-3

G

- Generic Technology Connectors
 - Oracle Identity Manager, 6-5
- governance, risk, and compliance, 1-4

I

- IBM HTTP Server

- and Oracle Access Manager, 2-3
- IBM Lotus Domino
 - and Oracle Access Manager, 2-3
- IBM Lotus Notes and Domino
 - Oracle Identity Manager Connector, 6-3
- IBM OS/400 Advanced
 - Oracle Identity Manager Connector, 6-3
- IBM RACF Advanced
 - Oracle Identity Manager Connector, 6-3
- IBM RACF Standard
 - Oracle Identity Manager Connector, 6-3
- IBM Tivoli Identity Manager
 - and ESSO Provisioning Gateway, 3-2
- Identity Governance, 7-1
- ISA proxy
 - Oracle Adaptive Access Manager, 5-2

J

- Java API
 - Oracle Adaptive Access Manager, 5-2
- JD Edwards EnterpriseOne User Management
 - Oracle Identity Manager Connector, 6-2

K

- Key Integration Scenarios, 1-3

L

- LDAP
 - Oracle Database Enterprise User Security, 9-2
- LDAP directories
 - and ESSO Authentication Manager, 3-3
 - and ESSO Synchronization Manager, 3-2

M

- Microsoft Active Directory
 - and ESSO Synchronization Manager, 3-2
 - and Oracle Database Net Services for Directory Naming using Oracle Virtual Directory, 9-2
- Microsoft Active Directory 2000 and 2003
 - and Oracle Entitlements Server, 10-3
- Microsoft ADAM
 - and ESSO Synchronization Manager, 3-2
 - and Oracle Entitlements Server, 10-3
- Microsoft Exchange
 - Oracle Identity Manager Connector, 6-4
- Microsoft Internet and Security Acceleration Server
 - and Oracle Access Manager, 2-3
- Microsoft Internet Information Server
 - and Oracle Access Manager, 2-3
- Microsoft .NET Framework 1.1 and 2.05
 - and Oracle Entitlements Server, 10-3
- Microsoft Office SharePoint Server 2007
 - and Oracle Entitlements Server, 10-3
- Microsoft SharePoint Server
 - and Oracle Access Manager, 2-3
- Microsoft Windows
 - and ESSO Authentication Manager, 3-3

- Oracle Identity Manager Connector, 6-4

N

- Novell eDirectory
 - Oracle Identity Manager Connector, 6-4
- Novell eDirectory v8.7.31
 - and Oracle Entitlements Server, 10-3
- Novell GroupWise
 - Oracle Identity Manager Connector, 6-4
- Novell Identity Manager
 - and ESSO Provisioning Gateway, 3-2

O

- Open LDAP v2.2.24
 - and Oracle Entitlements Server, 10-3
- Oracle Access Manager, 2-1
 - and Apache Webservers, 2-3
 - and IBM HTTP Server, 2-3
 - and IBM Lotus Domino, 2-3
 - and Microsoft Internet and Security Acceleration Server, 2-3
 - and Microsoft Internet Information Server, 2-3
 - and Microsoft SharePoint Server, 2-3
 - and Oracle Adaptive Access Manager, 2-1, 5-2
 - and Oracle Application Server 10g, 2-2
 - and Oracle applications, 2-3
 - and Oracle Business Intelligence, 2-2
 - and Oracle E-Business Suite, 2-3
 - and Oracle Entitlements Server, 10-1
 - and Oracle Fusion Middleware, 2-2
 - and Oracle HTTP Server 10g, 2-2
 - and Oracle HTTP Server 11g, 2-2
 - and Oracle Identity Federation, 2-2, 4-1
 - and Oracle Identity Management, 2-1
 - and Oracle Identity Manager, 2-1, 8-1
 - and Oracle Identity Navigator, 2-2
 - and Oracle WebCache, 2-2
 - and Oracle WebLogic Server, 2-2
 - and PeopleSoft Enterprise, 2-3
 - and SAP mySAP, 2-3
 - and Siebel, 2-3
 - and third-party applications, 2-3
 - and Windows Native Authentication, 2-3
- SP Integration with Oracle Identity Federation, 4-3
 - with Oracle Adaptive Access Manager and Oracle Identity Manager, 8-1
- Oracle Access Manager and Oracle Adaptive Access Manager
 - with Oracle Identity Manager, 8-1
- Oracle Access Manager and Oracle Identity Manager
 - with Oracle Adaptive Access Manager, 8-1
- Oracle Adaptive Access Manager, 5-1
 - and Oracle Access Manager, 2-1, 5-2
 - and Oracle Entitlements Server, 10-1
 - and Oracle Identity Management, 5-1
 - and Oracle Identity Manager, 5-2, 8-1
 - and Oracle Internet Directory, 5-2

- and Oracle Virtual Directory, 5-2
- and risk management for applications, 5-2
- Java API, 5-2
- proxy for Apache, 5-2
- proxy for ISA, 5-2
- Web Services and SOAP API, 5-2
- with Oracle Access Manager and Oracle Identity Manager, 8-1
- Oracle Adaptive Access Manager and Oracle Identity Manager
 - with Oracle Access Manager, 8-1
- Oracle Application Server 10g
 - and Oracle Access Manager, 2-2
- Oracle Applications
 - Oracle Identity Manager Connectors, 6-2
- Oracle applications
 - and Oracle Access Manager, 2-3
- Oracle Business Intelligence
 - and Oracle Access Manager, 2-2
- Oracle Data Service Integrator
 - and Oracle Entitlements Server, 10-2
- Oracle Database Enterprise User Security LDAP, 9-2
- Oracle Database Net Services
 - Directory Naming with LDAP, 9-1
 - Directory Naming with Microsoft Active Directory using Oracle Virtual Directory, 9-2
 - Directory Naming with Oracle Directory Service Enterprise Edition using Oracle Virtual Directory, 9-2
 - Directory Naming with Oracle Internet Directory, 9-2
 - Directory Naming with Oracle Virtual Directory, 9-2
- Oracle Directory Server Enterprise Edition
 - and Oracle Entitlements Server, 10-2
 - Oracle Identity Manager Connector, 6-1
- Oracle Directory Service Enterprise Edition
 - and Enterprise User Security using Oracle Virtual Directory, 9-2
 - and Oracle Database Net Services for Directory Naming using Oracle Virtual Directory, 9-2
- Oracle E-Business Employee Reconciliation
 - Oracle Identity Manager Connector, 6-2
- Oracle E-Business Suite
 - and Oracle Access Manager, 2-3
- Oracle E-Business User Management
 - Oracle Identity Manager Connector, 6-2
- Oracle Enterprise Repository
 - and Oracle Entitlements Server, 10-2
- Oracle Enterprise Single Sign-On Suite, 3-1
 - for Password Reset, 8-2
 - Logon Manager, 3-1
- Oracle Entitlements Server
 - and Microsoft Active Directory 2000 and 2003, 10-3
 - and Microsoft ADAM, 10-3
 - and Microsoft .NET Framework 1.1 and 2.05, 10-3
 - and Microsoft Office SharePoint Server 2007, 10-3
 - and Novell eDirectory v8.7.31, 10-3
 - and Open LDAP v2.2.24, 10-3
 - and Oracle Access Manager, 10-1
 - and Oracle Adaptive Access Manager, 10-1
 - and Oracle Data Service Integrator, 10-2
 - and Oracle Directory Server Enterprise Edition, 10-2
 - and Oracle Enterprise Repository, 10-2
 - and Oracle Identity Federation, 10-2
 - and Oracle Identity Manager, 10-1
 - and Oracle Service Bus, 10-2
 - and Oracle Virtual Directory, 10-2
 - and Oracle WebLogic Server, 10-2
 - and Websphere Application Server 6.1, 10-3
 - for Oracle Fusion Middleware, 10-2
 - for Oracle Identity Management, 10-1
 - for third-party products, 10-3
- Oracle Fusion Middleware
 - and Oracle Access Manager, 2-2
 - and Oracle Entitlements Server, 10-2
 - and Oracle Identity Federation, 4-1
- Oracle HTTP Server
 - and Oracle Identity Federation for access management, 4-2
 - as proxy for Oracle Identity Federation, 4-2
- Oracle HTTP Server 10g
 - and Oracle Access Manager, 2-2
- Oracle HTTP Server 11g
 - and Oracle Access Manager, 2-2
- Oracle Identity Analytics, 7-1
 - and ETL process, 7-2
 - and Oracle Identity Manager, 7-1
 - and Oracle Waveset, 7-1
 - and third-party provisioning servers, 7-2
 - for Oracle Identity Management, 7-1
 - for third-party products, 7-2
- Oracle Identity Federation, 4-1
 - and Oracle Access Manager, 2-2, 4-1
 - and Oracle Entitlements Server, 10-2
 - and Oracle Fusion Middleware, 4-1
 - and Oracle HTTP Server for access management, 4-2
 - and Oracle Identity Management, 4-1
 - and Oracle Single Sign-On 10g, 4-1
 - Authentication Engines, 4-2
 - authentication mechanisms, 4-2
 - SP Integration
 - Oracle Access Manager, 4-3
 - Oracle Single Sign-On 10g, 4-3
 - Third-party IAM, 4-3
 - SP Integration Modules, 4-2
 - with Oracle HTTP Server as proxy, 4-2
- Oracle Identity Management
 - and Oracle Access Manager, 2-1
 - and Oracle Adaptive Access Manager, 5-1
 - and Oracle Entitlements Server, 10-1
 - and Oracle Identity Analytics, 7-1
 - and Oracle Identity Federation, 4-1
 - integration objectives, 1-1
 - Oracle Identity Manager Connectors, 6-1
 - Oracle Identity Manager for password

- management, 8-1
- Oracle Identity Manager
 - Adapter Factory Connectors, 6-5
 - and ESSO Provisioning Gateway, 3-2
 - and Oracle Access Manager, 2-1, 8-1
 - and Oracle Adaptive Access Manager, 5-2, 8-1
 - and Oracle Entitlements Server, 10-1
 - and Oracle Identity Analytics, 7-1
 - Connector for AD Password Synchronization, 6-4
 - Connector for AD User Management, 6-3
 - Connector for BMC Remedy Ticket Management, 6-3
 - Connector for BMC Remedy User Management, 6-3
 - Connector for CA ACF2 Advanced, 6-3
 - Connector for CA Top Secret Advanced, 6-3
 - Connector for Database Application Tables, 6-2, 6-3
 - Connector for Database User Management, 6-2, 6-3
 - Connector for IBM Lotus Notes and Domino, 6-3
 - Connector for IBM OS/400 Advanced, 6-3
 - Connector for IBM RACF Advanced, 6-3
 - Connector for IBM RACF Standard, 6-3
 - Connector for JD Edwards EnterpriseOne User Management, 6-2
 - Connector for Microsoft Exchange, 6-4
 - Connector for Microsoft Windows, 6-4
 - Connector for Novell eDirectory, 6-4
 - Connector for Novell GroupWise, 6-4
 - Connector for Oracle Directory Server Enterprise Edition, 6-1
 - Connector for Oracle E-Business Employee Reconciliation, 6-2
 - Connector for Oracle E-Business User Management, 6-2
 - Connector for Oracle Internet Directory, 6-1
 - Connector for Oracle Retail Warehouse Management System, 6-2
 - Connector for PeopleSoft Employee Reconciliation, 6-2
 - Connector for PeopleSoft User Management, 6-2
 - Connector for RSA Authentication Manager, 6-4
 - Connector for RSA ClearTrust, 6-4
 - Connector for SAP Employee Reconciliation, 6-4
 - Connector for SAP Enterprise Portal, 6-4
 - Connector for SAP User Management, 6-4
 - Connector for Siebel User Manager, 6-2
 - Connector for Unix SSH, 6-4
 - Connector for Unix Telnet, 6-5
 - Custom Connector with GTC, 6-5
 - for password flow, 5-2
 - for password management, 8-1
 - for provisioning, 6-1
 - Password Management for Oracle Identity Management, 8-1
 - password management with Connectors, 8-1
 - with Oracle Access Manager and Oracle Adaptive Access Manager, 8-1
- Oracle Identity Manager Connectors

- for Databases, 6-1
- for Oracle Applications, 6-2
- for Oracle Identity Management, 6-1
- Third-Party Applications, 6-3
- Oracle Identity Navigator
 - and Oracle Access Manager, 2-2
- Oracle Internet Directory
 - and Enterprise User Security, 9-2
 - and Oracle Adaptive Access Manager, 5-2
 - and Oracle Database Net Services, 9-2
 - as authentication provider, 5-2
 - Oracle Identity Manager Connector, 6-1
- Oracle Retail Warehouse Management System
 - Oracle Identity Manager Connector, 6-2
- Oracle Service Bus
 - and Oracle Entitlements Server, 10-2
- Oracle Single Sign-On 10g
 - and Oracle Identity Federation, 4-1
 - SP Integration with Oracle Identity Federation, 4-3
- Oracle Virtual Directory
 - and Oracle Adaptive Access Manager, 5-2
 - and Oracle Database Net Services, 9-2
 - and Oracle Entitlements Server, 10-2
 - as authentication provider, 5-2
 - Enterprise User Security with Microsoft Active Directory, 9-2
- Oracle Waveset
 - and ESSO Provisioning Gateway, 3-2
 - and Oracle Identity Analytics, 7-1
- Oracle WebCache
 - and Oracle Access Manager, 2-2
- Oracle WebLogic Server
 - and Oracle Access Manager, 2-2
 - and Oracle Entitlements Server, 10-2
 - SSO for applications, 2-2

P

- Password Management, 8-1
- password management, 1-3
 - with Oracle Identity Manager, 8-1
 - with Oracle Identity Manager connectors, 8-1
- Password Reset
 - with Oracle Enterprise Single Sign-On Suite, 8-2
- password reset
 - with ESSO-PR, 8-2
- PeopleSoft Employee Reconciliation
 - Oracle Identity Manager Connector, 6-2
- PeopleSoft Enterprise
 - and Oracle Access Manager, 2-3
- PeopleSoft User Management
 - Oracle Identity Manager Connector, 6-2
- Provisioning, 6-1
- Proximity cards
 - and ESSO Authentication Manager, 3-3

R

- Risk Management, 5-1

- RSA Authentication Manager
 - Oracle Identity Manager Connector, 6-4
- RSA ClearTrust
 - Oracle Identity Manager Connector, 6-4
- RSA SecurID
 - and ESSO Authentication Manager, 3-3

S

- SAP Employee Reconciliation
 - Oracle Identity Manager Connector, 6-4
- SAP Enterprise Portal
 - Oracle Identity Manager Connector, 6-4
- SAP mySAP
 - and Oracle Access Manager, 2-3
- SAP User Management
 - Oracle Identity Manager Connector, 6-4
- Siebel
 - and Oracle Access Manager, 2-3
- Siebel User Manager
 - Oracle Identity Manager Connector, 6-2
- smart cards
 - and ESSO Authentication Manager, 3-3

T

- Third-Party Applications
 - Oracle Identity Manager Connectors, 6-3
- third-party applications
 - and Oracle Access Manager, 2-3
- Third-party IAM
 - SP Integration with Oracle Identity Federation, 4-3
- third-party products
 - and Oracle Entitlements Server, 10-3
 - and Oracle Identity Analytics, 7-2
- third-party provisioning servers
 - and Oracle Identity Analytics, 7-2
- types of integration, 1-2

U

- Unix SSH
 - Oracle Identity Manager Connector, 6-4
- Unix Telnet
 - Oracle Identity Manager Connector, 6-5

W

- Web Access Management, 2-1
- Web access management, 1-3
- Web Services and SOAP API
 - Oracle Adaptive Access Manager, 5-2
- Web single sign-on, 2-1
- Websphere Application Server 6.1
 - and Oracle Entitlements Server, 10-3
- Windows Native Authentication
 - and Oracle Access Manager, 2-3

