

Oracle® Application Server Single Sign-On

Administrator's Guide

10g (10.1.4.0.1)

B15988-01

July 2006

Oracle Application Server Single Sign-On Administrator's Guide, 10g (10.1.4.0.1)

B15988-01

Copyright © 1996, 2006, Oracle. All rights reserved.

Contributing Author: Nina Wishbow

Contributors: Gaurav Bhatia, Kamalendu Biswas, Margaret Chou, Lee Cooper, Mike Hwa, Ganesh Kirti, Peifung Eric Lam, Andrew Maywah, Mark Nelson, Saurabh Shrivastava, Tim Willard

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States 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, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

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

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

Preface	xiii
Audience.....	xiii
Documentation Accessibility	xiii
Related Documents	xiv
Conventions	xiv
What's New in OracleAS Single Sign-On?	xv
Federated Authentication.....	xv
Configuring Custom (Deployment-Specific) Pages	xvi
Changes to the Syntax for Invoking OracleAS Single Sign-On.....	xvi
Changing the Single Sign-On Administration Group	xvi
Globalization Support.....	xvi
Elimination of the Database Access Descriptor (DAD)	xvi
Protecting URLs in the Absence of a Load Balancer	xvi
Information on Authentication Levels	xvii
Login Page Error Codes.....	xvii
Authentication URL	xvii
Configuring Single Sign-On Server for Multiple Realms.....	xvii
Configuring SSL for Partner Applications.....	xvii
Debug Log Files	xvii
URLs to Protected Resources Fail to Return the Resource.....	xvii
Secure Transmission of mod_osso Cookies.....	xviii
Obsolete Error Messages	xviii
1 About OracleAS Single Sign-On	
Key Components in the Single Sign-On System	1-1
Single Sign-On Server.....	1-1
Partner Applications.....	1-2
External Applications	1-2
mod_osso.....	1-2
Oracle Internet Directory	1-3
Oracle Identity Management Infrastructure	1-3
Single Sign-On Processes	1-3
Accessing the Single Sign-On Server.....	1-3

Accessing a Partner Application.....	1-4
Authenticating to a Partner Application After the First Time	1-4
Logging Out of an Partner Application.....	1-5
Accessing an External Application.....	1-5
Accessing the External Applications Portlet in OracleAS Portal.....	1-5
Authenticating to an External Application for the First Time.....	1-5
Authenticating to an External Application After the First Time	1-5
Logging Out of an External Application	1-6
Limitations on URLs to Access Applications.....	1-6
Single Sign-Off.....	1-6
Changing Passwords	1-6
Global User Inactivity Timeout.....	1-7
Signing On Using the Wireless Option.....	1-7

2 Basic Administration

The Single Sign-On Administrator's Role	2-1
Granting Administrative Privileges	2-2
Changing the Single Sign-On Administration Group.....	2-3
policy.properties	2-4
Stopping and Starting Single Sign-On Components.....	2-4
Using the Application Server Control Console	2-4
Using the Command Line.....	2-5
Stopping and Starting the Oracle HTTP Server	2-5
Stopping and Starting the OC4J_SECURITY Instance	2-5
Stopping and Starting the Single Sign-On Middle Tier	2-5
Stopping and Starting All Components	2-6
Stopping and Starting the Database	2-6
Troubleshooting an Inaccessible Server	2-6
Setting Browser Preferences for OracleAS Single Sign-On	2-7
Accessing the Administration Pages	2-8
Using the Edit Single Sign-On Server Page to Configure the Server	2-9
Configuring Globalization Support.....	2-9
Configuring the Global User Inactivity Timeout	2-10
Obtaining the Sample Files.....	2-12

3 Directory-Enabled Single Sign-On

Managing Users in Oracle Internet Directory	3-1
Password Policies	3-2
Password Rules	3-2
Configuring Password Life.....	3-2
Change Password Page Behavior	3-2
Password Has Expired	3-2
Password Is About to Expire.....	3-2
Grace Login Is in Force.....	3-3
Force Change Password.....	3-3
Configuring Account Lockout	3-3
Unlocking Users	3-3

Configuring Password Policies	3-3
Directory Tree for OracleAS Single Sign-On	3-3
Changing Single Sign-On Server Settings for Directory Access	3-5
Updating the Single Sign-On Server with Directory Changes	3-5
4 Configuring and Administering Partner Applications	
Registering a Partner Application: What It Means	4-1
Registering mod_osso	4-1
Syntax and Parameters for ssoresg.....	4-2
Command Example	4-4
Restarting the Oracle HTTP Server	4-4
Deploying Multiple Partner Applications with a Load Balancer	4-5
Usage Scenario.....	4-5
Configuration Steps	4-6
Installing the Partner Applications	4-6
Configuring the Oracle HTTP Servers on the Partner Application Middle Tiers	4-6
Configuring the HTTP Load Balancer	4-7
Reregistering mod_osso on the Partner Application Middle Tiers	4-8
Configuring mod_osso with Virtual Hosts (SSL and non-SSL)	4-9
5 Configuring and Administering External Applications	
Using the Interface to Deploy and Manage External Applications	5-1
Adding an External Application.....	5-1
Editing an External Application	5-4
Storing External Application Credentials in the Single Sign-On Database.....	5-4
Proxy Authentication for Basic Authentication Applications	5-5
Configuring the Oracle HTTP Server as a Proxy for Basic Authentication.....	5-5
Configuration Requirements	5-6
Configuration Steps	5-6
6 Multilevel Authentication	
What Is Multilevel Authentication?	6-1
How Multilevel Authentication Works	6-1
Components of a Multilevel System	6-2
Authentication Levels.....	6-2
Authentication Plugins.....	6-3
Configuring Multilevel Authentication	6-4
Configuration Steps	6-4
7 Enabling SSL	
Enable SSL on the Single Sign-On Middle Tier	7-2
Reconfigure the Identity Management Infrastructure Database	7-3
Change Single Sign-On URLs.....	7-3
Update targets.xml.....	7-4
Configure Oracle Enterprise Manager Security	7-4

Protect Single Sign-On URLs	7-4
Protecting URLs in the Absence of a Load Balancing Router	7-5
Protecting URLs in the Presence of a Load Balancing Router	7-5
Restart the Oracle HTTP Server and the Single Sign-On Middle Tier	7-5
Caveats About Configuring SSL	7-5
Reregister Partner Applications	7-6
Secure Transmission of mod_osso Cookies	7-6

8 Signing On with Digital Certificates

How Certificate-Enabled Authentication Works	8-1
System Requirements	8-2
Configuring the Single Sign-On System for Certificates	8-2
Oracle HTTP Server	8-2
Setting SSL Parameters.....	8-2
Choosing a Certificate Authority.....	8-3
Single Sign-On Server	8-3
Configure policy.properties with the Default Authentication Plugin	8-4
Modify the Configuration File for the Authentication Plugin (Optional)	8-4
Customize the User Name Mapping Module (Optional)	8-5
Restart the Single Sign-On Middle Tier	8-6
Oracle Internet Directory	8-6
Maintaining a Certificate Revocation List	8-7

9 Advanced Deployment Options

Deployment Scenarios	9-1
One Single Sign-On Middle Tier, One Oracle Internet Directory	9-1
Multiple Single Sign-On Middle Tiers, One Oracle Internet Directory	9-2
To Cluster Or Not to Cluster	9-3
Usage Scenario	9-3
Configuration Steps	9-4
Multiple Single Sign-On Middle Tiers, Replicated Oracle Internet Directory	9-8
Multiple, Geographically Distributed Single Sign-On Instances	9-8
Usage Scenario	9-8
Configuration Steps	9-9
Other High Availability Deployments.....	9-10
OracleAS Cold Failover Cluster (Infrastructure)	9-10
Disaster Recovery	9-10
Backup and Recovery	9-10
Replicating the Identity Management Database	9-11
The Replication Mechanism	9-11
Configuring the Identity Management Database for Replication.....	9-12
Adding a Node to a Replication Group,.....	9-13
Deleting a Node from a Replication Group	9-13
Deploying OracleAS Single Sign-On with a Proxy Server	9-13
Turn Off IP Checking.....	9-14
Enable the Proxy Server	9-14
Setting Up Directory Synchronization for User Nickname Changes	9-15

10	Enabling Support for Application Service Providers	
	Application Service Providers: Deciding to Deploy Multiple Realms	10-1
	Setting Up and Enabling Multiple Realms	10-1
	How the Single Sign-On Server Enables Authentication to Multiple Realms.....	10-2
	Locating Realms in Oracle Internet Directory	10-2
	Validating Realm-Affiliated Users to Partner Applications	10-3
	Configuring the Single Sign-On Server for Multiple Realms	10-4
	Granting Administrative Privileges for Multiple Realms	10-6
11	Monitoring the Single Sign-On Server	
	Setting the Database Monitoring Password	11-1
	Accessing the Monitoring Pages	11-1
	Interpreting and Using the Home Page on the Standalone Console	11-2
	Interpreting and Using the Details of Login Failures Page	11-3
	Updating the Port Property for the Single Sign-On Monitoring Target.....	11-4
	Using the OracleAS Web Cache Instance to Monitor the Server.....	11-5
	Monitoring a Single Sign-On Server Enabled for SSL.....	11-5
12	Creating Deployment-Specific Pages	
	How the Single Sign-On Server Uses Deployment-Specific Pages	12-1
	How to Write Deployment-Specific Pages	12-2
	Login Page Parameters.....	12-3
	Forgot My Password.....	12-4
	Change Password Page Parameters	12-4
	Single Sign-Off Page Parameters	12-5
	External Application Login Page Parameters	12-6
	Page Error Codes	12-7
	Login Page Error Codes	12-7
	Post-Login Messages	12-9
	Change Password Page Error Codes	12-9
	Change External Application Login Page Error Codes	12-9
	Adding Globalization Support	12-10
	Deciding What Language to Display the Page In	12-10
	Use the Accept-Language Header to Determine the Page	12-10
	Use Page Logic to Determine the Language	12-10
	Rendering the Page	12-11
	Guidelines for Deployment-Specific Pages	12-11
	Installing Deployment-Specific Pages	12-12
	Using policy.properties to Install Login, Single Sign-Off, and Change Password Pages ..	12-12
	Using policy.properties to Install Wireless Login and Change Password Pages	12-12
	Using policy.properties to Install External Application Login Pages	12-12
	Examples of Deployment-Specific Pages	12-13
	Using Custom Classes	12-13

13	Integrating with Oracle Identity Federation	
	How Federated Single Sign-On Works	13-1
	Federated Single Sign-On From the User’s Perspective	13-2
	Configuring the Oracle Stack as the Service Provider	13-2
	Configuring the Oracle Stack as the Identity Provider	13-4
	Adding Federated Authentication URLs to a Web Portal	13-6
14	Integrating with Third-Party Access Management Systems	
	How Third-Party Access Management Works	14-1
	Scenario 1: The user has not yet authenticated to the third-party server	14-2
	Scenario 2: The user has already authenticated to the third-party server	14-3
	Synchronizing the Third-Party Repository with Oracle Internet Directory	14-3
	Third-Party Integration Modules	14-3
	Using Vendor-Supplied Packages	14-4
	Building Your Own Package	14-4
	Guidelines for Using the Interfaces	14-4
	The Classes and Interfaces	14-4
	Configuration Steps	14-9
	Logging Out of the Integrated System	14-10
	Integrating with Windows Native Authentication	14-11
	Integration Case Study: SSOAcme	14-11
	Sample Integration Package	14-12
	Migrating the Release 9.0.2 Sample Implementation to Release 10.1.3	14-13
	New Authentication Interface	14-13
	Get User Name from HTTP Header	14-14
	Error Handling if User Name Not Present	14-14
	Return User Name to Single Sign-On Server	14-14
15	Exporting and Importing Data	
	What’s Exported and Imported?	15-1
	Export and Import Script: Syntax and Parameters	15-1
	Script Syntax	15-1
	Script Parameters	15-2
	Exporting Data from One Server to Another	15-3
	Export and Import Scenarios and Script Examples	15-3
	Export Scenarios	15-3
	Import Scenarios	15-4
	Running the Script	15-4
	Verifying That Export and Import Succeeded	15-5
	Consolidating Multiple Servers	15-5
	Error Messages	15-5
A	Troubleshooting OracleAS Single Sign-On	
	Problems and Solutions for General Single Sign-On Server Errors	A-1
	URL Exceeds Maximum Length	A-2
	Internal Server Error	A-2

Unexpected Error	A-3
File Not Found Error	A-4
Authentication Failed	A-4
The User Name Submitted for Authentication Does Not Match the User Name Present in the Existing Single Sign-On Session	A-5
White Page Displayed When Accessing OracleAS Single Sign-On Administration	A-5
Administrator Cannot See OracleAS Single Sign-On Administration Pages.....	A-6
The "SSO Server Administration" Link is Missing from the OracleAS Single Sign-On Administration Page	A-6
Audit Log Insertion Exception: ORA-00018: Maximum Number of Sessions Exceeded	A-7
Connection Limit Exceeded.....	A-7
Failed Login Message when System has been Idle	A-7
Error due to Idle LDAP or Database Connection Timeouts	A-8
Login to Portal Fails.....	A-8
Problems and Solutions for Certificate Authentication Errors	A-9
Network Error: Connection Refused.....	A-9
The Single Sign-On Server Fails to Prompt the User for a Certificate.....	A-10
Certificate Authentication Fails - User Is Presented with the Login Page.....	A-10
User's Browser Certificate Not Found	A-10
Mapping Module Class Name Not Found.....	A-10
Mapping Module Instance Creation Failed.....	A-11
Cannot Create the Mapping Module Object.....	A-11
Exception in Creating Mapping Module	A-11
Certificate Match Failed	A-11
Problems and Solutions for Windows Native Authentication Errors	A-11
A User Cannot Access a URL After Authenticating in Windows.....	A-12
A User Who Is Already Authenticated in Windows Cannot Authenticate in the Browser.	A-13
single sign-on server Fails to Start with a Credential Not Found Error	A-13
Single Sign-On Server Displays Internal Server Error.....	A-13
Single Sign-On Users Unable to Authenticate to KDC.....	A-13
Windows Login Dialog Appears When Accessing a Partner Application.....	A-14
Problems and Solutions for Password Policy Errors	A-14
A Disabled User Can Still Log In.....	A-14
A Disabled User Sees "Authentication Failed" Instead of "Account Disabled" Message	A-14
The User Receives a Password Expiration Message at Login	A-15
Password Expiration Message Does Not Appear on Command-Line Tools	A-15
Diagnosing OracleAS Single Sign-On Problems	A-15
Viewing the Log Files	A-15
Increasing the Debug Log Level	A-16
Enabling the Debug Option in the Single Sign-On Database	A-17
Enabling LDAP Tracing for UI Operations	A-18
Maintenance Tasks for OracleAS Single Sign-On.....	A-19
Managing Single Sign-On Audit Records	A-19
Refreshing the LDAP Connection Cache.....	A-19
Restarting OC4J After Modifying Oracle Internet Directory.....	A-20
A Word About Non-GET Authentication	A-20
Need More Help?	A-20

B Obtaining the Single Sign-On Schema Password

Using the Command Line	B-1
Using Oracle Directory Manager	B-2

C policy.properties

Glossary

Index

List of Figures

1-1	Single Sign-On with mod_osso	1-4
2-1	iASAdmins Tab of Oracle Directory Manager	2-3
2-2	Using the Console to Restart the Single Sign-On Middle Tier	2-5
2-3	SSO Server Administration Page	2-9
3-1	Directory Information Tree for OracleAS Single Sign-On	3-4
4-1	Load Balancer with Multiple Partner Applications	4-6
5-1	External Application Login Page	5-4
5-2	Authentication Flow Using mod_osso/mod_proxy	5-6
6-1	Multilevel Authentication Flow	6-2
8-1	Certificate-Enabled Single Sign-On	8-1
9-1	Default Single Sign-On Installation: One Computer	9-2
9-2	Single Sign-On Installation: Two Computers	9-2
9-3	Two Single Sign-On Middle Tiers, One Oracle Internet Directory	9-4
9-4	A Highly Available, Geographically Distributed Single Sign-On System	9-9
9-5	Multimaster Replication Architecture	9-11
10-1	The Big Picture: Single Sign-On in Multiple Realms	10-3
10-2	mod_osso Headers for Users with the Same Name	10-4
11-1	Monitoring Home Page for OracleAS Single Sign-On	11-3
11-2	Details of Login Failures Page	11-4
14-1	Accessing Oracle Partner Applications Using a Third-Party Server	14-2

List of Tables

2-1	Single Sign-On Session Policy.....	2-9
5-1	External Application Login	5-2
5-2	Authentication Method	5-2
5-3	Additional Fields.....	5-2
6-1	Default Authentication Levels	6-3
8-1	HTTP Parameters for Certificate-Enabled Single Sign-On	8-3
9-1	Parameters for ssoReplSetup.....	9-13
10-1	Parameters for enblhstg.csh and addsub.csh.....	10-6
12-1	Login Page Parameters Submitted to the Page by the Single Sign-On Server.....	12-3
12-2	Login Page Parameters Submitted by the Page to the Single Sign-On Server.....	12-3
12-3	Change Password Parameters Submitted to the Page.....	12-4
12-4	Change Password Page Parameters Submitted by the Page	12-5
12-5	Parameters Submitted to the Single Sign-Off Page.....	12-5
12-6	Parameters Submitted to the External Application Login Page	12-6
12-7	Parameters the External Application Login Page Submits to the Application.....	12-6
12-8	Login Page Error Codes	12-7
12-9	Post-Login Messages	12-9
12-10	Change Password Page Error Codes	12-9
12-11	External Application Login Page Error Codes	12-9
15-1	Parameters Passed to ssomig	15-2
15-2	Error Codes for Export and Import.....	15-5

Preface

Oracle Application Server Single Sign-On Administrator's Guide contains concepts and procedures for managing user authentication to Oracle Application Server (OracleAS). The material presented in this book applies to UNIX and Windows platforms.

This preface contains these topics:

- [Audience](#)
- [Documentation Accessibility](#)
- [Related Documents](#)
- [Conventions](#)

Audience

Oracle Application Server Single Sign-On Administrator's Guide is intended for the following users:

- Administrators charged with configuring and managing authentication to OracleAS.
- Developers of features for which OracleAS Single Sign-On is the authentication mechanism. The book is particularly for those who want to integrate these features with `mod_osso`, an authentication module on the Oracle HTTP Server.
- Anyone who wants to understand how to use OracleAS Single Sign-On to protect access to Web applications.

This document assumes that the reader has a rudimentary knowledge of OracleAS and has installed, or is able to install, release 10.1.3.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. 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.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, see these Oracle resources:

- *Oracle Identity Management Application Developer's Guide*
- *Oracle Internet Directory Administrator's Guide*

Printed documentation is available for sale in the Oracle Store at

<http://oraclestore.oracle.com/>

To download free release notes, installation documentation, white papers, or other collateral, please visit the Oracle Technology Network (OTN). You must register online before using OTN; registration is free and can be done at

<http://www.oracle.com/technology/membership>

If you already have a user name and password for OTN, then you can go directly to the documentation section of the OTN Web site at

<http://www.oracle.com/technology/documentation/>

To keep abreast of the latest developments in OracleAS Single Sign-On, see the following link:

http://www.oracle.com/technology/products/id_mgmt/osso/index.html

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 OracleAS Single Sign-On?

This section describes new features of the OracleAS Single Sign-On 10g (10.1.4.0.1) and provides pointers to additional information. Information from previous releases is also retained to help those users migrating to the current release.

The following sections describe the new features in OracleAS Single Sign-On that are presented in this book:

- [Federated Authentication](#)
- [Configuring Custom \(Deployment-Specific\) Pages](#)
- [Changes to the Syntax for Invoking OracleAS Single Sign-On](#)
- [Changing the Single Sign-On Administration Group](#)
- [Globalization Support](#)
- [Elimination of the Database Access Descriptor \(DAD\)](#)
- [Protecting URLs in the Absence of a Load Balancer](#)
- [Information on Authentication Levels](#)
- [Login Page Error Codes](#)
- [Authentication URL](#)
- [Configuring Single Sign-On Server for Multiple Realms](#)
- [Configuring SSL for Partner Applications](#)
- [Debug Log Files](#)
- [URLs to Protected Resources Fail to Return the Resource](#)
- [Secure Transmission of mod_osso Cookies](#)
- [Obsolete Error Messages](#)

Federated Authentication

- You can implement federated authentication using Oracle Application Server Single Sign-On and Oracle Identity Federation. Federated single sign-on permits users to access information on different corporate Web sites while authenticating to only one of those sites. You can configure either Oracle Application Server Single Sign-On or Oracle Identity Federation to be the authentication mechanism for users who want to access resources that are protected by either product.

See Also: ["Integrating with Oracle Identity Federation"](#) on page 13-1.

Configuring Custom (Deployment-Specific) Pages

- The WWSSO_LS_CONFIGURATION_INFO\$ table is no longer required for the single sign-off page.
- You can configure custom login pages for external applications.

See Also: ["Installing Deployment-Specific Pages"](#) on page 12-12.

Changes to the Syntax for Invoking OracleAS Single Sign-On

- The syntax for invoking OracleAS Single Sign-On has been simplified. For example, instead of accessing the administration home page by typing the following URL:

```
http://host:port/pls/orasso
```

You can now use the following:

```
http://host:port/sso
```

See Also: ["Accessing the Single Sign-On Server"](#) on page 1-3, ["Accessing the Administration Pages"](#) on page 2-8, ["Reregistering mod_osso on the Partner Application Middle Tiers"](#) on page 4-8, ["Enabling SSL"](#) on page 7-1, ["Advanced Deployment Options"](#) on page 9-1, ["Monitoring a Single Sign-On Server Enabled for SSL"](#) on page 11-5, ["Creating Deployment-Specific Pages"](#) on page 12-1,

Changing the Single Sign-On Administration Group

- The steps for this procedure have changed.

See Also: ["Changing the Single Sign-On Administration Group"](#) on page 2-3.

Globalization Support

- This information for this has been updated. Pointers have been added to additional information.

See Also: ["Configuring Globalization Support"](#) on page 2-9.

Elimination of the Database Access Descriptor (DAD)

- This table no longer is needed and has been removed.

See Also: ["Troubleshooting an Inaccessible Server"](#) on page 2-6.

Protecting URLs in the Absence of a Load Balancer

- The syntax for this operation has changed.

See Also: ["Protecting URLs in the Absence of a Load Balancing Router"](#) on page 7-5.

Information on Authentication Levels

- Information on authentication levels has been expanded.

See Also: ["Authentication Levels"](#) on page 6-2.

Login Page Error Codes

- Information on login page error codes has been updated.

See Also: ["Login Page Error Codes"](#) on page 12-7 and ["Post-Login Messages"](#) on page 12-9.

Authentication URL

- Information on the authentication URL has been updated.

See Also: ["How the Single Sign-On Server Uses Deployment-Specific Pages"](#) on page 12-1.

Configuring Single Sign-On Server for Multiple Realms

- This procedure has changed.

See Also: ["Configuring the Single Sign-On Server for Multiple Realms"](#) on page 10-4.

Configuring SSL for Partner Applications

- Information has been added about configuring SSL for partner applications (including OracleAS Single Sign-On).

See Also: ["Caveats About Configuring SSL"](#) on page 7-5 and ["Automated SSL Configuration"](#) on page 7-1.

Debug Log Files

- A note has been added to notify users that debug log files should not be deleted when OC4J is running.

See Also: ["Diagnosing OracleAS Single Sign-On Problems"](#) on page A-15.

URLs to Protected Resources Fail to Return the Resource

- A note has been added regarding some browsers' limitations regarding URL length. For some situations, configuring mod_osso to use the POST method instead of the GET directive can be an effective work-around.

See Also: ["URL Exceeds Maximum Length"](#) on page A-2.

Secure Transmission of mod_osso Cookies

- A section has been added regarding adding the OsoSecureCookies directive to ensure that cookies are transmitted using HTTPS.

See Also: ["Secure Transmission of mod_osso Cookies"](#) on page 7-6.

Obsolete Error Messages

- The error, "Forbidden Error When Accessing OracleAS Single Sign-on Administration" is now obsolete, as are all Type 41400 errors.

See Also: ["Troubleshooting OracleAS Single Sign-On"](#) on page A-1.

About OracleAS Single Sign-On

Oracle Application Server (OracleAS) Single Sign-On enables you to use a single user name, password, and optionally a realm ID to log in to all features of OracleAS as well as to other Web applications.

OracleAS Single Sign-On provides the following benefits:

- Reduced administrative costs
The single sign-on server eliminates the need to support multiple accounts and passwords.
- Convenient login
Users do not have to maintain a separate user name and password for each application that they access.
- Increased security
When a password is required only once, users are less likely to use simple, easily exposed passwords or to write these passwords down.

This chapter contains the following topics:

- [Key Components in the Single Sign-On System](#)
- [Single Sign-On Processes](#)

Key Components in the Single Sign-On System

OracleAS Single Sign-On interacts with several components that are described in the following sections.

Single Sign-On Server

The single sign-on server consists of program logic that enables users to log in securely to single sign-on applications such as expense reports, mail, and benefits. The single sign-on server program logic resides in the Oracle Application Server database, Oracle HTTP Server, and OC4J server.

The single sign-on server enables you to log in securely to applications such as expense reports, mail, and benefits. These applications take two forms: partner applications and external applications. In both cases, you gain access to several applications by authenticating only once.

Partner Applications

A partner application is an Oracle Application Server application or non-Oracle application that delegates the authentication function to the OracleAS Single Sign-On server. This type of application spares users from reauthenticating by accepting headers from an authentication module named `mod_osso`.

The `mod_osso` module enables partner applications to accept authenticated user information instead of a user name and password once the user has logged in to the single sign-on server.

A partner application is responsible for determining whether a user authenticated by OracleAS Single Sign-On is authorized to use the application.

Examples of partner applications include OracleAS Portal, OracleAS Discoverer, and Oracle Delegated Administration Services.

External Applications

External applications do not delegate authentication to the OracleAS Single Sign-On server. Instead, they display HTML login forms that ask for application user names and passwords. Each external application may require a unique user name and password. For example, Yahoo! Mail is an external application that uses HTML login forms.

At the first login to an external application, users can choose to have the OracleAS Single Sign-On server retrieve these credentials for them. To save these credentials, the user selects the **Remember My Login Information For This Application** check box when first logging in. Once the credentials have been saved, server uses the single sign-on user name to locate and retrieve application names and passwords and to log the user in without requiring the user to authenticate.

You can configure the single sign-on server to provide user names and passwords to external applications on users' behalf once they have logged in to the single sign-on server. Users have the option of storing application credentials in the single sign-on database.

`mod_osso`

The `mod_osso` module is an Oracle HTTP Server module that provides authentication to OracleAS applications. This module resides on the Oracle HTTP Server that enables applications protected by OracleAS Single Sign-On to accept HTTP headers in lieu of a user name and password once the user has logged into the OracleAS Single Sign-On server. The values for these headers are stored in a `mod_osso` cookie.

The `mod_osso` module replaces the single sign-on SDK that was used in earlier releases of OracleAS Single Sign-On to integrate partner applications. Located on the application server, `mod_osso` simplifies the authentication process by serving as the sole partner application to the single sign-on server. In this way, `mod_osso` renders authentication transparent to OracleAS applications. The administrator for these applications is spared the burden of integrating them with an SDK.

After authenticating a user, `mod_osso` transmits the simple header values that applications may use to authorize the user:

- User name
- User GUID
- Language and territory

To learn more about the attributes that the single sign-on server passes to `mod_osso`, see the chapter about `mod_osso` in *Oracle Identity Management Application Developer's Guide*. This chapter explains how to develop applications for single sign-on.

`mod_osso` works only with the Oracle HTTP listener. You can use OracleAS SSO Plug-in to protect applications that work with third-party listeners such as Sun One and IIS. To learn how to use OracleAS SSO Plug-in, see the appendix about this tool in *Oracle HTTP Server Administrator's Guide*.

Oracle Internet Directory

The Oracle Internet Directory is a general purpose LDAP directory service that enables retrieval of information about dispersed users and network resources. Oracle Internet Directory is the repository for all single sign-on user accounts and passwords—administrative and nonadministrative. The single sign-on server authenticates users against their entries in the directory. At the same time, it retrieves user attributes from the directory that enable applications to validate users.

Oracle Identity Management Infrastructure

This is an infrastructure that enables you to manage centrally and securely all enterprise identities and their access to applications in the enterprise. OracleAS Single Sign-On is just one link in an integrated infrastructure that also includes Oracle Internet Directory, Oracle Directory Integration and Provisioning, Oracle Delegated Administration Services, and OracleAS Certificate Authority. Working together, these components, called the Oracle Identity Management infrastructure, manage the security life cycle of users and other network entities in an efficient, cost-effective way.

To learn more about the benefits of Oracle Identity Management, see *Oracle Identity Management Administrator's Guide*.

Single Sign-On Processes

This section describes the following processes:

- [Accessing the Single Sign-On Server](#)
- [Accessing an External Application](#)
- [Single Sign-Off](#)
- [Changing Passwords](#)
- [Global User Inactivity Timeout](#)
- [Signing On Using the Wireless Option](#)

Accessing the Single Sign-On Server

Nonadministrative users first gain access to the single sign-on server by entering the URL of a partner application such as OracleAS Portal. Entering such a URL invokes the single sign-on login screen. Once they have entered the correct user name and password, users gain access to other partner applications and to external applications without having to provide credentials again.

Administrative users can access the administration home page for single sign-on by typing a URL of this form:

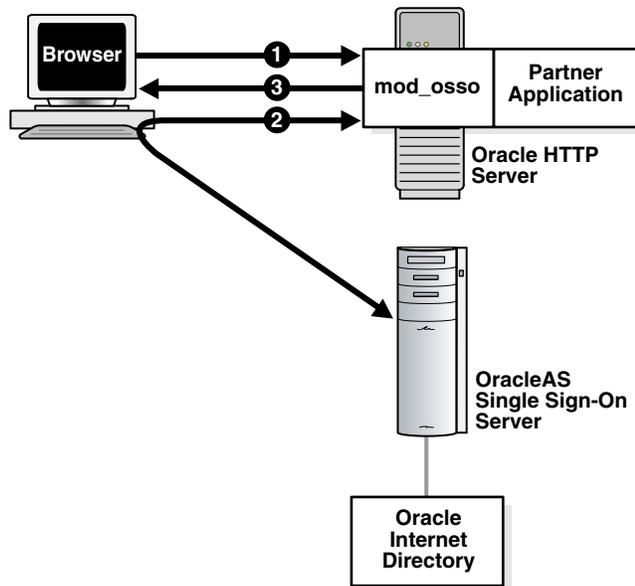
`http://host:port/sso`

where *host* is the computer where the single sign-on server is located and *port* is the port number of the server. If the server is enabled for SSL, `https` must be substituted for `http`. If the port number is 80 or 443 (SSL), it may be omitted from the URL. These numbers are the defaults.

Accessing a Partner Application

Figure 1–1 shows what happens when the user requests the URL of a partner application that is protected by `mod_osso`.

Figure 1–1 Single Sign-On with `mod_osso`



1. The user tries to access a partner application.
2. The user is redirected to the single sign-on server. The server challenges the user for credentials. After verifying the credentials in Oracle Internet Directory, the server sets the SSO session cookie and passes an authentication token to the partner application.
3. The application serves up the requested content.

Authenticating to a Partner Application After the First Time

Requesting access to a partner application initiates the partner application login process. The following occurs if you are accessing a new partner application after having already logged in to the Single Sign-On server:

1. The user tries to access a partner application.
2. The user is redirected to the single sign-on server. The server does not challenge the user for authentication credentials. The SSO session cookie is used to validate the user identity.
3. The server passes an authentication token to the partner application.
4. The application serves the requested content.

Logging Out of an Partner Application

Unlike external applications, partner applications cede logout control to the single sign-on server. When the user logs out of one partner application, he or she is automatically logged out of the other partner applications.

Accessing an External Application

External applications are available through OracleAS Portal, a single sign-on partner application.

This section contains these topics:

- [Accessing the External Applications Portlet in OracleAS Portal](#)
- [Authenticating to an External Application for the First Time](#)
- [Authenticating to an External Application After the First Time](#)
- [Logging Out of an External Application](#)

Accessing the External Applications Portlet in OracleAS Portal

To gain access to an external application, you select the External Applications portlet on the OracleAS Portal home page; then, from the list of external applications that appears, you select an application.

Authenticating to an External Application for the First Time

Selecting an application in the External Applications portlet initiates the external application login procedure. The following occurs if you are accessing the application for the first time:

1. The external application login procedure checks the single sign-on password store for your credentials. If it finds no credentials, the single sign-on server prompts you for them.
2. You enter your user name and password. You can save these credentials in the password store by selecting the **Remember My Login Information** check box on the application login screen.
3. If you elect to save your credentials in the password store, the server uses these credentials to construct a login form to submit to the login processing routine of the application. This routine has been preconfigured by the administrator and is associated with the requested application.
4. The server sends the form to the client browser, with a directive to post it immediately to the external application.
5. The client posts the form to the external application and logs you in.

If you decline to save your credentials in the password store, you must enter a user name and password each time that you log in.

Authenticating to an External Application After the First Time

If you saved your credentials when accessing an external application for the first time, the single sign-on server retrieves your credentials for you during subsequent logins. The process works like this:

1. You click one of the links in the External Applications portlet of OracleAS Portal.
2. The external application login procedure checks the password store for your credentials.

3. The single sign-on server finds your credentials and uses them to construct a login form to submit to the login processing routine of the application. This routine has been preconfigured by the administrator and is associated with the requested application.
4. The server sends the form to the client browser, with a directive to post it immediately to the external application.
5. The client posts the form to the external application and logs you in.

Logging Out of an External Application

Unlike partner applications, external applications do not cede logout control to the single sign-on server. It is the user's responsibility to log out of each of these applications.

Limitations on URLs to Access Applications

On some browsers, user attempts to access resources may exceed the maximum URL length, even though the originally requested URL is shorter than the maximum allowed by the browser.

Single Sign-Off

You can terminate a single sign-on session and log out of all active partner applications simultaneously by logging out of whatever application you are working in. Clicking **Logout** in a partner application takes you to the single sign-off page, where logout occurs.

If you signed off successfully, each of the applications listed on the single sign-off page has a check mark next to the application name. A broken image next to an application name denotes an unsuccessful logout.

Once all of the application names activated in a session have a check mark, you can click **Return** to go to the application from which you initiated logout.

Changing Passwords

The change password screen appears only when your password is about to expire and you fall within a grace login period. If the password is still valid, you can click **Cancel** on this screen and proceed with the login.

To change or reset a password under other circumstances, a nonadministrative user must go to Oracle Delegated Administration Services, a service of Oracle Internet Directory that performs user and group management functions.

The Oracle Delegated Administration Services home page is found at a URL of the following form:

```
http://host:port/oiddas/
```

where *host* is the name of the computer where Oracle Delegated Administration Services is located, and *port* is the port number of this server. Oracle Delegated Administration Services and OracleAS Single Sign-On generally have the same host name. If the Oracle HTTP Server hosting Oracle Delegated Administration Services and OracleAS Single Sign-On is enabled for SSL, `https` must be substituted for `http`. The port number may be omitted if it is 80 or 443 (SSL) because these numbers are the defaults.

Your password cannot contain the following characters: `&`, `{`, `}`, `<`, `>`, `"`, `'`, `(`, and `)`.

Note: Unlike single sign-on user names, single sign-on passwords are case sensitive and must conform to the Oracle Internet Directory realms that users belong to.

Global User Inactivity Timeout

The global user inactivity timeout is a feature that enables applications to force you to reauthenticate if you have been idle for a preconfigured amount of time. This timeout is a useful feature for sensitive applications that require a shorter user inactivity timeout than the single sign-out session timeout.

When you exceed the global user inactivity timeout limit and try to access the application, the application sends the single sign-on server an authentication request as usual. The server, ascertaining that you have exceeded the timeout limit, prompts you to log in. If you have not exceeded the limit, the server uses the session cookie to authenticate you.

Note: You may have a valid single sign-on session, but if you have exceeded the global timeout limit, the server prompts you for credentials.

See Also: ["Configuring the Global User Inactivity Timeout"](#) on page 2-10

Signing On Using the Wireless Option

You can use mobile, or wireless, devices such as personal digital assistants, cellular phones, and voice recognition systems to access OracleAS applications. As in PC-based systems, the authentication mechanism is OracleAS Single Sign-On. You can select the wireless option when installing OracleAS. If you do, Portal-to-Go, the gateway for mobile devices, is registered with the single sign-on server automatically.

To learn more about OracleAS Wireless see *Oracle Application Server Wireless Administrator's Guide* and *Oracle Application Server Wireless Developer's Guide*.

Basic Administration

This chapter introduces you to the tasks involved in administering single sign-on. The chapter contains the following topics:

- [The Single Sign-On Administrator's Role](#)
- [Granting Administrative Privileges](#)
- [Changing the Single Sign-On Administration Group](#)
- [policy.properties](#)
- [Stopping and Starting Single Sign-On Components](#)
- [Troubleshooting an Inaccessible Server](#)
- [Setting Browser Preferences for OracleAS Single Sign-On](#)
- [Accessing the Administration Pages](#)
- [Using the Edit Single Sign-On Server Page to Configure the Server](#)
- [Configuring Globalization Support](#)
- [Configuring the Global User Inactivity Timeout](#)
- [Obtaining the Sample Files](#)

The Single Sign-On Administrator's Role

When the single sign-on server is accessed for the first time, only one single sign-on administrator exists. This administrator is named `orcladmin`, the Oracle Application Server Single Sign-On super user. The person installing Oracle Application Server Single Sign-On selects the password for this user at install time. A password cannot contain the following characters: `&`, `{`, `}`, `<`, `>`, `"`, `'`, `(`, and `)`. The `orcladmin` account is used to create other accounts, including accounts for `iASAdmins`, the group that administers single sign-on.

As a single sign-on administrator, you can use the administration pages to do the following:

- Configure server settings
- Administer partner applications
- Administer external applications

Granting Administrative Privileges

To exercise your privileges as a single sign-on administrator, you must be a member of the administrative group `iASAdmins`. This means that an existing member of this group must add you to it.

To assign a user to `iASAdmins`:

1. Start Oracle Directory Manager. To learn how to start this tool, see *Oracle Internet Directory Administrator's Guide*.
2. Log in as `cn=orcladmin`, the directory super user. You must use the password that was assigned to this user when Oracle Internet Directory was installed.

Note: The directory superuser `cn=orcladmin` is not the same as the OracleAS super user `orcladmin`. These are separate, hierarchically unequal accounts.

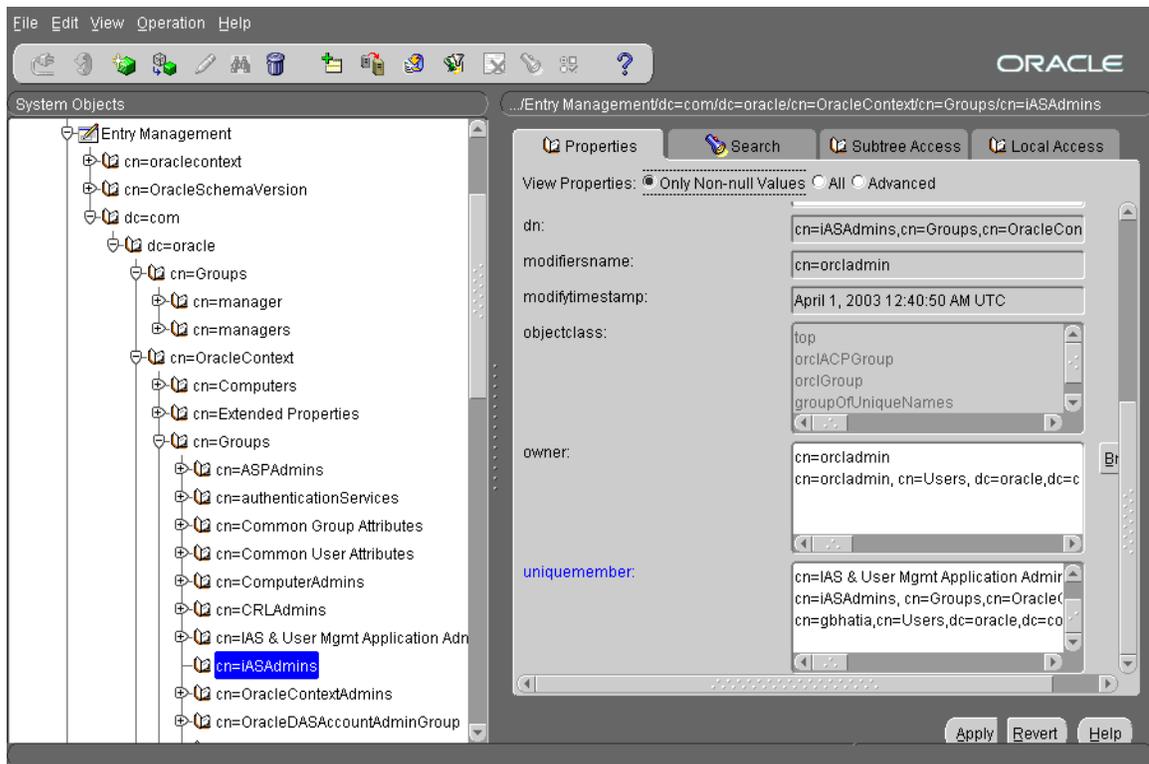
3. In the **System Objects** frame, click in succession the following entries:
 - Entry Management
 - `dc=default_identity_management_realm`
 - `cn=OracleContext`
 - `cn=Groups`
 - `cn=iASAdmins`

For example:

```
cn=iASAdmins,cn=Groups,cn=OracleContext,dc=oracle,dc=com
```

Where `dc=oracle`, `dc=com` is the default identity management realm. In reality, the default is likely the domain name of your installation.

4. In the **uniquemembers** text box of the **iASAdmins** tab, add an entry for the user. `uniquemembers` is an attribute of the entry `iASAdmins`. As such it defines members of the group `iASAdmins`. Be sure to add the user's full DN. In [Figure 2-1](#) on page 2-3 the user `cn=gbbhatia,cn=users,dc=oracle,dc=com` has been added.
5. Click **Apply**.

Figure 2-1 *iASAdmins Tab of Oracle Directory Manager*

To create new users, use Oracle Delegated Administration Services. See the chapter about the Oracle Internet Directory Self-Service Console in *Oracle Identity Management Guide to Delegated Administration*.

Changing the Single Sign-On Administration Group

By default, the single sign-on server uses the directory entry `cn=iASAdmins, cn=Groups, cn=OracleContext, default_realm_dn` to determine whether a user has administrative privileges for OracleAS Single Sign-On. Once you complete the following steps, all users in the group `cn=sso_admins, dc=us, dc=acme, dc=com` can administer the single sign-on server. You may also include groups as members by following these steps:

1. Create a new group in the directory relative to the default realm DN. If, for example, your default realm is `dc=us, dc=acme, dc=com`, and you want the default administration group to be called `sso_admins`, create this entry:

```
cn=sso_admins, dc=us, dc=acme, dc=com
```

Use either Oracle Directory Manager or LDAP command line tools to create the entry.

2. In the `policy.properties` file located in `ORACLE_HOME/sso/conf`, update the `ssoAdministratorGroupDN` to identify the group entry in the directory:

```
ssoAdministratorGroupDN = cn=sso_admins
```

You do not have to include the default realm (`dc=us, dc=acme, dc=com` in the example). The single sign-on server appends the realm when it checks for group membership.

3. Restart the OC4J_SECURITY instance, as described in ["Stopping and Starting the OC4J_SECURITY Instance"](#) on page 2-5.

policy.properties

The `policy.properties` file is a configuration file for OracleAS Single Sign-On. This file contains basic parameters required by the single sign-on server. The default values for these parameters are adequate for most installations. The file requires no modification out of the box.

You can configure `policy.properties` to implement advanced single sign-on features such as multilevel authentication. The `policy.properties` file is located in `ORACLE_HOME/sso/conf`. A copy of this file is provided in [Appendix C, "policy.properties"](#).

Note: When editing `policy.properties`, take care not to insert blank space at the end of each line. After editing the file, restart the single sign-on server. See the section immediately following for instructions.

Stopping and Starting Single Sign-On Components

You can use either the command line or the Oracle Enterprise Manager Application Server Control console to start and stop single sign-on components. The console offers the benefit that you can stop or start several components at once. The command line requires several commands for the same tasks.

Using the Application Server Control Console

Use these steps to stop and start single sign-on components with the console:

1. Go to the standalone console for the infrastructure instance of Oracle Enterprise Manager that you want to administer. To do this, enter the host name of the computer hosting the OracleAS instance and the port number of Oracle Enterprise Manager. The default port number is 1156. You can find the instance-specific port number as follows:

UNIX: `ORACLE_HOME/install/setupinfo.txt`

Windows: `ORACLE_HOME\install\setupinfo.txt`

2. Log in using the credentials of an OracleAS administrator.
3. From the **Standalone Instances** section of the Farm page, choose the appropriate OracleAS instance.
4. From the **System Components** list of the Application Server page, select the check boxes for the components that you want to stop, start, or restart; then click the appropriate button at the top of the list. [Figure 2-2](#) on page 2-5 shows the single sign-on middle tier being restarted. To stop or restart the entire identity management infrastructure, click **Stop All** or **Restart All** at the top of the page.

Figure 2–2 Using the Console to Restart the Single Sign-On Middle Tier

Page Refreshed Sep 30, 2004 6:39:45 PM

General



Status **Up**
 Host **isunnae29**
 Installation Type **Infrastructure_ID**
 Oracle Home **/private/iaatest/oracle/ias1012**
 Farm **ias1012.us.oracle.com**

CPU Usage



Application Server (0%)
 Idle (97%)
 Other (3%)

Memory Usage



Application Server (84% 863MB)
 Free (16% 161MB)
 Other (0% 0MB)

System Components

Select All | Select None

Select Name	Status	Start Time	CPU Usage (%)	Memory Usage (MB)
<input checked="" type="checkbox"/> HTTP_Server	↑	Sep 24, 2004 12:55:50 PM	0.00	70.12
<input checked="" type="checkbox"/> OC4J_SECURITY	↑	Sep 24, 2004 12:56:03 PM	0.03	172.08
<input type="checkbox"/> oca	↑	Sep 24, 2004 12:57:06 PM	0.03	149.19
<input type="checkbox"/> Single_Sign-On.oraasso	↑	N/A	N/A	N/A
<input type="checkbox"/> Management	↑	Sep 24, 2004 12:58:18 PM	0.40	471.45

TIP This table contains only the enabled components of the application server. Only components that have the checkbox enabled can be started or stopped.

Related Links

- [Process Management](#)
- [All Metrics](#)

Using the Command Line

You can issue separate commands to stop and start just the Oracle HTTP Server or the entire single sign-on middle tier. Another command stops and starts just the OC4J_SECURITY instance. Still another command stops and starts all infrastructure components.

Stopping and Starting the Oracle HTTP Server

Issue these two commands to stop and then start the Oracle HTTP Server:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl startproc process-type=HTTP_Server
```

You can also stop and start the server by issuing this command:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
```

Stopping and Starting the OC4J_SECURITY Instance

Issue these two commands to stop and then start the OC4J_SECURITY instance:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=OC4J_SECURITY
ORACLE_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY
```

You can also stop and start the OC4J_SECURITY instance by issuing this command:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

Stopping and Starting the Single Sign-On Middle Tier

To stop and then start the single sign-on middle tier, stop and start both the Oracle HTTP Server and the OC4J_SECURITY instance:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=HTTP_Server
```

```
ORACLE_HOME/opmn/bin/opmnctl startproc process-type=HTTP_Server
```

```
ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=OC4J_SECURITY  
ORACLE_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY
```

You can also stop and start the single sign-on middle tier by issuing these commands:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server  
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

Stopping and Starting All Components

Issue the following commands to stop and then start the Oracle HTTP Server, the single sign-on server, OC4J, and Oracle Internet Directory:

```
ORACLE_HOME/opmn/bin/opmnctl stopall  
ORACLE_HOME/opmn/bin/opmnctl startall
```

This command assumes that infrastructure components are all in the same Oracle home.

Stopping and Starting the Database

If the database needs to be shut down, use the following steps to stop and start affected components including the database:

1. Stop the Oracle HTTP Server, the single sign-on server, OC4J, and Oracle Internet Directory:

```
ORACLE_HOME/opmn/bin/opmnctl stopall
```

2. Shut down the database.
3. Start the database.
4. Start the Oracle HTTP Server, the single sign-on server, OC4J, and Oracle Internet Directory:

```
ORACLE_HOME/opmn/bin/opmnctl startall
```

Troubleshooting an Inaccessible Server

Occasionally OracleAS applications are inaccessible because the single sign-on server is inaccessible. Use these steps to diagnose the problem:

1. Follow the instructions in "[Accessing the Monitoring Pages](#)" in Chapter 10 to access the Application Server page of the Application Server Control console.
2. Verify that the single sign-on server is indeed down by examining the System Components table on the Application Server page. A down-facing red arrow signifies that the server is down, an up-facing green arrow that the server is up.
3. Check the table to determine whether the Oracle HTTP Server is down.
4. If the Oracle HTTP Server is down, restart it using either the command line or the Application Server Control console. See "[Stopping and Starting Single Sign-On Components](#)".
5. If the Oracle HTTP Server fails to start, check the log files for the server to determine the problem. The files are found in `ORACLE_HOME/opmn/logs` and in `ORACLE_HOME/Oracle/Oracle/Logs/error_log`.
6. Check the status of the OracleAS metadata repository:
 - a. Start the Oracle Enterprise Manager Database Control console:

```
ORACLE_HOME/bin/emctl start dbconsole
```

- b. In your browser, enter the URL for Oracle Enterprise Manager Database Control:

```
http://host_name.domain:port/em
```

In the URL, *host_name* is the name of the computer on which the metadata repository is installed. *port* is the port number reserved for Database Control during installation. You can find this number by examining the file *ORACLE_HOME/install/portlist.ini*. Look for this line:

```
Enterprise Manager Console HTTP Port(database_name) = port_number
```

The port number is a value in the range 5500–5519.

7. Log in to the Database Control page with the SYSaccount; then connect as SYSDBA.
8. On the Database Home page, examine the status indicator in the General section. If the database is up, continue to step 10. If the database is down, click the Startup button—or, when appropriate—the Perform Recovery button.

If the database starts, restart the Application Server Control console, the Database Control console, the infrastructure middle tier, and middle tiers associated with the metadata repository installation. If you need help, see the chapter about starting and stopping in *Oracle Application Server Administrator's Guide*.

If the database fails to start, consult *Oracle Database Administrator's Guide*.

9. Determine whether the OC4J_SECURITY instance is running by examining the System Components table on the Application Server page of the Application Server Control Console. Or use the command line for this purpose:

```
opmnctl status
```

If the OC4J_SECURITY instance is down, restart it by using the Application Server Control console. If OC4J_SECURITY starts successfully, see if the single sign-on server is accessible. If OC4J_SECURITY fails to start, check the OC4J_Security logs for errors. See "[Viewing the Log Files](#)" in [Appendix A](#) for more about these logs.

10. Check the status of Oracle Internet Directory, using the same procedures that you used to check the status of the OC4J_SECURITY instance in step 10. Use the Application Server Control console to start the directory if necessary. If the directory fails to start, check directory error logs.

Setting Browser Preferences for OracleAS Single Sign-On

Logging in and out of OracleAS Single Sign-On successfully requires that the following browser settings be in place:

Cache Settings

To enable the correct cache settings:

1. Go to the cache settings dialog box by clicking the following in succession:
 - Internet Explorer:
 - Tools
 - Internet Options

- General
 - Settings
 - Netscape Communicator:
 - Edit
 - Preferences
 - Advanced
 - Cache
2. Select **Every visit to the page** in Internet Explorer or **Every time** in Netscape Communicator.

Image Settings

To ensure that images are automatically loaded:

1. Click the following in succession:
 - Internet Explorer:
 - Tools
 - Internet Options
 - Advanced
 - Netscape Communicator:
 - Edit
 - Preference
 - Advanced
2. Select **Show pictures** in Internet Explorer or **Automatically load images** in Netscape Communicator.

Accessing the Administration Pages

You can use the administration pages within the single sign-on UI to set the single sign-on session length and to enable the server to verify IP addresses. You can also use these pages to administer partner applications and external applications.

To access the administration pages:

1. Enter a URL of the following form:

`http://host:port/sso`

where *host* is the name of computer on which the server is located and *port* is the port number of the server. If the server is enabled for SSL, `https` must be substituted for `http`. The port number may be omitted if it is 80 or 443 (SSL) because these numbers are the defaults.

The **Access Partner Applications** page appears.

2. Click **Login** in the upper right corner of the **Access Partner Applications** page.
The login page appears.
3. Enter the administrator's user name and password; then click **Login**.

4. The home page appears. To perform administrative functions, click **SSO Server Administration**.

Figure 2–3 shows the **SSO Server Administration** page.

Figure 2–3 SSO Server Administration Page



Using the Edit Single Sign-On Server Page to Configure the Server

Use the Edit Single Sign-On Server page to fix the length of single sign-on sessions and to verify IP addresses. To access the Edit Single Sign-On Server page, click **Edit Single Sign-On Server Configuration** on the SSO Server Administration page.

The Edit Single Sign-On Server page contains the following heading and fields:

Table 2–1 Single Sign-On Session Policy

Field	Description
Single sign-on session duration	Enter the number of hours users can be logged in to the server before their session expires. The default is eight hours.
Verify IP addresses for requests made to the single sign-on server	Select to verify that the IP address of the browser is the same as the IP address in the authentication request. This check box is not selected by default.

If you change either of these parameters, restart the OC4J_SECURITY instance:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

Configuring Globalization Support

When installed, OracleAS Single Sign-On product supports dozens of languages. The default language is English, but users can set their browser preferences to any of the supported languages.

For a complete list of the language codes supported, see Appendix A in *Oracle Application Server Globalization Guide* at the following URL:

<http://www.oracle.com/technology/documentation/index.html>

From the landing page for the URL, click a link for the OracleAS Single-Sign on documentation, then click the View Library link to view the library for the appropriate release.

Configuring the Global User Inactivity Timeout

Before reading this section, read "Global User Inactivity Timeout" in Chapter 1, "Components and Processes: an Overview."

The global user inactivity timeout is applicable to one domain only. This means that computers enabled for the timeout must reside in the same cookie domain. The applications on these computers use the domain cookie to track user activity. If, for example, you use `login.acme.com` for the single sign on server, other computers in the system must have the `.acme.com` domain in their host name. One of these computers might be `host1.acme.com`. Another might be `host2.acme.com`. In addition, clocks on all of these computers, including the single sign-on server computer, must be synchronized with 10 seconds of one another.

The global user inactivity timeout is not configured by default. You must enable it by running the `ssogito.sql` script. The script is found at `ORACLE_HOME/sso/admin/plsql/sso`. The steps that follow include an example of `ssogito.sql`.

To configure the global user inactivity timeout:

1. Log in to SQL*Plus, using the single sign-on schema name and password. The default schema name is `orasso`. To obtain the password, see [Appendix B](#).
2. Run `ssogito.sql` by entering the following command:

```
SQL> @ssogito.sql
```

A list of fields appears.

3. In the **Enter value for timeout_cookie_domain field**, enter a domain name that is common to all of the applications enabled by the single sign-on server. Be sure to place a period before the domain name.

Note: If this field is left blank, the domain name defaults to the host name of the single sign-on server.

4. In the **Enter value for inactivity period field**, enter the length of the desired inactivity period in minutes.
5. To enable the new settings, press the **Return** or **Enter** key. To cancel the transaction, press the **Return** or **Enter** key twice.

Once you have completed a transaction, the script provides you with a summary of the new timeout settings. Here is an example of `ssogito.sql`:

```
SQL> @ssogito
=====
SSO Server Inactivity Timeout Configuration
=====
Timeout           : DISABLED
```

```

Cookie name      : OSSO_USER_CTX
Cookie domain    :
Inactivity period: 15 minutes
Encryption key   : 093D678526DAA66D
Note: timeout cookie domain will be defaulted
to the SSO Server hostname
-----
To disable timeout set inactivity period to 0, (zero)
Press return key twice if you do not want
to change timeout configuration.

```

PL/SQL procedure successfully completed.

```

Enter value for timeout_cookie_domain: .oracle.com
Enter value for inactivity_period: 15
Timeout                : ENABLED
New timeout cookie domain: .oracle.com
New inactivity period  : 15 minutes

```

PL/SQL procedure successfully completed.

No errors.

6. Restart the single sign-on middle tier:

```

ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl startproc process-type=HTTP_Server

```

```

ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=OC4J_SECURITY
ORACLE_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY

```

7. On the application middle tiers where the inactivity timeout is to be enabled, edit the `mod_osso.conf` file. Make sure that the `OssoIdleTimeout` parameter exists and that it is set to `on`. The file is at `ORACLE_HOME/Apache/Apache/conf`. Here is an example file with the correct setting:

```

LoadModule osso_module libexec/mod_osso.so
<IfModule mod_osso.c>
    OssoIpCheck off
    OssoIdleTimeout on
    OssoConfigFile /u01/oracleas10g/Apache/Apache/conf/osso/osso.conf
#
#Insert Protected Resources
#
.
.
.
</IfModule>

```

8. Restart the Oracle HTTP Server on the application middle tiers.

```

ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server

```

If Oracle Delegated Administration Services and the single sign-on server are located on the same middle tier, and you want the global user inactivity timeout to apply to the former, perform steps seven and eight on the single sign-on middle tier.

Obtaining the Sample Files

The `ipassample.jar` file contains sample code for single sign-on features such as certificate-enabled sign-on and deployment-specific pages. Use this command to extract the file:

```
ORACLE_HOME/jdk/bin/jar -xvf ORACLE_HOME/sso/lib/ipassample.jar
```

Directory-Enabled Single Sign-On

This chapter examines those aspects of OracleAS Single Sign-On that are dependent upon Oracle Internet Directory. The directory is the repository for all single sign-on user accounts and passwords—administrative and nonadministrative. All user and group management functions are handled by the directory.

Note: Oracle Internet Directory can be configured to authenticate to third-party repositories. To learn more, see *Oracle Identity Management Integration Guide*.

The chapter contains the following topics:

- [Managing Users in Oracle Internet Directory](#)
- [Password Policies](#)
- [Directory Tree for OracleAS Single Sign-On](#)
- [Changing Single Sign-On Server Settings for Directory Access](#)
- [Updating the Single Sign-On Server with Directory Changes](#)

Managing Users in Oracle Internet Directory

Use the following tools to manage single sign-on users:

- Oracle Delegated Administration Services

Oracle Delegated Administration Services is a self-service application that enables administrators to manage users and groups. For example, you can create and delete users and change passwords.

You can access Oracle Delegated Administration Services with a URL of this form:

`http://host:port/oiddas/`

where *host* is the name of the computer on which the Oracle Delegated Administration Services server is located, and *port* is the port number of the server. In a typical infrastructure installation, Oracle Delegated Administration Services and OracleAS Single Sign-On have the same host name.

- Oracle Directory Manager

Oracle Directory Manager is a Java-based tool for managing most functions in Oracle Internet Directory. Use it to configure password policies.

- LDAP Command-Line Tools

You can use command-line tools like `ldapmodify` in place of Oracle Delegated Administration Services and Oracle Directory Manager. These tools operate on text files. They take arguments that use the Lightweight Directory Interchange Format.

Password Policies

The single sign-on user password is stored in Oracle Internet Directory as an attribute of the user's entry. Users can change their passwords in the single sign-on UI only when their passwords are about to expire. They may use Oracle Delegated Administration Services for this purpose at any time. The directory administrator can use Oracle Directory Manager to adjust password expiry behavior to suit enterprise needs.

This section covers the following topics:

- [Password Rules](#)
- [Configuring Password Life](#)
- [Change Password Page Behavior](#)
- [Configuring Account Lockout](#)
- [Unlocking Users](#)
- [Configuring Password Policies](#)

Password Rules

Oracle Directory Manager has fields that enable you to specify the minimum number of characters that a password requires. To learn what the defaults are, see the chapter about password policies in *Oracle Internet Directory Administrator's Guide*.

A password cannot contain the following characters: `&`, `{`, `}`, `<`, `>`, `"`, `'`, `(`, and `)`.

Configuring Password Life

Using either Oracle Directory Manager or LDAP command-line tools, you can configure password life and can specify when users are prompted to change their passwords. You can also configure a grace login period for users. This is a period after which users' passwords have expired. If they neglect to change their passwords within this period, they must have an administrator reset them.

Change Password Page Behavior

Users who try to log in when their passwords have expired or are about to expire experience the following server behavior:

Password Has Expired

Users are shown the password expiry screen. They must contact the directory administrator to have the password reset.

Password Is About to Expire

Users are shown an error message on the login page. They have the option of cancelling the page or changing their passwords. In either case, authentication proceeds in the same manner as it does when the change password page is not thrown.

Grace Login Is in Force

If a grace login period has been configured in the directory, users are presented the change password page after their passwords have expired. They have the option of cancelling the page or changing their passwords. In either case, the authentication sequence is the same as it is for users with valid passwords.

Force Change Password

This feature prompts users to change their password after it has been reset by an administrator. You enable force change password by setting the `pwdMustChange` attribute in the directory entry

```
cn=pwdpolicyentry, cn=common, cn=products, cn=OracleContext, dc=default_identity_management_realm.
```

You can use the command-line tool `ldapmodify` for this purpose. The value `TRUE` enables this feature. `FALSE` disables it. See the chapter about password policies in *Oracle Internet Directory Administrator's Guide* to learn how to run the tool.

Configuring Account Lockout

An account lockout occurs when users submit the incorrect user name and password combination more times than is permitted by Oracle Internet Directory. Once they are locked out, they are unable to access the single sign-on server from any number of workstations. By default, lockout occurs after 10 login attempts. Once this limit has been reached, even a valid user name and password combination fails to log a user in.

Because single sign-on user accounts are managed in the directory, the directory administrator determines account lockout policies. Oracle Directory Manager has fields for enabling and disabling lockout and for specifying lockout duration.

The default lockout duration is one day.

Unlocking Users

To learn how to unlock users, see the chapter about password policies in *Oracle Internet Directory Administrator's Guide*.

Configuring Password Policies

To learn how to configure password policies, see the chapter about these policies in *Oracle Internet Directory Administrator's Guide*.

Directory Tree for OracleAS Single Sign-On

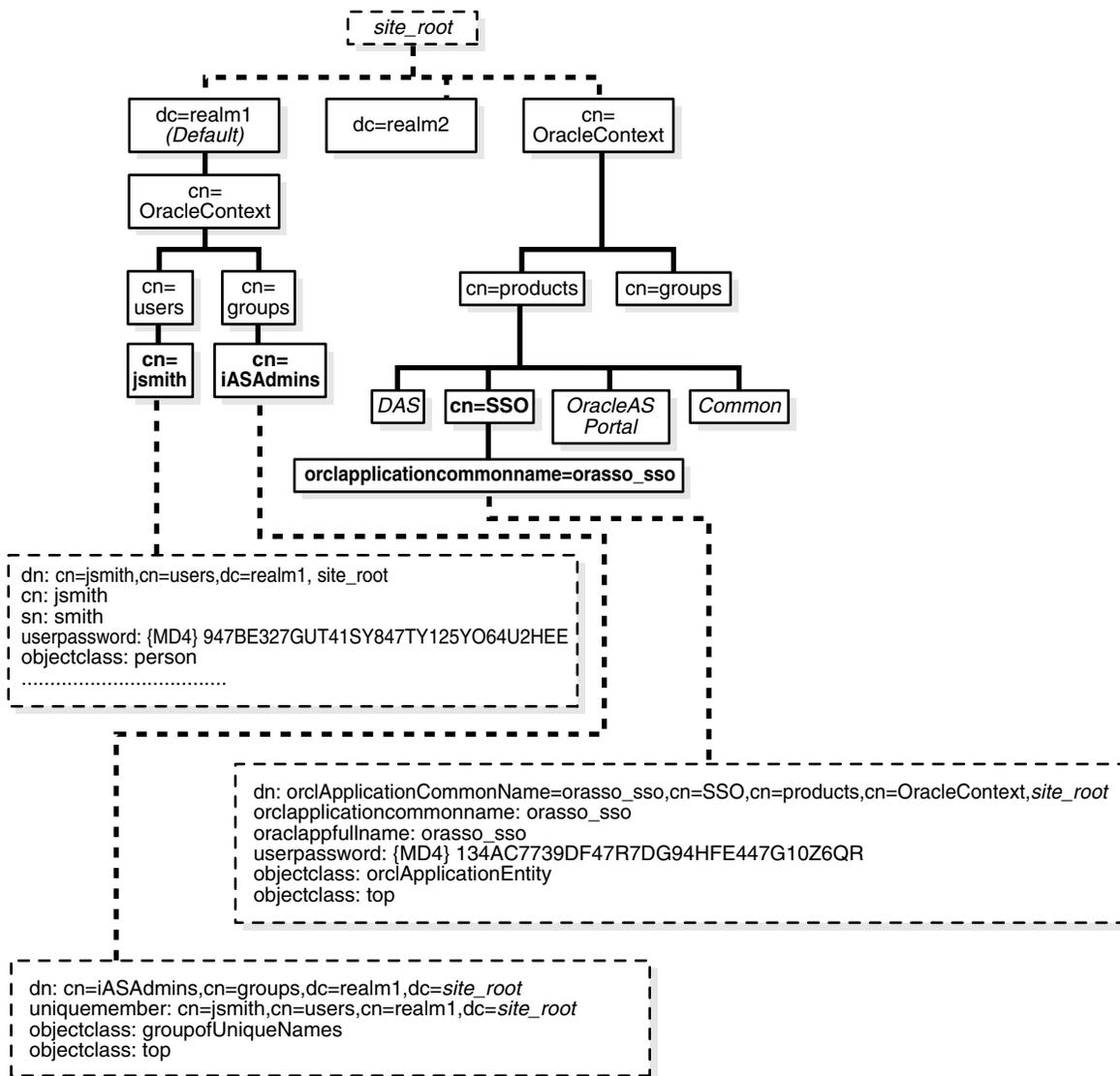
OracleAS Single Sign-On, like other components in the OracleAS complement, has its own container in the directory information tree (DIT). This container is in the Oracle Context, an entry that serves as the root for all Oracle-specific data. In the simplified DIT shown in [Figure 3-1](#) on page 3-4, both the root Oracle Context and the realm-specific Oracle Context are expanded. The root Oracle Context is the repository for sitewide information—that is, information that applies to all identity management realms and products. Structurally, realm-specific Oracle Contexts are mirror images of the root context, but the information they contain pertains only to a particular realm. These realms store configuration information unique to specific users and other network entities. To learn more about realms, see [Chapter 10, "Enabling Support for Application Service Providers"](#).

In [Figure 3-1](#), the single sign-on container is identified by the entry `cn=SSO`. It contains a single entry, `orclApplicationCommonName=orasso_sso`. This is the

entry for the single sign-on server. In the illustration, the entry has been expanded to show the object classes and attributes that define the entry. For example, the `orclapplicationcommonname` attribute gives the default name of the single sign-on server, `orasso`. Note, too, that the single sign-on server has its own password, which, along with `orclapplicationcommonname`, the directory server uses to authenticate the single sign-on server when the latter performs user searches.

The container `Common` is a repository for information common to all OracleAS products. For instance, it contains attributes that enable products to identify the realm search base, or node, and the realm nickname. Realm-specific `Common` containers—not shown here—contain attributes that enable products to locate users within a realm subtree. In addition to expanding the `SSO` container, the illustration expands entries for an OracleAS user who is also an administrator.

Figure 3-1 Directory Information Tree for OracleAS Single Sign-On



Changing Single Sign-On Server Settings for Directory Access

The `ssooconf.sql` script enables you to change the following settings in the directory:

- directory host name
- directory port
- password for single sign-on server
- SSL connections to the directory

Note: You can change the host name and port number only if the new instance of Oracle Internet Directory is a replicated instance.

To change directory settings for the single sign-on server:

1. Navigate to the script at `ORACLE_HOME/sso/admin/plsql/sso`.
2. Log in to SQL*Plus as the schema `orasso`. To obtain the schema password, see [Appendix B](#).

Note: You can run the script only as `orasso`.

3. Run `ssooconf.sql` by issuing the following command:

```
SQL> @ssooconf.sql
```

This prompt appears:

```
Enter value for new_oid_host
```

4. Enter a value for the directory host name; then press **Return** or **Enter**. If, on the other hand, you do not want to change the directory host name, simply press **Return** or **Enter** to move to the next prompt.
5. Repeat step 4 for each of the remaining three prompts, which are `Enter value for new_oid_port`, `Enter value for new_ssoserver_password`, and `Enter value for new_ldapussl`. The last requires that you enter either **Y** (enable) or **N** (disable).

Note: An SSL connection between the single sign-on server and the directory exists by default.

6. To apply the changes, press **Return** or **Enter** one last time.

The script displays updated settings for the single sign-on server along with the old ones.

If you run the script and then decide not to make changes, press **Return** or **Enter** to retain existing values.

Updating the Single Sign-On Server with Directory Changes

The single sign-on server caches metadata about the Oracle Internet Directory DIT. This metadata includes the user search base, user nickname attribute, and

realm-related metadata. In the event that the directory DIT changes, the cache for the single sign-on server must be refreshed. This is effected by running the `ssoreoid.sql` script.

1. Navigate to the script at `ORACLE_HOME/sso/admin/plsql/sso`.

2. Log in to the single sign-on schema:

```
SQL> connect orasso/orasso_password
```

See [Appendix B](#) to obtain the `orasso` schema password.

Note: This script cannot be run as `sys`.

3. Run the script:

```
SQL> @ssoreoid.sql
```

4. Restart the single sign-on server.

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server  
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

These are just a few of the DIT changes that require that the script be run:

- The default realm name or realm DN changes or both change
- A new default realm is created
- The user search base or group search base for the default realm changes or both change
- The user nickname attribute changes

To learn how realm information is changed in Oracle Internet Directory, see *Oracle Internet Directory Administrator's Guide*.

Configuring and Administering Partner Applications

This chapter explains how to enable partner applications for single sign-on. This process involves registering the authentication module `mod_osso` with the single sign-on server. See [Chapter 1](#) for more about `mod_osso` and partner applications.

The chapter contains the following topics:

- [Registering a Partner Application: What It Means](#)
- [Registering `mod_osso`](#)
- [Deploying Multiple Partner Applications with a Load Balancer](#)
- [Configuring `mod_osso` with Virtual Hosts \(SSL and non-SSL\)](#)

Registering a Partner Application: What It Means

Single sign-on partner applications are integrated with `mod_osso`, which is registered automatically by the OracleAS installer. In essence, partner applications are registered *by way* of `mod_osso`. Registering the module creates an entry for it in the identity management infrastructure database as well as on the application computer.

`mod_osso`-integrated applications are registered either by the `ssoreg.sh` script or by the `ssoreg.bat` batch file, depending upon whether the platform is UNIX or Windows. OracleAS Portal, an application enabled for single sign-on not by `mod_osso` but by an SDK, is registered by the `ptlconfig` script. All three tools are invoked by the installer. Only `ssoreg.sh` and `ssoreg.bat` are discussed here. To learn how to use `ptlconfig`, see the appendix devoted to this tool in *Oracle Application Server Portal Configuration Guide*.

Registering `mod_osso`

Under certain circumstances, you must reregister `mod_osso` manually, using the single sign-on registration tool. For instance, the host name and port number of the Oracle HTTP Server on either the infrastructure or the application tier may change after OracleAS is installed. Or SSL may be enabled after installation.

Running the single sign-on registration tool updates the `mod_osso` registration record in `osso.conf`. The tool generates this file whenever it runs.

This section contains the following topics:

- [Syntax and Parameters for `ssoreg`](#)
- [Command Example](#)

- [Restarting the Oracle HTTP Server](#)

Syntax and Parameters for ssoreg

The `ssoreg.sh` and `ssoreg.bat` scripts share the same parameters. The syntax for both commands is provided here. Before running the script, set the `ORACLE_HOME` environment variable to point to the directory where OracleAS is installed. See the section "[Command Example](#)" if you need help. In the example, the home directory is called `gitml`.

Here is the command:

- UNIX:

```
$ORACLE_HOME/sso/bin/ssoreg.sh
-oracle_home_path orcl_home_path
-site_name site_name
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
[-virtualhost]
[-update_mode CREATE | DELETE | MODIFY]
[-remote_midtier]
[-config_file config_file_path]
[-admin_info admin_info]
[-admin_id adminid]
```

- Windows:

```
%ORACLE_HOME%\sso\bin\ssoreg.bat
-oracle_home_path orcl_home_path
-site_name site_name
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
[-virtualhost]
[-update_mode CREATE | DELETE | MODIFY]
[-remote_midtier]
[-config_file config_file_path]
[-admin_info admin_info]
[-admin_id adminid]
```

oracle_home_path

Absolute path to the Oracle home.

site_name

Name of the site—typically, the effective host name and port of the partner application. For example, `application.mydomain.com`.

config_mod_osso

If set to `TRUE`, this parameter indicates that the application being registered is `mod_osso`. You must include `config_mod_osso` for `osso.conf` to be generated.

mod_osso_url

The effective URL of the partner application. This is the URL that is used to access the partner application. The value should be specified in this URL format:

```
http://oracle_http_host.domain:port
```

For example:

`http://application.mydomain.com:7777`

Omit the port number if the partner Oracle HTTP Server is listening on the default HTTP port of 80 or on the default HTTPS port of 443.

virtualhost

Optional. Include this parameter only if you are registering an Oracle HTTP virtual host with the single sign-on server. Omit the parameter if you are not registering a virtual host.

If you are creating an HTTP virtual host, use the `httpd.conf` file to fill in the following directive for each protected URL:

```
<VirtualHost host_name>
    OssoConfigFile $ORACLE_HOME/Apache/Apache/conf/osso/host_name/osso.conf
    OssoIpCheck off
    #<Location /your_protectedORACLE_HOME_url>
    # AuthType basic
    #   Require valid-user
    #</Location>
    #Other configuration information for the virtual host
</VirtualHost>
```

If, on the other hand, you are creating an HTTPS virtual host, use the `ssl.conf` file to fill in the same directive. Note that the commented lines must be uncommented before the application is deployed. Both `httpd.conf` and `ssl.conf` are in `ORACLE_HOME/Apache/Apache/conf`.

After creating a virtual host, run this command to update the Distributed Cluster Management schema:

```
ORACLE_HOME/dcm/bin/dcmctl updateConfig -v -d
```

update_mode

Optional. Creates, deletes, or modifies the partner registration record. `CREATE`, the default, generates a new record. `DELETE` removes the existing record. `MODIFY` deletes the existing record and then creates a new one.

remote_midtier

Specifies that the `mod_osso` partner application to be registered is at a remote midtier. Specify this option only when the `mod_osso` partner application to be configured is at a different `ORACLE_HOME`, and the OracleAS Single Sign-On server runs locally at the current `ORACLE_HOME`.

config_file

Location of the `osso.conf` file. The path is typically in the form of `<ORACLE_HOME_PATH>/Apache/Apache/conf/osso/<filename>` or a subdirectory under it. This parameter is optional **except** when `-virtualhost` or `-remote_midtier` is specified.

- when `-virtualhost` is specified, this is the location of the `osso.conf` file for the virtual host if one is being configured.

For example, it may be specified as the following:

```
ORACLE_HOME/Apache/Apache/conf/osso/virtual_host_
name/osso.conf.
```

This parameter is mandatory if you are registering a virtual host. If you omit `config_file`, the assumption is that you are registering a nonvirtual host. In this case, `ssoreg` creates a file with the name `osso.conf` in `ORACLE_HOME/Apache/Apache/conf/osso`.

- when `-remote_midtier` is specified, the partner application is at a remote midtier. The resulting `osso.conf` configuration file can then be copied or sent using `ftp` to the remote midtier.

admin_info

Optional. User name of the `mod_osso` administrator. If you omit this parameter, the Administrator Information field on the Edit Partner Application page is left blank.

admin_id

Optional. Any additional information, such as email address, about the administrator. If you omit this parameter, the Administrator E-mail field on the Edit Partner Application page is left blank.

Command Example

This command sequence that follows shows a `mod_osso` instance being reregistered with the single sign-on server. In the example, the Oracle home is a directory called `gitml`

- UNIX (csh and tcsh):

```
setenv ORACLE_HOME /private/oracle/gitml
```

```

$ORACLE_HOME/sso/bin/ssoreg.sh
-oracle_home_path $ORACLE_HOME
-site_name myhost.mydomain.com
-config_mod_osso TRUE
-mod_osso_url http://myhost.mydomain.com
```

- UNIX (Bourne and ksh)

```
ORACLE_HOME=/private/oracle/gitml; export ORACLE_HOME
```

```

$ORACLE_HOME/sso/bin/ssoreg.sh
-oracle_home_path $ORACLE_HOME
-site_name myhost.mydomain.com
-config_mod_osso TRUE
-mod_osso_url http://myhost.mydomain.com
```

- Windows:

```
set ORACLE_HOME=c:\private\oracle\gitml

%ORACLE_HOME%\sso\bin\ssoreg.bat
-oracle_home_path %ORACLE_HOME%
-site_name myhost.mydomain.com
-config_mod_osso TRUE
-mod_osso_url http://myhost.mydomain.com
```

Restarting the Oracle HTTP Server

After running `ssoreg`, restart the Oracle HTTP Server:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
```

Deploying Multiple Partner Applications with a Load Balancer

You can configure two or more partner application instances in a highly available deployment by placing a load balancer in front of them. The load balancer publishes a single address for partner applications while providing a farm of application servers that actually service requests. The HTTP load balancer can detect when one of the Oracle HTTP Server instances has failed and can then fail over requests to another instance.

The usage scenario presented here takes you through the steps required to configure partner applications with a load balancer.

Usage Scenario

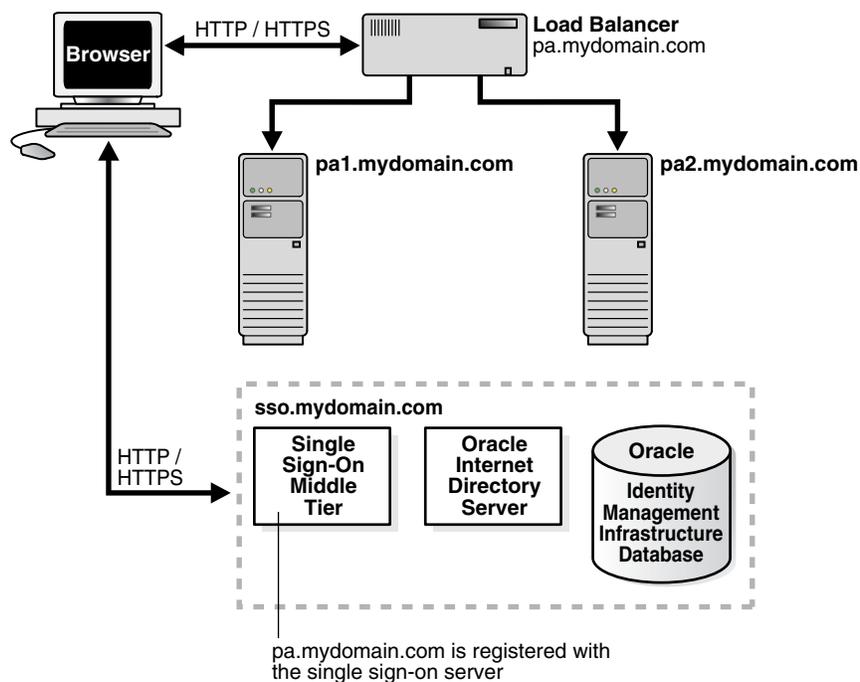
This scenario assumes the following hypothetical configurations:

- There are two partner application computers: `pa1.mydomain.com` and `pa2.mydomain.com`. Both application servers listen on non-SSL port 7777.
- The partner application computers are configured to use the single sign-on server located at `sso.mydomain.com`.
- The effective host name of the partner application published to users is `pa.mydomain.com`. An HTTP load balancer is configured to listen at this address, on port 80. It load balances and fails over user requests between `pa1.mydomain.com` and `pa2.mydomain.com`.
- The single sign-on server, directory server, and identity management infrastructure database are located at `sso.mydomain.com`.

Note:

- In this scenario, the load balancer is listening on port 80, a non-SSL port number. If the load balancer is configured to use SSL to interact with the browser, a different port number must be selected. The default SSL port number is 443.
 - Two partner application computers are deployed. There can, in fact, be any number of them.
 - The host names presented are examples only. These names may not work in an actual implementation. Substitute values that apply to your installation.
-
-

Figure 4–1 shows what this hypothetical system looks like.

Figure 4–1 Load Balancer with Multiple Partner Applications

Configuration Steps

Setting up the system depicted in [Figure 4–1](#) involves the following tasks:

- [Installing the Partner Applications](#)
- [Configuring the Oracle HTTP Servers on the Partner Application Middle Tiers](#)
- [Configuring the HTTP Load Balancer](#)
- [Reregistering mod_osso on the Partner Application Middle Tiers](#)

Installing the Partner Applications

Install the partner applications on `pa1.mydomain.com` and `pa2.mydomain.com`. When prompted by the installer for a directory location, choose the server located at `sso.mydomain.com`.

Note: The partner application mentioned here can be any Web-based application. In a simple case, it can be an OracleAS core installation that includes the Oracle HTTP Server and OC4J. Consult application-specific installation documentation.

Configuring the Oracle HTTP Servers on the Partner Application Middle Tiers

When a load balancer is placed between the user and the Oracle HTTP servers on the OracleAS middle tier, the effective URL of the partner application changes. The configuration file `httpd.conf` on both middle tiers must be modified to reflect this change. This file is found at `ORACLE_HOME/Apache/Apache/conf`.

Complete the following steps:

1. Modify the Oracle HTTP servers at the OracleAS middle tier to listen at the externally published name, which, in the scenario presented, is `pa.mydomain.com`.

Add the following lines to the `httpd.conf` file on `pa1.mydomain.com` and `pa2.mydomain.com`:

```
ServerName pa.mydomain.com
Port 80
```

Note: If multiple ports are listed in `httpd.conf`, the effective port must appear last.

2. If you configure SSL between the browser and the load balancer, and the SSL connection terminates at the load balancer, configure `mod_certheaders` on both `pa1.mydomain.com` and `pa2.mydomain.com`. This module enables the Oracle HTTP Server to treat requests that it receives over HTTP as SSL requests. Add the lines that follow to `httpd.conf`. You can place them at the end of the file. Where they appear is unimportant.

- a. Enter this line to load the module:

```
LoadModule certheaders_module libexec/mod_certheaders.so
```

- b. If you are using OracleAS Web Cache as a load balancer, enter this line:

```
AddCertHeader HTTPS
```

If you are using a hardware load balancer, enter this line:

```
SimulateHttps on
```

Configuring the HTTP Load Balancer

The HTTP load balancer that you use can be either hardware or software. If you elect to use the latter, you can use OracleAS WebCache.

- Hardware Load Balancer

If you use a hardware load balancer, configure one pool of real servers with the addresses `pa1.mydomain.com` and `pa2.mydomain.com`. Configure one virtual server with the address `pa.mydomain.com`. This virtual server is the external interface of the load balancer. For instructions, consult the documentation provided by your load balancer vendor.

- Software Load Balancer

If you use OracleAS Web Cache to load balance connection requests, see the following documents:

- "Leveraging Oracle Identity Management Infrastructure" in *Oracle Application Server Web Cache Administrator's Guide*.
- "Routing Single Sign-On Server Requests," also in *Oracle Application Server Web Cache Administrator's Guide*.

Note: For optimal performance, use a hardware load balancer.

Reregistering mod_osso on the Partner Application Middle Tiers

On both partner application instances, reregister mod_osso as the partner application pa.mydomain.com.

To reregister mod_osso on pa1.mydomain.com, run ssoreg, the registration script. See "Registering mod_osso" earlier in the chapter to learn how to run the script. Following the example, the script creates a partner application called pa.mydomain.com.

Note: If you are configuring the partner application computers for Distributed Cluster Management, omit the remaining steps. Instead, run this command on pa1.mydomain.com:

```
ORACLE_HOME/dcm/bin/dcmctl updateConfig -v -d
```

This command saves your changes to the Distributed Cluster Management repository, which serves as a backup facility for OracleAS configuration files.

To reregister mod_osso on pa2.mydomain.com:

1. On pa2.mydomain.com, log in to the single sign-on administration pages as the single sign-on administrator. Be sure to log in to this URL:

```
http://sso.mydomain.com/sso
```

2. Use the Administer Partner Applications page to delete the existing entry for the partner application pa2.mydomain.com.
3. Copy the osso.conf file from pa1.mydomain.com. Make sure that you use binary mode if you FTP the file. The default location of the file is `ORACLE_HOME/Oracle/Oracle/conf/osso`.
4. Synchronize the Distributed Cluster Management repository with the file copy. You do this by running the following command on pa2.mydomain.com:

```
ORACLE_HOME/Oracle/Oracle/bin/ssotransfer ORACLE_
HOME/Oracle/Oracle/conf/osso/osso.conf
```

Note: The ssotransfer command should not be used to synchronize the Distributed Cluster Management repository with the mod_osso configuration file created for a virtual host. To learn how to register mod_osso for a virtual host, see "Configuring mod_osso with Virtual Hosts (SSL and non-SSL)".

5. Restart the Oracle HTTP Server:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
```

6. Test the partner application, using the effective URL:

```
http://pa.mydomain.com
```

For more information about integrating partner applications with mod_osso, see the chapter about developing applications for single sign-on in *Oracle Identity Management Application Developer's Guide*.

Configuring mod_osso with Virtual Hosts (SSL and non-SSL)

Some deployments may require more than one Web site to be deployed on a single Oracle HTTP Server.

In the scenario that follows, an SSL virtual host is configured to be protected by mod_osso. Although the virtual host is an SSL host, the scenario applies to any virtual host.

The scenario assumes the following conditions:

- The host name of the application middle tier is `app.mydomain.com`.
- The middle tier is already configured as a non-SSL partner application. This is typically done by the OracleAS Installer when the application is first installed.
- The default SSL port number of the application middle tier is 4443.

To configure `app.mydomain.com` as an SSL virtual host:

1. Make sure that Oracle Identity Management components are up and running—especially Oracle Internet Directory and the single sign-on server.
2. Check that `app.mydomain.com` has been defined as an SSL virtual host. The OracleAS installer does this in the `Virtual Host Context` section of the `ssl.conf` file. The file is in `ORACLE_HOME/Apache/Apache/conf`.
3. Create a partner application for the SSL site:
 - a. Make sure that the Oracle home of the middle tier is set with the correct path. If you need help, see the command examples in the section "[Registering mod_osso](#)".
 - b. Run this command on the middle tier:

– UNIX:

```
$ORACLE_HOME/sso/bin/ssoreg.sh
-oracle_home_path $ORACLE_HOME
-site_name app.mydomain.com
-config_mod_osso TRUE
-mod_osso_url https://app.mydomain.com:4443
-virtualhost
-config_file $ORACLE_HOME/Apache/Apache/conf/osso/osso-https.conf
```

– Windows:

```
%ORACLE_HOME%\sso\bin\ssoreg.bat
-oracle_home_path %ORACLE_HOME%
-site_name app.mydomain.com
-config_mod_osso TRUE
-mod_osso_url https://app.mydomain.com:4443
-virtualhost
-config_file $ORACLE_HOME/Apache/Apache/conf/osso/osso-https.conf
```

4. Go to the `mod_osso.conf` file at `ORACLE_HOME/Apache/Apache/conf`. Once there, comment this directive:

■ UNIX:

```
LoadModule osso_module libexec/mod_osso.so
```

■ Windows:

```
LoadModule osso_module modules\ApacheModuleOsso.dll
AddModule mod_osso.c
```

5. In `httpd.conf`, found in the `conf` directory, add the directive that you just commented in the preceding step. In a default setup, place the directive right after `LoadModule wchandshake_module libexec/mod_wchandshake.so`.

6. Restart the Oracle HTTP server:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
```

7. In `ssl.conf`, which is also in the `conf` directory, update `VirtualHost` to include the `osso.conf` file for the virtual host. Name the file `osso-https.conf` to avoid conflict with the default `osso.conf` file. Check that the file name matches the name used in the registration script.

```
<VirtualHost _default_:4443>
.
.
.
OssConfigFile ORACLE_HOME/Apache/Apache/conf/osso/osso-https.conf
OssIpCheck off
<Location /your_protected_url_for_the_virtual_site>
    AuthType basic
    Require valid-user
</Location>
.
.
.
</VirtualHost>
```

8. Update the Distributed Cluster Management Repository:

```
ORACLE_HOME/dcm/bin/dcmctl updateConfig -v -d
```

9. Restart the Oracle HTTP Server on the application middle tier:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
```

10. Test both the SSL and the non-SSL site.

Configuring and Administering External Applications

This chapter describes how to configure external applications for single sign-on support. These are Web applications that are not modified to delegate authentication to the single sign-on server. Configuring a Web application as an external application enables it to be single sign-on enabled without having to change its interface. See "External Applications" in [Chapter 1](#) for more about these applications.

The chapter contains the following topics:

- [Using the Interface to Deploy and Manage External Applications](#)
- [Proxy Authentication for Basic Authentication Applications](#)

Using the Interface to Deploy and Manage External Applications

The Administer External Applications page, accessible as a link on the SSO Server Administration page, is used to add, edit, or delete external applications. Once you add these applications, users can access them in the External Applications portlet of OracleAS Portal. This portlet can be added to your Portal page after OracleAS is installed. See the chapter about viewing and customizing pages in *Oracle Application Server Portal User's Guide*.

This section covers the following topics:

- [Adding an External Application](#)
- [Editing an External Application](#)
- [Storing External Application Credentials in the Single Sign-On Database](#)

Adding an External Application

From the Single Sign-On Server Administration page, clicking the Administer External Applications link, then clicking Add External Application link takes you to the Add External Applications page. This page contains the following headings and fields:

Table 5–1 External Application Login

Field	Description
Application Name	Enter a name that identifies the external application. This is the default name for the external application.
Login URL	Enter the URL to which the HTML login page for the external application is submitted for authentication. This, for example, is the login URL for Yahoo! Mail: <code>http://login.yahoo.com/config/login?6p4f5s403j3h0</code>
Username/ID Field Name	Enter the term that identifies the user name or user ID field of the HTML login form for the application. You find this term by viewing the HTML source of the form. (See the example after the steps immediately following). This field is not applicable if you are using basic authentication.
Password Field Name	Enter the term that identifies the password field of the HTML login form for the application. You find this term by viewing the HTML source of the form. (See the example after the steps immediately following). This field is not applicable if you are using basic authentication.

Table 5–2 Authentication Method

Field	Description
Type of Authentication Use	<p>Use the pulldown menu to select the form submission method for the application. This method specifies how message data is sent by the browser. You find this term by viewing the HTML source for the login form. Select one of the following three methods:</p> <p>POST: Posts data to the single sign-on server and submits login credentials within the body of the form.</p> <p>GET: Presents a page request to a server, submitting the login credentials as part of the login URL.</p> <p>Basic authentication: Submits the login credentials in the application URL, which is protected by HTTP basic authentication.</p> <p>Notes:</p> <ul style="list-style-type: none"> ■ Basic authentication uses pop-up windows, which by default are blocked by Windows XP, service pack 2. If you use this service pack, make sure that you reconfigure browser settings to display the window for the single sign-on login page. Use the pop-up blocker item in the Tools menu of Internet Explorer. Other browsers and browser plugins are able to block popups. Mozilla is one of these. Make sure that these do not block the single sign-on login page. ■ If you use Internet Explorer 5.0 or a later version, basic authentication may not work with external applications. This version of Internet Explorer includes Microsoft MS04-004 Cumulative Security Update (832894). See this link for a workaround: <code>http://support.microsoft.com</code>

Table 5–3 Additional Fields

Field	Description
Field Name	Enter the name of any additional fields on the HTML login form that may require user input to log in. This field is not applicable if you are using basic authentication.
Field Value	Enter a default value for a corresponding field name value, if applicable. This field is not applicable if you are using basic authentication.

To add an external application:

1. From the Administer External Applications page, select **Add External Application**.

The Add External Applications page appears.

2. In the **External Application Login** field, enter the name of the external application and the URL to which the HTML login form is submitted. If you are using basic authentication, enter the protected URL.
3. If the application uses HTTP POST or HTTP GET authentication, in the **User Name/ID Field Name** field, enter the term that identifies the user name or user ID field of the HTML login form.

You can find the name by viewing the HTML source of the login form.

If the application uses the basic authentication method, the **User Name/ID Field Name** field should be empty.

4. If the application uses HTTP POST or HTTP GET authentication, in the **Password Field Name** field, enter the term that identifies the password field of the application.

See the HTML source of the login form.

If the application uses the basic authentication method, the **Password Field Name** field should be empty.

5. In the **Additional Fields** field, enter the name and default values for any additional fields on the HTML login form that may require user input.

If the application uses the basic authentication method, these fields should be empty.

6. Select the **Display to User** check box to allow the default value of an additional field to be changed by the user on the HTML login form.
7. Click **OK**. The new external application appears under the **Edit/Delete External Application** heading on the Administer External Applications page, along with the other external applications.
8. Click the application link to test the login.

The following example shows the source of the values that are used for Yahoo! Mail.

```
<form method=post action="http://login.yahoo.com/config/login?6p4f5s403j3h0"
autocomplete=off name=a>
...
<td><input name=login size=20 maxlength=32></td>
....
<td><input name=passwd type=password size=20 maxlength=32></td>
...
<input type=checkbox name=".persistent" value="Y" >Remember my ID & password
...
</form>
```

The source provides values for the following:

- Login URL :
http://login.yahoo.com/config/login?6p4f5s403j3h0
- Username/ID Field Name: login
- Password Field Name: passwd

- Type of Authentication Used: POST
- Field Name: .persistent Y
- Field Value: [off]

Note: If you change the host name of the AS middle tier, you must manually update the Login URL field for external applications on this middle tier. You do this on the Edit External Applications page, described in the next section.

Editing an External Application

Clicking the pencil icon next to an application takes you to the Edit External Applications page, where you can edit the values that you entered when you added the application. When you are finished editing, click **Apply** to enter the changes and to redisplay the page with the updated values.

Storing External Application Credentials in the Single Sign-On Database

Each external application expects to receive a user name and password each time the user logs in to the application. To enable single sign-on to these applications, users are given the option of storing their credentials in the single sign-on database when they log in.

If single sign-on users are logging in to an external application for the first time, they are presented with the External Application Login page. After entering credentials, they can select the check box **Remember My Login Information for This Application**. If they choose this option, the next time they access the application, the single sign-on server logs in on their behalf.

Figure 5–1 reproduces the External Application Login page.

Figure 5–1 External Application Login Page

The screenshot shows the Oracle Identity Management interface for logging into an external application named 'Yahoo!'. The page has a blue header with the Oracle logo and 'Identity Management' text. Below the header, there is a title bar 'Login - Yahoo!' with a help icon and 'OK' and 'Cancel' buttons. The main content area is titled 'External Application Login' and contains the following text: 'Enter your user name (or other form of application identification) and password for this application. You may also enter custom values for and additional login parameters shown. The Single Sign-On Server uses this information to login on your behalf. If you click Remember My Login Information For This Application, you will then be logged in automatically each time you access this application.' Below this text are three input fields: 'Application Name: Yahoo!' (pre-filled), 'User Name/ID', and 'Password'. At the bottom of the form is a checked checkbox labeled 'Remember My Login Information for this Application' and 'OK' and 'Cancel' buttons.

Note:

- If you change your password, you must also update the password on the External Application Login page. If you neglect to do so, this page returns an error message when you try to log in.
 - Your password cannot contain the following characters: &, {, }, <, >, ", ', (, and).
-

Proxy Authentication for Basic Authentication Applications

The standard way to access external applications enabled by single sign-on is through the External Applications portlet of OracleAS Portal, an SDK-enabled partner application. Applications accessed in this way can be configured for GET, POST, or basic authentication.

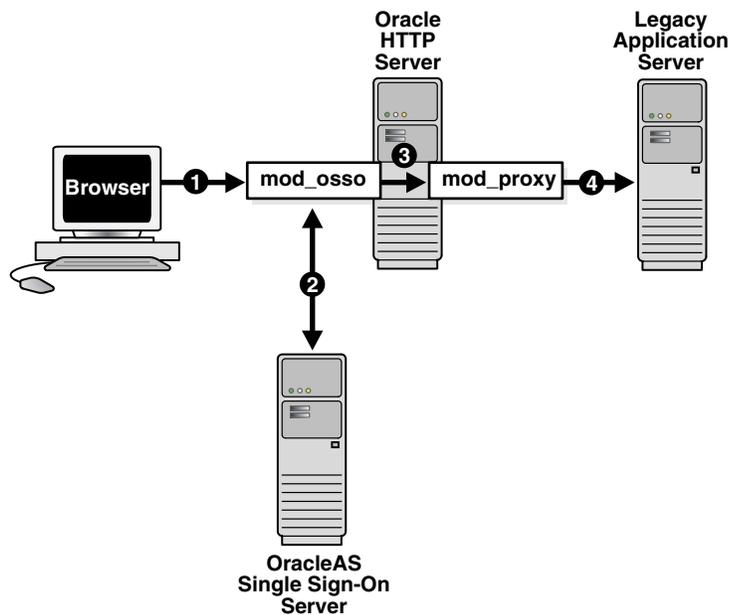
An alternative method is to use the Oracle HTTP Server as a secure proxy for applications that reside on a separate Web server. This method involves configuring the modules `mod_osso` and `mod_proxy` to support single-sign-on-enabled basic authentication. The advantage of the proxy approach is that it eliminates the brief screen flicker that occurs when external applications are accessed in the standard way.

This section contains the following topics:

- [Configuring the Oracle HTTP Server as a Proxy for Basic Authentication](#)
- [Configuration Requirements](#)
- [Configuration Steps](#)

Configuring the Oracle HTTP Server as a Proxy for Basic Authentication

Configured correctly, authentication to `mod_osso`-enabled external applications is similar to what it is for partner applications: `mod_osso` intercepts a URL request and redirects it to the single sign-on server. [Figure 5-2](#) illustrates the process.

Figure 5–2 Authentication Flow Using mod_osso/mod_proxy

1. The single sign-on user requests an external application by selecting a bookmark or by entering a virtual URL. This URL enables the Oracle HTTP Server to intercept the request.
2. mod_osso adds an authentication header to the intercepted request and retrieves the user's credentials from the single sign-on server.
3. mod_osso sets the header value with the user's credentials, retrieved from the single sign-on server. mod_osso then passes this header to mod_proxy.
4. mod_proxy passes the user's credentials—in the form of a basic authentication header—to the real URL. mod_proxy does this by using directives that map the virtual URL to the real URL.

Configuration Requirements

The following criteria must be met before the Oracle HTTP Server can be configured for basic authentication to legacy applications:

- The application to be proxied must be registered as a basic authentication application with the single sign-on server. See ["Adding an External Application"](#) for instructions.
- The Oracle HTTP Server must have mod_osso installed and enabled.
- The Oracle HTTP Server must have the default mod_proxy installed and enabled.
- If the Web server that hosts the external application uses the Oracle HTTP Server as a proxy, the Web server must not have mod_osso enabled.

Configuration Steps

To configure the Oracle HTTP Server for basic authentication to external applications, complete these steps:

1. Add the section that follows to mod_osso.conf on the application tier. The file is at `ORACLE_HOME/Apache/Apache/conf`.

```

<IfModule mod_proxy.c>
<Location /application_virtual_path>
    require valid-user
    AuthType Basic
    OsoLegacyApp on | off
</Location>

ProxyPass /application_virtual_path/ http://host:port/application_real_path/
ProxyPassReverse /application_virtual_path/ http://host:port/application_real_path/
</IfModule>

```

The `OsoLegacyApp` directive indicates whether the protected URL is a legacy application. If the directive is missing or is set to `off`, the code that retrieves the application user name and password from the single sign-on database is not executed. The two `mod_proxy` directives `ProxyPass` and `ProxyPassReverse` map the virtual URL to the real URL.

2. Add this line to `httpd.conf`:

```
Listen 5000
```

This parameter instructs `mod_osso` to use the non-SSL port 5000 to access information about external applications.

3. Restart the Oracle HTTP Server:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
```

4. Update the Distributed Cluster Management schema:

```
ORACLE_HOME/dcm/bin/dcmctl updateConfig -v -d
```

Note:

- The directory where the virtual URL resides need not be specified. For convenience, this URL may consist of only the application name.
 - If SSL is enabled, substitute `https` for `http` in the real URL of the application.
-
-

Multilevel Authentication

This document explains how to configure a single sign-on system that assigns different authentication levels to different partner applications. Such a system enables the administrator to tailor authentication behavior to the security level of the application requested.

The document contains the following topics:

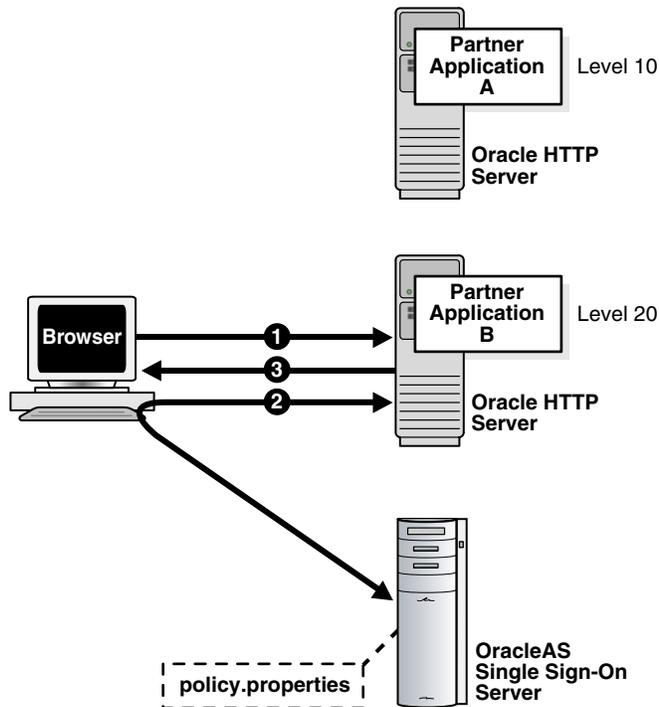
- [What Is Multilevel Authentication?](#)
- [How Multilevel Authentication Works](#)
- [Components of a Multilevel System](#)
- [Configuring Multilevel Authentication](#)

What Is Multilevel Authentication?

OracleAS Single Sign-On enables you to assign different authentication levels to the applications that it protects. You can then map these authentication levels to specific authentication plugins. You may, for example, configure a highly sensitive application to require a user certificate and a less sensitive application to require a user name and password.

How Multilevel Authentication Works

[Figure 6-1](#) on page 6-2 illustrates how multilevel authentication works.

Figure 6–1 Multilevel Authentication Flow

1. The user has already authenticated to Application A. He or she now goes to Application B.
2. Application B redirects the user to the single sign-on server.
3. Because Application B has a higher authentication level than Application A, the single sign-on server forces the user to authenticate again, this time with a higher credential.

Note: In release 10.1.4, authentication is at the root level of a partner application. You cannot assign authentication levels to URLs under the root.

Components of a Multilevel System

The following topics are key to understanding how multilevel authentication works:

- [Authentication Levels](#)
- [Authentication Plugins](#)

Authentication Levels

Authentication levels are parameters that enable you to define different authentication behaviors for different applications. There are six authentication levels defined in the `ORACLE_HOME/sso/conf/policy.properties` file. This file contains authentication level names and values. A copy of this file appears in [Appendix C](#).

[Table 6–1](#) provides examples of authentication levels. You can customize these levels and create new ones.

Table 6–1 Default Authentication Levels

Authentication Level Names	Authentication Level Values	Description
LowSecurity	20	The default value is used for weak authentication.
LowMediumSecurity	30	This value is typically used for custom authentication modules.
MediumSecurity	40	The default value for MediumSecurity indicates user name and password authentication.
MediumHighSecurity	50	The default value indicates that certificate authentication is required.
HighSecurity	60	This value is typically used for custom authentication modules.

Each security level has an associated name, a java class that contains the plug-in parameters for the security level being implemented, and a hostname and port for each application protected by this security level.

The authentication level name can be any name. Names must be unique, and any change to a name must be reflected in all relevant locations in `policy.properties`. For example, you cannot specify `NoSecurity=10` and `NoSecurity=20`. The lower the numeric value of a level, the lower the level of security. Values must be positive integers. These values are used when comparing the current authentication level and checking if a higher level of authentication is required.

The security level provides the authentication method. It is represented as a URL to the java class that contains the plug-in parameters.

For example, if you want to enforce user name and password authentication for most partner applications, but you want certificate authentication for a particular partner, you can add the following to `policy.properties`:

```
partner_application_host.example_company.com\:7777 = MediumHighSecurity
MediumHighSecurity=oracle.security.soo.auth.SSOX509CertAuth
```

Users who log in at a higher level and then attempt to access a lower-level application are not rechallenged for credentials. Users who log in at a lower-level application and then attempt to access a higher-level one are challenged using the authentication method set at the higher level. For example, a user who has logged in with `MediumSecurity` can access an application that requires `LowSecurity`, but a user who has logged in with `LowSecurity` must authenticate to access an application that requires `MediumSecurity`.

Authentication Plugins

An authentication plugin is an implementation of a specific authentication method. This method collects credentials from users and authenticates them.

You can pair one of the authentication levels introduced in the preceding section with one of the authentication methods described in the bulleted list that follows. The authentication level that an authentication plugin maps to is deployment specific. You use `policy.properties` to achieve the pairing.

- Password authentication
 - This is the default, standard method.

- Digital certificates
See [Chapter 8](#) for a discussion of certificate authentication.
- Windows native authentication
See the chapter about integrating with Microsoft Active Directory in *Oracle Identity Management Integration Guide*.

Configuring Multilevel Authentication

If you do not configure an authentication level for an application, the `DefaultAuthLevel` parameter in the `policy.properties` file determines the default level that is used for authentication.

The default plug-in for authentication is the one that is associated with the default level. For example, if the value of `DefaultAuthLevel` is `MediumSecurity`, the application uses the plug-in that is provided in the definition of `MediumSecurity` in the `policy.properties` file.

Usage Scenario

This usage scenario explains how two hypothetical partner applications are configured to use different authentication levels and plugins. It assumes these conditions:

- Application `pa1` is deployed on host `pa1.mydomain.com`. It listens on port `7777`.
- `pa1` is already registered with the single sign-on server.
- `pa1` must use certificate authentication.
- Application `pa2` is deployed on host `pa2.mydomain.com`. It listens on port `7777`.
- `pa2` is already registered with the single sign-on server.
- `pa2` must use password authentication.

Configuration Steps

Modify `policy.properties` with the following configurations.

1. Choose the name of the authentication level from `policy.properties`. If necessary, add a new authentication level and corresponding name to the file.
2. Assign authentication levels to the root URLs of the two partner applications:

```
pa1.mydomain.com\:7777 = HighSecurity
pa2.mydomain.com\:7777 = MediumSecurity
```

Note: Be sure to include the backslash after the domain name.

3. Assign authentication plugins to the authentication level names that you assigned in step 1:

```
HighSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOX509CertAuth
MediumSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOServerAuth
```

Note that the authentication plugin name is a combination of the authentication level name that you assigned in step 1 and the suffix `_AuthPlugin`.

4. Save `policy.properties`; then restart the single sign-on middle-tier.

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
```

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

5. Test the partner applications.

Enabling SSL

This chapter explains how to enable the single sign-on server for Secure Sockets Layer (SSL). In SSL, a secret session key is created, enabling the exchange of information over a secure channel. When the user logs in, the Web server sends the browser a digital certificate. The browser uses a public key sent by the Web server to encrypt a random number. This encrypted data is used in turn to create the secret key. Enabling the single sign-on server for SSL confers this form of protection on the server's partner applications. The process provides OracleAS with a high degree of security.

Out of the box, the single sign-on server uses the HTTP port of the Oracle HTTP Server. You can, however, configure SSL after installation using either an automated or manual approach.

Automated SSL Configuration

For common topologies, the SSL Configuration Tool can perform the steps required to enable post-installation SSL of the Oracle HTTP Server. For details about the tool and how to run it, see "Using the SSL Configuration Tool" in the *Oracle Application Server Administrator's Guide*.

If you want to monitor your server, the Beacon Certificate Authorities certificate file, `b64InternetCertificate.txt`, in the installation directory for the Enterprise Manager Agent, must contain the certificate of the infrastructure server. See the document *Oracle Enterprise Manager Advanced Configuration* for details. In particular, see the section on configuring beacons to monitor Web applications over HTTPS in the chapter on Oracle Enterprise Manager security.

Note: Before using the SSL Configuration Tool, you must understand the limitations of configuring an SSL port. See "[Caveats About Configuring SSL](#)" on page 7-5 for details.

Manual SSL Configuration

If you prefer a manual approach to enabling SSL, complete the following tasks in the order listed:

- [Enable SSL on the Single Sign-On Middle Tier](#)
- [Reconfigure the Identity Management Infrastructure Database](#)
- [Protect Single Sign-On URLs](#)
- [Restart the Oracle HTTP Server and the Single Sign-On Middle Tier](#)
- [Reregister Partner Applications](#)

- [Secure Transmission of mod_osso Cookies](#)

Note: If the Oracle HTTP Server is configured for SSL (topic 1) you must configure the single sign-on server for SSL as well (remaining topics); otherwise users will be unable to access single sign-on URLs. To skirt this restriction, disable SSL directives for URLs that you want to access over HTTP. You do this by editing `ORACLE_HOME/sso/conf/sso_apache.conf`.

Enable SSL on the Single Sign-On Middle Tier

The following steps involve configuring the Oracle HTTP Server. In performing them, keep the following in mind:

- You must configure SSL on the computer where the single sign-on middle tier is running—that is, on the computer that hosts the single sign-on server.
- You are configuring one-way SSL.
- You may enable SSL for simple network encryption; PKI authentication is not required. Note though that you must use a valid wallet and server certificate. The default wallet location is `ORACLE_HOME/Oracle/HTTPServer/conf/ssl.wlt/default`. If you want to use a different wallet, see the guidelines in the section "[Oracle HTTP Server](#)" in [Chapter 8](#). The chapter about managing wallets and certificates in *Oracle Application Server Administrator's Guide* is also helpful.

To quickly enable SSL on the Oracle HTTP Server, do the following:

1. Back up the `opmn.xml` file, found at `ORACLE_HOME/opmn/conf`.
2. In `opmn.xml`, change the value for the `start-mode` parameter to `ssl-enabled`. This parameter appears in boldface in the xml tag immediately following.

```
<ias-component id="HTTP_Server">
  <process-type id="HTTP_Server" module-id="OHS">
    <module-data>
      <category id="start-parameters">
        <data id="start-mode" value="ssl-enabled"/>
      </category>
    </module-data>
    <process-set id="HTTP_Server" numprocs="1"/>
  </process-type>
</ias-component>
```

3. Update the distributed cluster management database with the following change:

```
ORACLE_HOME/dcm/bin/dcmctl updateconfig -ct opmn
```

4. Reload the modified `opmn` configuration file:

```
ORACLE_HOME/opmn/bin/opmnctl reload
```

5. Keep a non-SSL port active on the Oracle HTTP Server that communicates with the OracleAS Single Sign-On server.

The External Applications portlet communicates with the single sign-on server over a non-SSL port. The HTTP port is enabled by default. If you have not disabled the port, this step requires no action. Note that users will not be able to

use this port for logins. See ["Caveats About Configuring SSL"](#) on page 7-5 for details.

6. Restart the Oracle HTTP Server:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl startproc process-type=HTTP_Server
```

7. Verify that you have enabled the single sign-on middle tier for SSL by trying to access the OracleAS welcome page, using the format `https://host:ssl_port`.

Note: If your installation has two or more middle tiers, make sure that you complete step 2 in ["Configure the Oracle HTTP servers on the single sign-on middle tiers"](#). This is a subsection of ["Multiple Single Sign-On Middle Tiers, One Oracle Internet Directory"](#) one of the deployment scenarios presented in [Chapter 9](#).

Reconfigure the Identity Management Infrastructure Database

To reconfigure the Identity Management Infrastructure Database, you must:

1. Change all references of `http` in single sign-on URLs to `https` within the identity management infrastructure database.
2. When you change single sign-on URLs in the database, you must also change these URLs in the `targets.xml` file on the single sign-on middle tier. `targets.xml` is the configuration file for the various targets that Oracle Enterprise Manager monitors. One of these targets is OracleAS Single Sign-On.
3. Configure Oracle Enterprise Manager Security.

These steps are described in the subsequent sections.

Change Single Sign-On URLs

Run the `ssocfg` script, taking care to enter the command on the computer where the single sign-on middle tier is located. Use the following syntax:

- UNIX:

```
$ORACLE_HOME/sso/bin/ssocfg.sh protocol host ssl_port
```

- Windows:

```
%ORACLE_HOME%\sso\bin\ssocfg.bat protocol host ssl_port
```

In this case, *protocol* is `https`. (To change back to HTTP, use `http`.) The parameter *host* is the host name, or server name, of the Oracle HTTP listener for the single sign-on server.

Here is an example:

```
ssocfg.sh https login.acme.com 4443
```

To determine the correct port number, examine the `ssl.conf` file. Port 4443 is the port number that the OracleAS installer assigns during installation.

If you run `ssocfg` successfully, the script returns a status 0. To confirm that you were successful, restart the OC4J_SECURITY instance:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

Then try logging in to the single sign-on server at its SSL address:

```
https://host:ssl_port/sso/
```

Update targets.xml

After running `ssocfg`, update the `targets.xml` file on the single sign-on middle tier.

To update `targets.xml`:

1. Back up the file:

```
cp ORACLE_HOME/sysman/emd/targets.xml ORACLE_HOME/sysman/emd/targets.xml.backup
```

2. Open the file and find the target type `oracle_sso_server`. Within this target type, locate and edit the three attributes that you passed to `ssocfg`:

- `HTTPMachine`—the HTTP server host name
- `HTTPPort`—the SSL port number of the Oracle HTTP server
- `HTTPProtocol`—the server protocol

If, for example, you run `ssocfg` like this:

```
ORACLE_HOME/sso/bin/ssocfg.sh https sso.mydomain.com:4443
```

Update the three attributes this way:

```
<Property NAME="HTTPMachine" VALUE="sso.mydomain.com"/>
<Property NAME="HTTPPort" VALUE="4443"/>
<Property NAME="HTTPProtocol" VALUE="HTTPS"/>
```

3. Save and close the file.
4. Reload the OracleAS console:

```
ORACLE_HOME/bin/emctl reload
```

Configure Oracle Enterprise Manager Security

Since you are enabling the single sign-on server for SSL, you will need to follow all the configuration instructions detailed in the chapter about Oracle Enterprise Manager security in *Oracle Enterprise Manager Advanced Configuration*. Specifically, pay close attention to the section titled "Configuring Beacons to Monitor Web Applications Over HTTPS." Oracle Beacons, which are part of the Application Service Level Management features of Enterprise Manager, provide application performance availability and performance monitoring. Beacons are used to monitor a URL over SSL using an HTTPS URL.

Protect Single Sign-On URLs

When the single sign-on server is enabled for SSL, you must specify that HTTP access be limited to those hosts that must access the server using this protocol. This is especially true in the case of those computers hosting the OracleAS installer and OracleAS Portal.

This section provides instructions for:

- [Protecting URLs in the Absence of a Load Balancing Router](#)
- [Protecting URLs in the Presence of a Load Balancing Router](#)

Protecting URLs in the Absence of a Load Balancing Router

Use these instructions when no load balancing router is deployed in front of the single sign-on server and OracleAS Portal. In `ORACLE_HOME/sso/conf/sso_apache.conf`, locate and uncomment the directives that follow, then provide a value for the `Allow from` parameter.

OracleAS Portal must use HTTP to access the URL that provides a list of external applications. The directive that follows enables such access. Replace `<your_domain_name>` with the fully qualified Portal host name; then uncomment the directive. If you have more than one Portal database, enter just the domain name for these databases.

```
#<Location "/sso/eappslist">
# Order deny,allow
# Deny from all
# Allow from <your_domain_name>
#</Location>
```

After editing `sso_apache.conf`, update the repository for Distributed Cluster Management:

```
ORACLE_HOME/dcm/bin/dcmctl updateConfig -v -d
```

Protecting URLs in the Presence of a Load Balancing Router

In a deployment configuration where the single sign-on server and OracleAS Portal are front-ended by a load-balancing router, the rule for limiting access to hosts should be set directly with the load-balancing router. Do not attempt to add such a rule in the `ORACLE_HOME/Apache/Apache/conf/sso_apache.conf` file to allow or deny access to a host for this configuration.

Here is an example of such a rule for BigIP:

```
if (client_addr != <infrastructure db IP> netmask 255.255.255.0 and
    (http_uri starts_with
     "/sso/eappslist")) {
discard
}
else {
    use pool SSO
}
```

Note: This is a specific example and is presented for illustration only. In practice, you should ensure that any access rule you apply is consistent with the load balancing router in use.

Restart the Oracle HTTP Server and the Single Sign-On Middle Tier

Issue these two commands:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

Caveats About Configuring SSL

There are two cases you must consider when configuring SSL:

- When you have configured SSL for the OracleAS Single Sign-On Server
- When you have configured a partner application for SSL.

When you have configured OracleAS Single Sign-On Server for SSL, you must also maintain a non-SSL port on the Oracle HTTP Server that front-ends the OracleAS Single Sign-On Server. This port is required for OracleAS Single Sign-On operation whether or not SSL is configured.

However, if you do this, note that users will not, by default, be able to use the non-SSL port to access OracleAS Single Sign-On-protected content on that Oracle HTTP Server. For example, if you have configured OracleAS Single Sign-On to protect `http://myhost.mydomain.com` on Oracle HTTP Server 1, users will receive an error if they enter this URL in their browser. They must use `https` instead.

When you have configured a partner application for SSL (this includes configuring OracleAS Single Sign-On), to enable users to access content using both an SSL and a non-SSL port, you must configure two instances of the partner application. One instance should use the SSL port and the other should use the non-SSL port. See "[Configuring and Administering Partner Applications](#)" on page 4-1 for details.

Note: Oracle does not recommend blocking the non-SSL port for the Oracle HTTP Server that is front-ending the OracleAS Single Sign-On Server.

Reregister Partner Applications

Once you have enabled the partner application for SSL, reregister `mod_osso` on the single sign-on middle tier and on the application middle tiers. This step configures `mod_osso` to use the effective single sign-on URL. See "[Configuring mod_osso with Virtual Hosts \(SSL and non-SSL\)](#)" in [Chapter 4](#) for instructions. To reregister OracleAS Portal, an application integrated with the single sign-on SDK, use the `ptlconfig` tool. To learn how to use `ptlconfig`, see Appendix B in *Oracle Application Server Portal Configuration Guide*.

Note: After reregistering the partner application, by default users will not be able to access protected content using a non-SSL port. See "[Caveats About Configuring SSL](#)" on page 7-5 for details.

Secure Transmission of mod_osso Cookies

You can add the `OsoSecureCookies` directive to set the `Secure` flag on all cookies created by `mod_osso`. This tells the browser to only transmit those cookies on connections secured by HTTPS.

An example of this directive, in the `mod_osso` configuration file located in `ORACLE_HOME/Apache/Apache/conf/mod_osso.conf`, is as follows:

```
<IfModule mod_osso.c>
OsoIpCheck off
OsoIdleTimeout off
OsoSecureCookies on
OsoConfigFile osso/osso.conf
<Location /j2ee/webapp>
require valid-user
AuthType Basic
</Location>
</IfModule>
```

Signing On with Digital Certificates

Single sign-on with X.509 client certificates provides a stronger degree of security than simple authentication. It offers the benefit that partner applications are, by default, PKI enabled when the single sign-on server is PKI enabled.

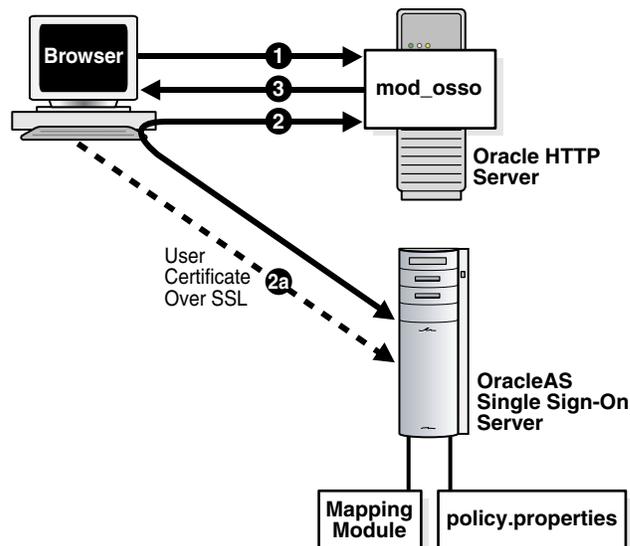
This chapter contains the following topics:

- [How Certificate-Enabled Authentication Works](#)
- [System Requirements](#)
- [Configuring the Single Sign-On System for Certificates](#)
- [Maintaining a Certificate Revocation List](#)

How Certificate-Enabled Authentication Works

Figure 8–1 depicts the authentication flow for certificate-enabled sign-on.

Figure 8–1 Certificate-Enabled Single Sign-On



1. The user tries to access a partner application.
2. The partner application redirects the user to the single sign-on server for authentication. As part of this redirection, the browser sends the user's certificate

to the login URL of the server (2a). If it is able to verify the certificate, the server returns the user to the requested application.

3. The application delivers content.

Note: Users whose browsers are configured to prompt for a certificate-store password may only have to present this password once, depending upon how their browser is configured. If they log out and then attempt to access a partner application, the browser passes their certificate to the single sign-on server automatically. This means that they never really log out. To effectively log out, they must close the browser.

System Requirements

The following criteria must be met before certificate-enabled single sign-on can proceed:

- The single sign-on server and Oracle Internet Directory must be installed.
- The Oracle HTTP Server must have a valid server certificate installed.
- The client certificate DN must be chosen in such a way that it meets one of the following two criteria:
 - The DN of the user certificate is the same as the user DN in Oracle Internet Directory
 - The DN of the user certificate contains the user nickname and, optionally, the name of the realm that the user belongs to
- The certificate of the client certificate issuer must be installed as a trusted certificate on the single sign-on server.
- The certificate of the server certificate issuer must be installed as a trusted certificate in the user's browser.

Configuring the Single Sign-On System for Certificates

Certificate-enabled single sign-on is not a default option in OracleAS, and it must be configured after installation. Before configuring certificate authentication, you must enable the single sign-on system for SSL. Perform the tasks in [Chapter 7](#); then return to this section and configure the following components for certificates:

- [Oracle HTTP Server](#)
- [Single Sign-On Server](#)
- [Oracle Internet Directory](#)

Oracle HTTP Server

Configuring the Oracle HTTP Server for certificates consists of adding parameters to the `ssl.conf` file and, optionally, choosing the certificate authority that issues server and user certificates.

Setting SSL Parameters

To set the required SSL parameters, complete the following steps:

1. Go to `ssl.conf`. The file is at `ORACLE_HOME/Apache/Apache/conf`.
2. In the `SSL Virtual Host Context` section of `ssl.conf`, add or edit the parameters listed in [Table 8-1](#). At the same time, verify that the `SSL Engine` parameter has been set to `on`. This should have been done as part of configuring the Oracle HTTP Server for SSL.

Table 8-1 HTTP Parameters for Certificate-Enabled Single Sign-On

Parameter	Description
<code>SSLWallet</code>	<p>The location, or path, of the server wallet. The default location is <code>ORACLE_HOME/Apache/Apache/conf/ssl.wlt/default</code>.</p> <p>Note:</p> <p>The actual location of the Oracle home must be substituted for the variable.</p> <p>If OracleAS Certificate Authority is installed in the same Oracle home as OracleAS Single Sign-On, and you want to use this CA to issue certificates, the wallet location is <code>ORACLE_HOME/oca/wallet/ssl</code>. See "Choosing a Certificate Authority" for details.</p>
<code>SSLWalletPassword</code>	Password for the server wallet
<code>SSLVerifyClient</code>	<p>The verification type for client certificates. These are the three types:</p> <ul style="list-style-type: none"> ■ <code>none</code>—SSL without certificates ■ <code>optional</code>—server certificate and optionally client certificate ■ <code>require</code>—server and client certificates <p>You must choose either <code>optional</code> or <code>require</code>.</p>

Choosing a Certificate Authority

If you have OracleAS Certificate Authority installed and want to use this CA to issue certificates, edit `ssl.conf` to point to the desired Oracle CA wallet. You can either use the Oracle CA wallet described in [Table 8-1](#) or have the Oracle CA issue a wallet that is specifically for the single sign-on server. If you choose the first option, copy the wallets that are in the wallet directory for the Oracle CA to the default wallet directory. If you choose the second option, see Chapter 7 in *Oracle Application Server Certificate Authority Administrator's Guide* for instructions. The relevant section is "Server/SubCA Certificates Tab." This is a subsection of "End-User Tabs and Processes." Once you obtain the wallet, edit `ssl.conf` to point to the wallet's location.

You may, of course, elect to use a third-party CA. In this case, too, you must edit `ssl.conf` to point to the wallet's location as explained in [Table 8-1](#).

Using OracleAS Single Sign-On in conjunction with OracleAS Certificate Authority simplifies the certificate provisioning process. You can configure the Oracle CA to broadcast the URL for its UI to single sign-on users. Users can then use this link to request a single sign-on certificate that is automatically linked to their entry in Oracle Internet Directory.

Single Sign-On Server

Configuring the single sign-on server to accept certificates consists of these tasks:

- [Configure policy.properties with the Default Authentication Plugin](#)
- [Modify the Configuration File for the Authentication Plugin \(Optional\)](#)

- [Customize the User Name Mapping Module \(Optional\)](#)
- [Restart the Single Sign-On Middle Tier](#)

Perform at least the first and the last step. Add the middle two if you want to customize the user name mapping module. The default module for user name mapping matches the distinguished name (DN) in the client certificate with a single sign-on user in Oracle Internet Directory. The default implementation assumes that the user's DN in the directory is the same as the certificate DN. A module that maps a field in the certificate DN to the user's name in Oracle Internet Directory is also available. If you want to substitute this module for the DN mapping module, modify the `CertificateMappingModule` parameter as prescribed in the third task.

Configure `policy.properties` with the Default Authentication Plugin

Update the `DefaultAuthLevel` section of the `policy.properties` file with the correct authentication level for certificate sign-on. This file is at `ORACLE_HOME/sso/conf`. Set the default authentication level to this value:

```
DefaultAuthLevel = MediumHighSecurity
```

Then, in the `Authentication plugins` section, pair this authentication level with the default authentication plugin:

```
MediumHighSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOX509CertAuth
```

For your convenience, `policy.properties` is available in [Appendix C, "policy.properties"](#).

Modify the Configuration File for the Authentication Plugin (Optional)

The `X509CertAuth.properties` file contains the parameters that follow. The file is in the same directory as `policy.properties`.

Note: Omit this step if you are using the DN-based mapping module.

CertificateMappingModule This parameter is set to the class file that performs user name mapping. The parameter can have one of two default values:

```
oracle.security.sso.server.auth.SSOCertMapperDn
```

or

```
oracle.security.sso.server.auth.SSOCertMapperNickname
```

The first module assumes that the user's DN in the directory is the same as the certificate DN. This is the default, out-of-the-box setting. The second module assumes that the first attribute in the user DN in the certificate is `cn`. It also assumes that this attribute is the same as the user nickname in the default realm of Oracle Internet Directory. If, for example, the user DN in the certificate is `cn=john, cn=users, dc=acme, dc=com`, you can use the second module. If, on the other hand, the DN is `e=john.smith@acme.com, cn=john, cn=users, dc=acme, dc=com`, you cannot use the module. You can, however, write a mapping module that uses this DN. See ["Customize the User Name Mapping Module \(Optional\)"](#) for details. If you decide to write your own module, set `CertificateMappingModule` to the class file name for your implementation.

CheckUserCertificate This parameter indicates whether the user certificate must be verified in Oracle Internet Directory. The default value is `true`. If you deem the SSL protection provided by the Oracle HTTP Server to be sufficient, set this parameter to `false`.

CertificateAuthFailureUrl If certificate authentication fails, the user is redirected to this URL, which displays an error message.

CertificateAuthFallback Set this parameter to `true` if you want to make password authentication available to a user who tries to log in without a valid certificate. This fallback does not occur by default. You must enable it. If the parameter is set to `false` or is absent entirely, users see a message that tells them they must present a valid certificate. You may have to add `CertificateAuthFallback` to the file. Place it at the end this way:

```
#Allow authentication fallback
CertificateAuthFallback=true
```

Note: If `CertificateAuthFallback` is set to `true`, you cannot use multilevel authentication.

Customize the User Name Mapping Module (Optional)

To customize the user name mapping module, implement a mapping module based on `oracle.security.sso.ias904.toolkit.IPASUserMappingInterface`. Refer to the example mapping modules shipped with this release. Again, these modules are `SSOCertMapperDN.java` and `SSOCertMapperNickname.java`.

Note: Omit this step if you are not writing your own mapping module.

The example modules contain the following classes:

- Mapping module Interface

This interface contains the following methods:

```
public IPASUserInfo getUserInfo(
    javax.servlet.http.HttpServletRequest request)
    throws IPASException;
```

- User information class

This class contains user information such as the user nickname and user DN. The package name is `oracle.security.sso.ias904.toolkit.IPASUserInfo`. The constructor looks like this:

```
Public IPASUserInfo(
    String userNickName
    String realmNickname)

Public IPASUserInfo(
    String userNickName,
    String userDN,
    String userGUID,
    String realmNickname,
    String realmDN,
    String realmGUID)
```

- Exception class

A problem with user name mapping raises this exception. The class name is `oracle.security.sso.ias904.toolkit.IPASException`. The super class is `java.lang.Exception`. The constructor looks like this:

```
public IPASException()  
public IPASException(String Message)
```

1. Extract `ipassample.jar`, the file that contains the modules:

```
ORACLE_HOME/jdk/bin/jar -xvf ORACLE_HOME/sso/lib/ipassample.jar
```

2. Create a Java class that implements the following interface:

```
oracle.security.sso.ias904.toolkit.IPASUserMappingInterface
```

3. Compile your custom implementation:

```
ORACLE_HOME/jdk/bin/javac -classpath ORACLE_HOME/sso/lib/  
ipastoolkit.jar:ORACLE_HOME/lib/servlet.jar -d class_directory  
java_file_name
```

4. Jar your class file and place it into `ORACLE_HOME/sso/plugin`:

```
ORACLE_HOME/jdk/bin/jar -cvf ORACLE_HOME/sso/plugin/CertMapImpl.jar class_  
directory
```

This step assumes that you do not have individual class files in the plugin directory. If the directory contains the individual files, they may be duplicated.

5. Update `x509CertAuth.properties` with your implementation. See ["Modify the Configuration File for the Authentication Plugin \(Optional\)"](#).

Restart the Single Sign-On Middle Tier

After configuring the server, restart the middle tier:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server  
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

Oracle Internet Directory

For certificate-based authentication to be successful, the user certificate must be present in Oracle Internet Directory. If the certificate is issued by OracleAS Certificate Authority, the certificate is published in the directory automatically. This may also be true if the CA is in-house. If the certificate issuer is a third-party CA, a self-service application can fulfill this function. Or the directory administrator can try to add the certificate to the directory as an LDIF file, using the command-line tool `ldapmodify`.

Note:

- The procedures in this section assume that the value of `CheckUserCertificate` is set to `true` in the `X509CertAuth.properties` file. See ["Modify the Configuration File for the Authentication Plugin \(Optional\)"](#).
 - You can search the directory for `usercertificate`, the binary attribute that stores certificates. See the appendix about certificate searching in *Oracle Internet Directory Administrator's Guide*.
-
-

Advanced Deployment Options

This chapter explores nondefault ways to use OracleAS Single Sign-On. It presents scenarios that you may encounter in a production environment. Some of these scenarios involve deploying and configuring the component to interact with other OracleAS components.

The chapter contains the following topics:

- [Deployment Scenarios](#)
- [Replicating the Identity Management Database](#)
- [Deploying OracleAS Single Sign-On with a Proxy Server](#)
- [Setting Up Directory Synchronization for User Nickname Changes](#)

Deployment Scenarios

This section describes different ways that the single sign-on server may be deployed to improve availability. The section contains the following topics:

- [One Single Sign-On Middle Tier, One Oracle Internet Directory](#)
- [Multiple Single Sign-On Middle Tiers, One Oracle Internet Directory](#)
- [Multiple, Geographically Distributed Single Sign-On Instances](#)
- [Other High Availability Deployments](#)

Note: The IP addresses and host names presented in the scenarios that follow are examples only. These addresses and names may not work in an actual implementation. Substitute values that apply to your installation.

One Single Sign-On Middle Tier, One Oracle Internet Directory

The simplest and quickest way to deploy OracleAS Single Sign-On is to install OracleAS infrastructure components on the same computer. To do this, you choose the installation type OracleAS Infrastructure and the installation option Identity Management and OracleAS Metadata Repository. When presented with the component list for this installation type, accept the default selected components.

Alternatively, you can install the single sign-on middle tier on a separate computer, choosing in succession OracleAS Infrastructure, Identity Management, and finally Single Sign-On. This is the simplest distributed configuration.

Figure 9–1 shows the first type of installation. Figure 9–2 shows the second. The first is typical of a testing, staging, or development environment. The second is appropriate when you want to position a firewall between the single sign-on computer and the Oracle Internet Directory computer. Placing these servers on separate computers has the added benefit that it improves performance. In Figure 9–2, the single sign-on server might be situated within a DMZ, where it filters internet traffic. In this configuration, the directory and the database are available only to intranet users.

Figure 9–1 Default Single Sign-On Installation: One Computer

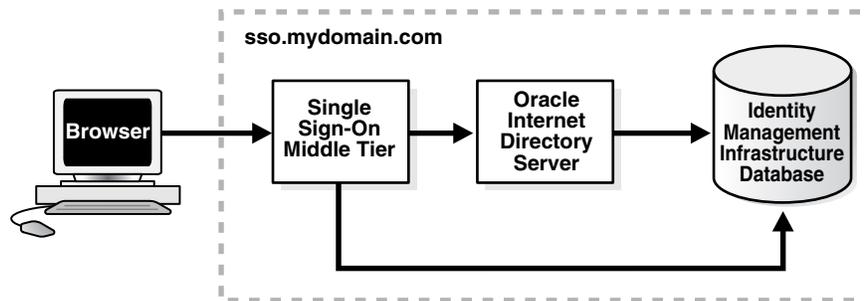
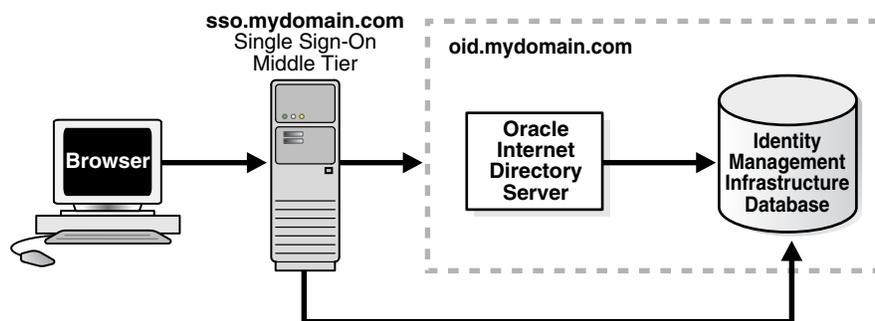


Figure 9–2 Single Sign-On Installation: Two Computers



Multiple Single Sign-On Middle Tiers, One Oracle Internet Directory

The simplest high availability scenario involves failover within the single sign-on instance itself, at the middle tier. Adding multiple middle tiers increases throughput and makes the single sign-on server more available.

In this configuration, a single HTTP load balancer is placed in front of two or more Oracle HTTP servers. At the backend is one directory server and one identity management infrastructure database. The purpose of the load balancer is to publish a single address to single sign-on partner applications while providing a farm of single sign-on middle tiers that actually service the application requests. The HTTP load balancer can detect when one of these Oracle HTTP Server instances has failed and can then fail over requests to another instance.

This section contains these topics:

- [To Cluster Or Not to Cluster](#)
- [Usage Scenario](#)
- [Configuration Steps](#)

To Cluster Or Not to Cluster

You may deploy two or more single sign-on middle tiers in one of two ways: as a cluster or manually. The first method recommends itself for ease of installation. The OracleAS installer clusters the single sign-on nodes automatically around one distributed cluster management (DCM) database. DCM is the component that replicates cluster configuration information among all nodes in a cluster whenever changes to that configuration occur on any one node. This configuration is known as OracleAS Cluster (Identity Management) because middle-tier components such as OracleAS Single Sign-On are clustered and configured identically across nodes.

If the DCM database fails, however, all single sign-on nodes fail. If you want to avoid this dependency, configure the middle tiers manually—both with their own DCM database.

The configuration steps for a manual deployment appear in the sections immediately following.

See Also: To learn how to install a cluster, see the chapter about OracleAS Cluster (Identity Management) in *Oracle Application Server Installation Guide*. More specifically, refer to the following:

- The section on "Installing an OracleAS Cluster (Identity Management) Configuration"
- The section on "Installing a Distributed OracleAS Cluster (Identity Management) Configuration"

Usage Scenario

The usage scenario presented here assumes the following hypothetical configurations:

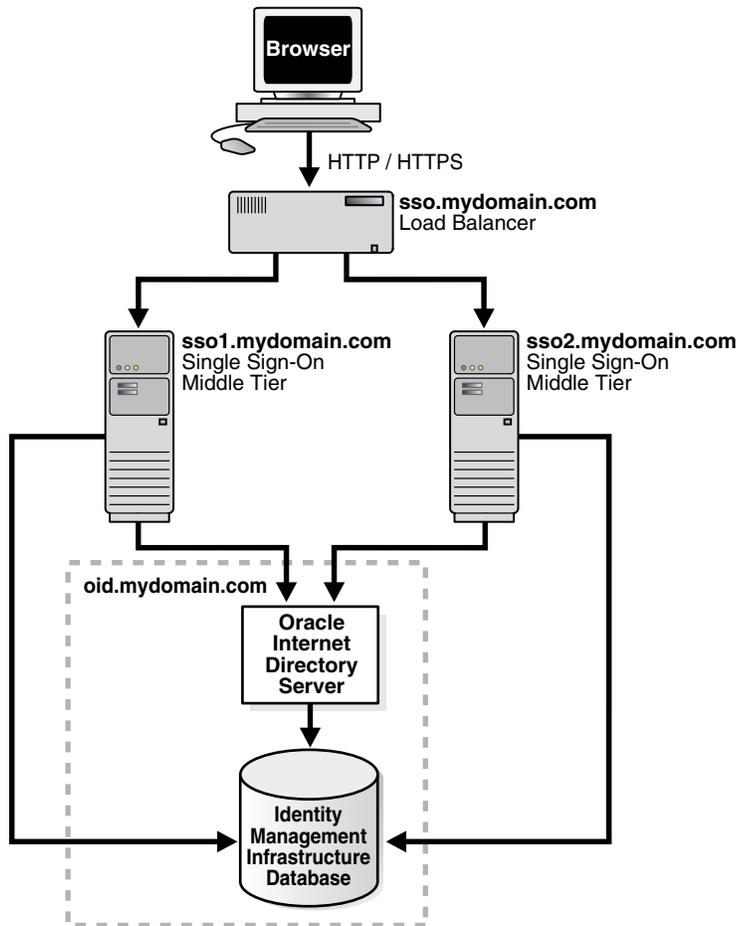
- The directory server and identity management infrastructure database are located at `oid.mydomain.com`.
- There are two single sign-on middle tiers. One is installed on host `sso1.mydomain.com`, IP address `138.1.34.172`. The other is installed on `sso2.mydomain.com`, IP address `138.1.34.173`. Both servers listen on non-SSL port `7777`. Both are configured to use the directory and identity management infrastructure database located at `oid.mydomain.com`.
- The effective URL of the single sign-on server that is published to partner applications is `sso.mydomain.com`, IP address `138.1.34.234`. The HTTP load balancer is configured to listen on `sso.mydomain.com`, port `80`. It load balances user requests between `sso1.mydomain.com` and `sso2.mydomain.com`.

Notes:

- In this scenario, the load balancer is listening on port `80`, a non-SSL port number.
 - If the load balancer is configured to use SSL to interact with the browser, a different port number must be selected. The default SSL port number is `4443`.
 - In this scenario and the one immediately following, two single sign-on middle tiers are used. There can, in fact, be any number of middle tiers.
-
-

Figure 9–3 on page 9-4 shows two single sign-on middle tiers configured to use a single instance of Oracle Internet Directory.

Figure 9–3 Two Single Sign-On Middle Tiers, One Oracle Internet Directory



Configuration Steps

Setting up the single sign-on system presented in Figure 9–3 involves the following tasks:

- Install the identity management infrastructure database, the directory server and the single sign-on servers
- Configure the Oracle HTTP servers on the single sign-on middle tiers
- Configure the HTTP load balancer
- Configure the identity management infrastructure database
- Reregister `mod_osso` on the single sign-on middle tiers

Install the identity management infrastructure database, the directory server and the single sign-on servers

1. Choose a single sign-on server name that will be published to partner applications. This will also be the address of the load balancer. In the scenario presented here, the address is `sso.mydomain.com`.

2. Install the OracleAS infrastructure on `oid.mydomain.com`, choosing the option Identity Management and OracleAS Metadata Repository. When presented with the component list for this installation type, choose Oracle Internet Directory only.
3. Install the OracleAS infrastructure on the middle tiers `sso1.mydomain.com` and `sso2.mydomain.com`, choosing the option Identity Management. When presented with the component list for this installation type, choose OracleAS Single Sign-On only. When the Oracle Universal Installer asks you to name the directory server associated with these single sign-on instances, enter `oid.mydomain.com`.

Note: The OracleAS installer, by default, assigns port numbers from a range of numbers. If you want the installer to assign a different port number to a component, see "Static Port Numbers" in Chapter 4 of *Oracle Application Server Installation Guide*.

Configure the Oracle HTTP servers on the single sign-on middle tiers

When a load balancer is placed between the user and the Oracle HTTP Server, the effective URL of the single sign-on server changes. The Oracle HTTP configuration `httpd.conf` file on both single sign-on middle tiers must be modified to reflect this change. This file can be found at `$ORACLE_HOME/Apache/Apache/conf`.

1. Edit the following lines in `httpd.conf` on `sso1.mydomain.com` and `sso2mydomain.com`:

```
KeepAlive off
ServerName sso.mydomain.com
Port 80
```

Note: If multiple ports are listed in `httpd.conf`, the effective port must appear last.

This step configures the Oracle HTTP servers at the single sign-on middle tiers to listen at the effective URL, which, in the scenario presented, is `sso.mydomain.com`.

2. If you configure SSL between the browser and the load balancer, and the SSL connection terminates at the load balancer, configure `mod_certheaders` on both `sso1.mydomain.com` and `sso2.mydomain.com`. This module enables the Oracle HTTP Server to treat requests that it receives over HTTP as SSL requests. Add the following steps. You can place them at the end of `httpd.conf`. Ordering is not important.
 - a. In `httpd.conf` on both middle tiers, enter the following line:


```
LoadModule certheaders_module libexec/mod_certheaders.so
```
 - b. If you are using OracleAS Web Cache as a load balancer, enter the following line:


```
AddCertHeader HTTPS
```

If you are using a hardware load balancer, enter the following line:

```
SimulateHttps on
```
3. Synchronize system clocks between both middle tiers.

4. Execute the following command to update the Distributed Configuration Management schema with the changes:

```
$ORACLE_HOME/dcm/bin/dcmctl updateConfig -v -d
```

Configure the HTTP load balancer

The HTTP load balancer used can be hardware such as BigIP, Alteon, or Local Director or software such as OracleAS Web Cache.

- **Hardware Load Balancer**

If you are using a hardware load balancer, configure one pool of real servers with the addresses 138.1.34.172 and 138.1.34.173. Configure one virtual server with the address 138.1.34.234. This virtual server is the external interface of the load balancer. For instructions, consult the documentation provided by your load balancer vendor.

- **Software Load Balancer**

If you are using OracleAS Web Cache to load balance connection requests, see the following documents:

- "Leveraging Oracle Identity Management Infrastructure" in *Oracle Application Server Web Cache Administrator's Guide*.
- "Routing Single Sign-On Server Requests," also in *Oracle Application Server Web Cache Administrator's Guide*.

Note: For optimal performance, use a hardware load balancer.

Configure the identity management infrastructure database

Run the ssocfg script on one of the single sign-on middle tiers. This script configures the single sign-on server to accept authentication requests from the externally published address of the single sign-on server. Using the example provided, the script would be executed in the following way.

- **UNIX:**

```
$ORACLE_HOME/sso/bin/ssocfg.sh http sso.mydomain.com 80
```

- **Windows NT/2000:**

```
%ORACLE_HOME%\sso\bin\ssocfg.bat http sso.mydomain.com 80
```

Note that the command example provides the listener protocol, host name, and port number of the load balancer as arguments. Recall that the load balancer address is the externally published address of the single sign-on server. If the load balancer is configured to use SSL, replace non-SSL port 80 with SSL port 4443 and `http` with `https`.

Reregister mod_osso on the single sign-on middle tiers

On both middle tier computers, reregister mod_osso as the partner application sso.mydomain.com.

To reregister mod_osso on sso1.mydomain.com:

1. Run the registration script. For the URLs, be sure to substitute values appropriate for your installation. The script creates a partner application called sso.mydomain.com.

```

$ORACLE_HOME/sso/bin/ssoreg.sh
-oracle_home_path orcl_home_path
-site_name site_name
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
-u userid
[-virtualhost]
[-update_mode CREATE | DELETE | MODIFY]
[-config_file config_file_path]
[-admin_id adminid]
[-admin_info admin_info]

```

For a description of command parameters, see ["Registering mod_osso"](#) in Chapter 4.

- Restart the middle tier at `sso1.mydomain.com`. For instructions, see ["Stopping and Starting the Single Sign-On Middle Tier"](#) in Chapter 2.

To reregister `mod_osso` on `sso2.mydomain.com`:

- On the computer `sso2.mydomain.com`, log in to the single sign-on administration pages as the single sign-on administrator. Be sure to log in to `http://sso.mydomain.com/sso`
- Use the Administer Partner Applications page to delete the existing entry for the partner application `sso2.mydomain.com`.
- Copy the `osso.conf` file from the computer `sso1.mydomain.com`. Make sure that you use binary mode if you FTP the file. Copy the file to `$ORACLE_HOME/Oracle/Oracle/conf/osso`.
- Synchronize the Distributed Configuration Management repository with the file copy. You do this by running the following command on `sso2.mydomain.com`:

```

$ORACLE_HOME/Oracle/Oracle/bin/ssotransfer $ORACLE_
HOME/Oracle/Oracle/conf/osso/osso.conf

```

Note: The `ssotransfer` command should not be used to synchronize the Distributed Configuration Management repository with the `mod_osso` configuration file created for a virtual host. To learn how to register `mod_osso` for a virtual host, see ["Configuring mod_osso with Virtual Hosts \(SSL and non-SSL\)"](#) in Chapter 4.

- Restart the middle tier at `sso2.mydomain.com`. For instructions, see ["Stopping and Starting the Single Sign-On Middle Tier"](#) in Chapter 2.
- If Oracle Delegated Administration Services is installed, change its base URL, using Oracle Directory Manager:

- Start the tool:

```
$ORACLE_HOME/bin/oidadmin
```

- Log in to Oracle Directory Manager as `cn=orcladmin`.
- Go to the entry that contains the `orcldasurlbase` attribute:

```
cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext,Entry Management
```

- Change the attribute to the following value:

`http://sso.mydomain.com/`

Make sure that you include the slash after the host name.

- e. Test the partner application oiddas:

`http://sso.mydomain.com/oiddas`

3. Test the single sign-on administration application:

`http://sso.mydomain.com/sso`

Multiple Single Sign-On Middle Tiers, Replicated Oracle Internet Directory

In local area networks that experience high traffic, it may be beneficial to supplement multiple single sign-on middle tiers with replicated instances of Oracle Internet Directory. This arrangement provides failover not only at the middle tier, but also at the directory server. It is useful for managing rolling upgrades because replica nodes can be removed for maintenance while other nodes continue to serve users.

To learn how to deploy an Oracle Identity Management system that uses multimaster replication, see the chapter about this topic in *Oracle Application Server High Availability Guide*. The chapter shows how to configure every component in the identity management infrastructure.

Multiple, Geographically Distributed Single Sign-On Instances

Server availability is critical for an enterprise whose operations are widely distributed geographically. If the enterprise uses a single server to authenticate remote users over a wide area network, the authentication time can be lengthy. To shorten network round-trips and speed access to applications, the enterprise can implement multiple, geographically distributed instances of the single sign-on server. This arrangement enables users to travel to remote locations and be authenticated by the nearest server, regardless of where applications are located.

In this scenario, single sign-on database tables are replicated over either a local area network or a wide area network. The DNS server located at each single sign-on middle tier site must be configured to resolve the effective address of the single sign-on server to the single sign-on instance that is nearest to the user.

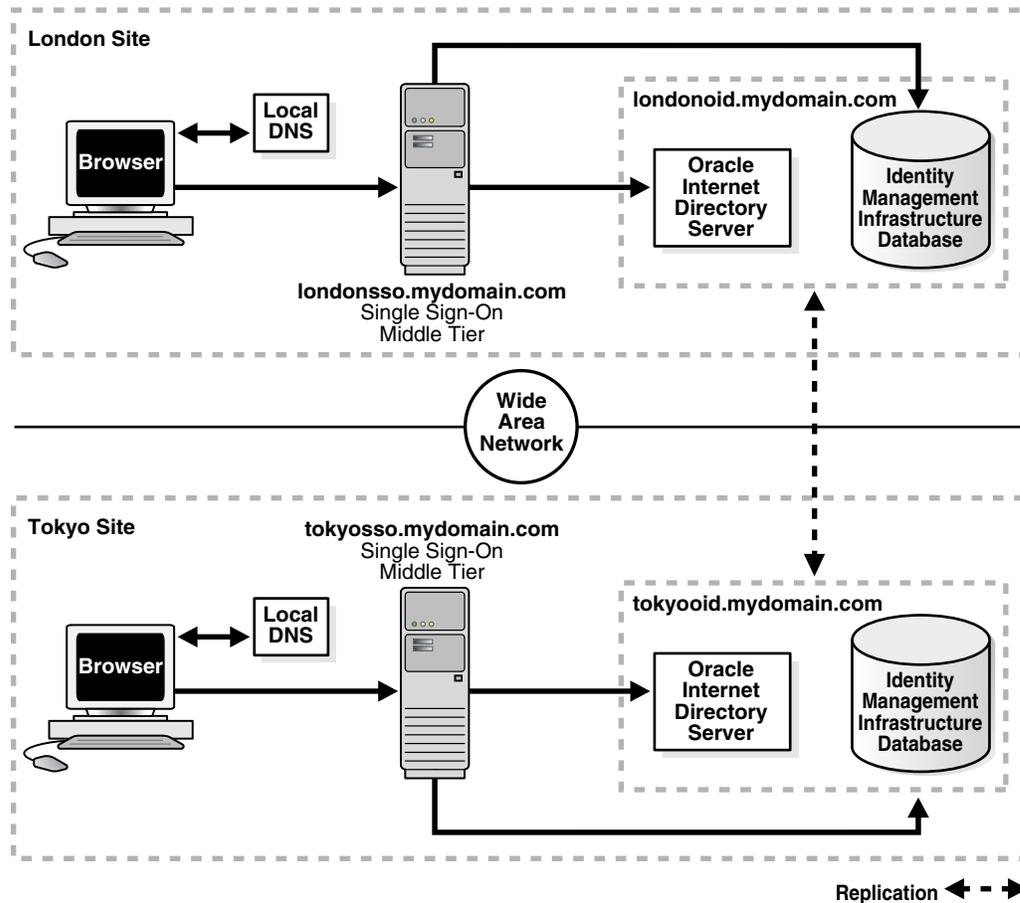
Usage Scenario

The usage scenario presented here assumes the following hypothetical configurations:

- There are two single sign-on middle tiers: `london.sso.mydomain.com` and `tokyo.sso.mydomain.com`. The effective address of the single sign-on server is `sso.mydomain.com`.
- There are two directory servers/identity management infrastructure databases associated with the two single sign-on middle tiers: `londonoid.mydomain.com` and `tokyooid.mydomain.com`.
- For replication purposes, `londonoid.mydomain.com` is the master definition site (MDS), the site from which the replication scripts are run and data is first replicated. `tokyooid.mydomain.com` is the remote master site (RMS), the site to which data is replicated.
- The single sign-on middle tiers and the identity management infrastructure databases are located on separate computers.

Figure 9–4 on page 9-9 depicts what this geographically distributed system looks like once it is deployed.

Figure 9–4 A Highly Available, Geographically Distributed Single Sign-On System



Configuration Steps

The geographically dispersed single sign-on system shown in Figure 9–5 incorporates steps presented in "Multiple Single Sign-On Middle Tiers, One Oracle Internet Directory" and "Configuring the Identity Management Database for Replication".

1. Install Oracle Internet Directory on the MDS, `londonoid.mydomain.com`, and on the RMS, `tokyooid.mydomain.com`; then set these servers up as a replication group. For instructions, see the appendix about deploying Oracle Identity Management with multimaster replication in *Oracle Application Server High Availability Guide*. These procedures cover both installation and replication. For replication concepts, see also *Oracle Internet Directory Administrator's Guide*.
2. Install the OracleAS infrastructure on the middle tier `londonosso.mydomain.com`, choosing the option "Identity Management." When presented with the component list for this installation type, choose "Single Sign-On." When the Oracle Universal Installer asks you to name the directory server associated with this single sign-on instance, enter `londonoid.mydomain.com`.

3. Repeat step 2, this time on middle tier `tokyosso.mydomain.com`. In this case, you must associate the single sign-on server with the directory server located at `tokyoid.mydomain.com`.
4. Synchronize single sign-on schema passwords between the MDS database and the RMS database. To do this, complete step 2 in "[Configuring the Identity Management Database for Replication](#)".
5. Although two single sign-on instances are now running at different locations, only one effective server URL is published to partner applications. Configure the single sign-on server to use this URL. In this scenario, we call the URL `sso.mydomain.com`. See "[Configure the Oracle HTTP servers on the single sign-on middle tiers](#)" for instructions.
6. Add a DNS alias, `sso.mydomain.com`, that points to the single sign-on middle tiers. Configure the DNS server to rout the user to the nearest middle tier when single sign-on authentication is required. When, for example, a London user is redirected to `http://sso.mydomain.com`, the DNS server should route the user to `http://london.sso.mydomain.com`. Similarly, a Tokyo user redirected to `http://sso.mydomain.com` should be routed to `http://tokyosso.mydomain.com`.

Note that some advanced DNS server products may be able to route users to the nearest server based on the geographic location.

Other High Availability Deployments

OracleAS supports cold failover clusters, disaster recovery, and backup and recovery for single sign-on as well as for other OracleAS components.

OracleAS Cold Failover Cluster (Infrastructure)

A cold failover cluster is a group of loosely coupled computers that together provide a single view of network services. Cluster software enables the logical IP address and processes of the primary node to be moved to a secondary node in the event that the primary fails. The node running the infrastructure is "hot." The node waiting to take over is "cold." Hence the term cold failover.

To learn more about cold failover clusters, see the chapter about infrastructure high availability in *Oracle Application Server High Availability Guide*.

Disaster Recovery

A disaster recovery deployment consists of two identically configured sites—one primary (production), the other secondary (standby). Both sites may be dispersed geographically and connected by a wide area network. When the primary site becomes unavailable due to a disaster, the secondary site can become operational within a reasonable amount of time. Client requests are always routed to the site playing the production role. After failover occurs, client requests are routed to the secondary site, which then assumes the production role. Both sites have identical middle tier servers, and these servers are also identical between the two sites. To learn more about disaster recovery, see the chapter devoted to this topic in *Oracle Application Server High Availability Guide*.

Backup and Recovery

Backup and recovery are terms used to describe strategies and procedures for preventing data loss and reconstructing lost data. To learn more about backup and

recovery, see the chapter devoted to this topic in *Oracle Application Server Administrator's Guide*.

Replicating the Identity Management Database

This section describes how to replicate the identity management database between two or more instances. Note that OracleAS Single Sign-On and Oracle Internet Directory share the scripts and procedures that replicate database tables. Before continuing with this section, become familiar with the following material:

- "Directory Replication Concepts" in *Oracle Internet Directory Administrator's Guide*
- "Oracle Directory Replication Administration" in *Oracle Internet Directory Administrator's Guide*
- "Replication-Management Command-Line Tools Syntax" also in *Oracle Internet Directory Administrator's Guide*

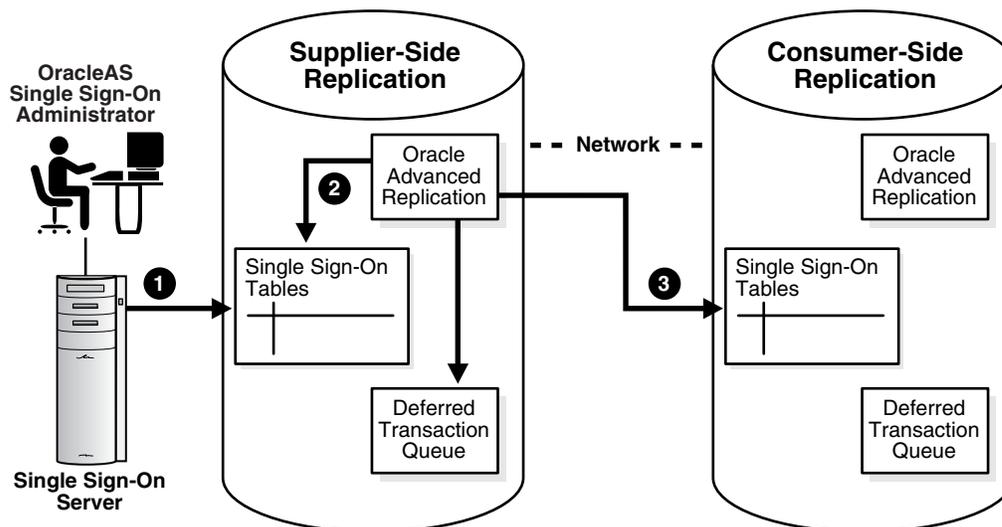
The section covers the following topics:

- [The Replication Mechanism](#)
- [Configuring the Identity Management Database for Replication](#)
- [Adding a Node to a Replication Group](#),
- [Deleting a Node from a Replication Group](#)

The Replication Mechanism

The identity management infrastructure uses Oracle9i Advanced Replication to replicate tables between two databases. This feature propagates data changes between databases asynchronously. In other words, suppliers write changes to single sign-on tables and periodically send batched changes to consumers, servers that replicate this data. All of the servers in a multiple, geographically distributed system can either propagate or receive data. This arrangement is called multimaster replication. [Figure 9-5](#) illustrates the process.

Figure 9-5 Multimaster Replication Architecture



1. The single sign-on administrator uses the single sign-on administration application to modify single sign-on partner applications or configuration data. This process modifies the corresponding table entry in the identity management infrastructure database.
2. Oracle9i Advanced Replication copies the change to a deferred transaction queue.
3. At a scheduled interval, Oracle9i Advanced Replication pushes transactions in the deferred transaction queue to the single sign-on table on the consumer side.

Configuring the Identity Management Database for Replication

Before proceeding with this section, become familiar with multimaster replication concepts in *Oracle Internet Directory Administrator's Guide*.

You may also want to familiarize yourself with the deployment scenario presented in "[Multiple, Geographically Distributed Single Sign-On Instances](#)". This section describes the circumstances under which single sign-on replication occurs.

The sequence for enabling the identity management database for replication is as follows:

1. To install and configure a multimaster replication group, see the section "Multimaster Replication Setup" in *Oracle Application Server High Availability Guide*. Note that single sign-on tables are replicated as part of this process.
2. After running the replication scripts, the administrator must run scripts to synchronize schema passwords among replicated nodes and to establish a connection between the single sign-on server and the directory. For details, see "Synchronizing the Oracle Application Server Single Sign-On Schema Password" in *Oracle Application Server High Availability Guide*.

On the MDS, run the `ssoreplsetup.jar` tool to synchronize single sign-on schema passwords between the MDS database and the RMS database. This step must be repeated for each RMS. [Table 9-1](#) on page 9-13 defines the tool parameters.

To run the script:

- a. Go to `ORACLE_HOME/sso/lib`.

- b. Set the library path:

* UNIX (csh and tcsh):

```
setenv LD_LIBRARY_PATH $ORACLE_HOME/lib32:$LD_LIBRARY_PATH
```

* Windows:

```
set PATH=%ORACLE_HOME%\bin;%PATH%
```

- c. Issue this command:

```
ORACLE_HOME/jdk/bin/java -jar ssoreplsetup.jar  
[-prompt]  
mds_oid_host  
mds_oid_port  
mds_oid_admin  
mds_oid_password  
mds_ssl_enabled  
rms_oid_host  
rms_oid_port  
rms_oid_admin
```

```

rms_oid_password
rms_ssl_enabled
rms_db_sys_password
[-help]

```

Table 9–1 Parameters for ssoReplSetup

Parameter	Description
<code>mds_oid_host</code>	Host name of the MDS directory server.
<code>mds_oid_port</code>	Port number of the MDS directory server.
<code>mds_oid_admin</code>	Bind DN—that is, the user authenticating to the MDS directory server.
<code>mds_oid_password</code>	Bind password of the MDS directory server.
<code>mds_ssl_enabled</code>	Indicates whether the MDS has SSL enabled. Can be either Y or N. Note that this parameter is case insensitive. This parameter is usually set to Y because the directory and the single sign-on server communicate over SSL by default.
<code>rms_oid_host</code>	Host name of the RMS directory server.
<code>rms_oid_port</code>	Port number of the RMS directory server.
<code>rms_oid_admin</code>	Bind DN—that is, the user authenticating to the RMS directory server.
<code>rms_oid_password</code>	Bind password of the RMS directory server.
<code>rms_ssl_enabled</code>	Indicates whether the RMS has SSL enabled. Can be either Y or N. Note that this parameter is case insensitive. This parameter is usually set to Y because the directory and the single sign-on server communicate over SSL by default.
<code>rms_db_sys_password</code>	SYS password of the RMS database.
<code>-prompt</code>	Prompts you for all values from the console.
<code>-help</code>	Displays usage notes.

Note: Repeat step 2 for each additional RMS node.

Adding a Node to a Replication Group,

If you want to add a node to an existing single sign-on replication group and have not replicated Oracle Internet Directory to this node, follow the instructions in *Oracle Internet Directory Administrator's Guide*. To configure this new node for single sign-on, install the single sign-on middle tier and repeat step 2 in "[Configuring the Identity Management Database for Replication](#)".

Deleting a Node from a Replication Group

To delete a node from the single sign-on replication group, follow the instructions in *Oracle Internet Directory Administrator's Guide*.

Deploying OracleAS Single Sign-On with a Proxy Server

OracleAS Single Sign-On can have reverse proxies deployed in front of it. Proxies fulfill various functions:

- They hide the host name of the single sign-on server.
- They terminate an SSL connection at the proxy instead of at the single sign-on server.
- They limit the number of ports exposed on a firewall

Whatever proxy you use in front of the single sign-on server, the configurations that follow apply. They assume that you have already installed OracleAS Single Sign-On and the proxy server. To install the proxy, use instructions provided by your proxy vendor.

Note: These instructions also apply to virtual hosts.

Turn Off IP Checking

In network configurations where a range of distinct proxy addresses "front" the single sign-on server, the single sign-on IP check feature must be turned off. IP check is turned off by default, but to verify this, go to the Edit SSO Server page. To learn how to access this page, see ["Accessing the Administration Pages"](#) in [Chapter 2](#). Once into the Edit SSO Server page, make sure that the box **Verify IP addresses for requests made to the SSO Server** is deselected.

Enable the Proxy Server

To enable a proxy server, do the following:

1. Run the `ssocfg` script on the single sign-on middle tier. This script changes the host name stored in the single sign-on server to the proxy host name. Use the following command syntax, entering values for the protocol, host name, and port of the proxy server:

- UNIX:

```
$ORACLE_HOME/sso/bin/ssocfg.sh http proxy_server_name proxy_port
```

- Windows:

```
%ORACLE_HOME%\sso\bin\ssocfg.bat http proxy_server_name proxy_port
```

If the server is configured for SSL, substitute `https` for `http` and an SSL port for a non-SSL port.

After running `ssocfg`, update the `targets.xml` file on the single sign-on middle tier. See ["Update targets.xml"](#) on page 7-4 for instructions.

2. Add the lines that follow to the `httpd.conf` file on the single sign-on middle tier. The file is at `ORACLE_HOME/Apache/Apache/conf`.

- a. These lines change the directive `ServerName` from the name of the actual server to the name of the proxy:

```
KeepAlive off
ServerName proxy_host_name
Port proxy_port
```

Note that if you are using SSL, the port must be an SSL port such as 4443.

- b. (SSL only) If you have configured SSL communication between just the browser and the proxy server, configure `mod_certheaders` on the middle tier. This module enables the Oracle HTTP Server to treat HTTP proxy requests

that it receives as SSL requests. Add the lines that follow to `httpd.conf`. You can place them at the end of the file. Where they appear is unimportant.

- * Enter this line to load the module:

UNIX:

```
LoadModule certheaders_module libexec/mod_certheaders.so
```

Windows:

```
LoadModule certheaders_module modules/ApacheModuleCertHeaders.dll
```

- * If you are using OracleAS Web Cache as a proxy, enter this line:

```
AddCertHeader HTTPS
```

If you are using a proxy other than OracleAS Web Cache, enter this line:

```
SimulateHttps on
```

3. Reregister `mod_osso` on the single sign-on middle tier. This step configures `mod_osso` to use the proxy host name instead of the actual host name. To learn how to run the registration tool, see "[Registering mod_osso](#)" in [Chapter 4](#).

4. Update the Distributed Configuration Management schema:

```
ORACLE_HOME/dcm/bin/dcmctl updateconfig
```

5. Restart the single sign-on middle tier:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

6. If you are deploying more than one single sign-on middle tier, repeat steps 2 through 4 on each additional middle tier.

7. Log in to the single sign-on server, using the single sign-on login URL:

```
http://proxy_host_name:proxy_port/sso/
```

This URL takes you to the single sign-on home page. If you are able to log in, you have configured the proxy correctly.

Setting Up Directory Synchronization for User Nickname Changes

The single sign-on database uses the user nickname to store and reference user data for external applications. In the event that the nickname attribute value changes in Oracle Internet Directory, users are forced to reenter their credentials when they log in with a new user ID. For their convenience, changes to their user names can be automatically synchronized between the directory and the single sign-on database. This synchronization mechanism, offered through Oracle Directory Integration and Provisioning, also deletes the external application data from the single sign-on database when a user's entry is deleted from the directory.

To synchronize nickname changes between the directory and the single sign-on database, follow these steps:

1. Start the Oracle Directory Integration and Provisioning server. For instructions, see the chapter about administration tools in *Oracle Identity Management Integration Guide*.

2. Load the synchronization package. First, navigate to `ORACLE_HOME/sso/admin/plsql/sso`; then connect to the single sign-on schema:

```
sqlplus orasso/password
```

See [Appendix B](#) to learn how to obtain the `orasso` password.

3. Run these packages in the order listed:

```
SQL> @ssodip.sql
SQL> @ssodip.pks
SQL> @ssodip.pkb
```

4. Register the single sign-on profile with Oracle Internet Directory. You do this by running the Provisioning Subscription Tool (`oidprovtool`):

```
ORACLE_HOME/bin/oidprovtool
operation=create
ldap_host=oid_host
ldap_port=oid_port
ldap_user_dn=cn=orcladmin
ldap_user_password=orcladmin_password
schedule=synchronization_interval_in_seconds
organization_dn=realm_DN
application_dn=orclApplicationCommonName=ORASSO_SSOSERVER, cn=SSO,
cn=Products, cn=OracleContext
interface_name=LDAP_NOTIFY interface_type=PLSQL
interface_connect_info=sso_database_host:sso_database_port:sso_
database_SID:orasso:orasso_schema_password
event_subscription=USER:user_search_base_for_realm:ADD(attribute_type)
event_subscription=USER:user_search_base_for_realm:MODIFY(attribute_type)
event_subscription=USER:user_search_base_for_realm:DELETE
```

If changes to the realm occur, reregister the profile. The user search base may change. Or the nickname attribute type. For example, the `uid` attribute may replace the `cn` attribute.

For help using `oidprovtool`, see the syntax appendix in *Oracle Internet Directory Administrator's Guide*.

5. Give the Oracle Directory Integration and Provisioning server privileges to proxy as `orasso`. This involves modifying the `orasso` entry in the directory.

First create an LDIF file:

```
dn: orclApplicationCommonName=ORASSO_SSOSERVER, cn=SSO, cn=Products,
cn=OracleContext
changetype: modify
add: orclaci
orclaci: access to entry by group="cn=odisgroup, cn=odi, cn=oracle internet
directory" (proxy)
```

6. Load the LDIF file into the directory as the super user `cn=orcladmin`.
7. Make sure that the Oracle Directory Integration and Provisioning server is running.

Depending upon how synchronization is scheduled, there may be a lapse between the time changes are made in the directory and the time they are synchronized with the single sign-on server. Because of this lapse, users whose user IDs have changed gain access to external applications only when synchronization finally occurs.

Enabling Support for Application Service Providers

This chapter explains how to enable the single sign-on server to support multiple realms within one instance of the Oracle Identity Management infrastructure.

The chapter contains the following topics:

- [Application Service Providers: Deciding to Deploy Multiple Realms](#)
- [Setting Up and Enabling Multiple Realms](#)
- [How the Single Sign-On Server Enables Authentication to Multiple Realms](#)
- [Configuring the Single Sign-On Server for Multiple Realms](#)
- [Granting Administrative Privileges for Multiple Realms](#)

Application Service Providers: Deciding to Deploy Multiple Realms

Application service providers are companies that install and maintain Oracle and non-Oracle applications and make them available to their customers, typically for a fee. These companies achieve economies of scale by serving multiple sets of users within the same application instance. The application service provider may, for example, use different realms, or namespaces, within one instance of the Oracle Identity Management infrastructure to set and store Oracle configuration information unique to different customers.

If user IDs are the only criterion for deciding whether to deploy multiple realms, and there are no ID conflicts, Oracle recommends maintaining users in a single, default realm. The application service provider may, for example, be one who has users log in with an email ID, which is unique. In situations where user IDs conflict, separate realms may be unavoidable. Note, too, that the decision to deploy multiple realms affects how Oracle 10g middle-tier components and customer applications are deployed.

Note: To gain a thorough understanding of Oracle Identity Management, see *Oracle Identity Management Administrator's Guide*.

Setting Up and Enabling Multiple Realms

The work involved in setting up multiple realms may require resources and administrative overhead that exceed those of OracleAS Single Sign-On. Other components are involved in the process. In fact, realm configuration is a three-part process that consists of the following:

- Creating realms in Oracle Internet Directory
- "Turning on" multiple realms in OracleAS Single Sign-On
- Making partner applications aware of identity management realms

The first process is discussed in *Oracle Internet Directory Administrator's Guide*. The second is the subject of this chapter. The third is discussed in product-relevant documentation.

How the Single Sign-On Server Enables Authentication to Multiple Realms

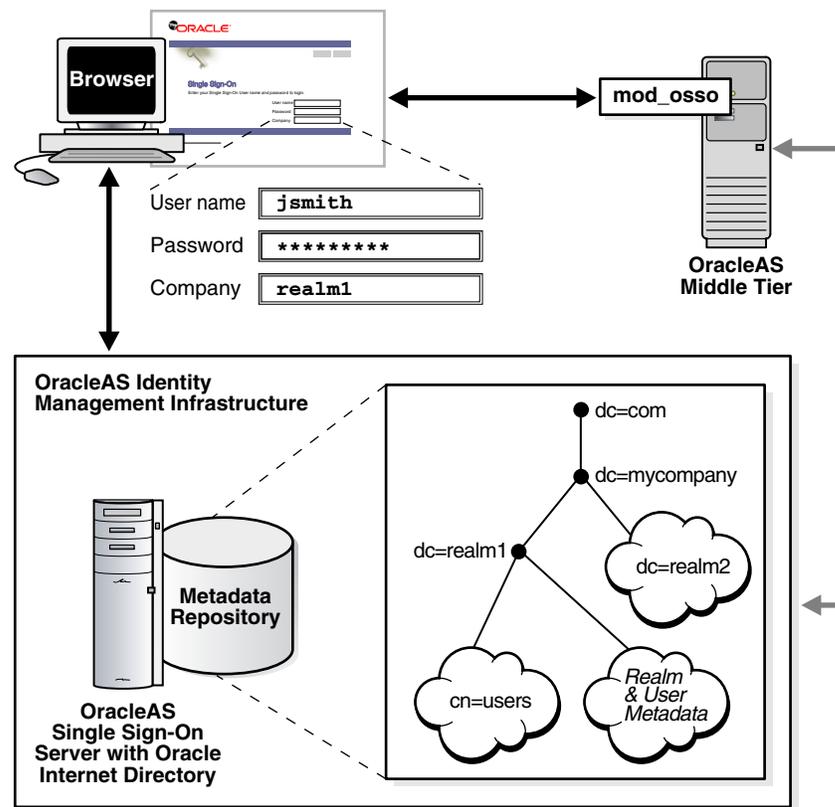
The authentication sequence for single sign-on to multiple realms is much the same as it is for single sign-on in a single, default realm. The only difference from the user's perspective is that, when the user affiliated with the first type of realm is presented with the login screen (see [Figure 10-1](#) on page 10-3), he or she must enter not only a user name and password but also a new credential: the realm nickname. The value entered can be case insensitive.

This section covers the following topics:

- [Locating Realms in Oracle Internet Directory](#)
- [Validating Realm-Affiliated Users to Partner Applications](#)

Locating Realms in Oracle Internet Directory

Once a user has entered his credentials, both his realm nickname and user name are mapped to entries in Oracle Internet Directory. More specifically, the single sign-on server uses directory metadata to find the realm entry in the directory. Once it finds this entry, the single sign-on server uses realm metadata to locate the user. Once the user's entry is found, his password, an attribute of his entry, is validated. And once his password is validated, he is authenticated.

Figure 10–1 The Big Picture: Single Sign-On in Multiple Realms

Validating Realm-Affiliated Users to Partner Applications

Presented with two users, both with the same nickname but affiliated with different realms, a partner application requires some mechanism for distinguishing between these users. The application requires such a mechanism because it must be able to adapt content—an OracleAS Portal page with stock news and stock listings, for instance—to match the needs of the realm requesting it. Accordingly, OracleAS release 9.0.4 adds the realm nickname, realm DN, and realm GUID as attributes passed to `mod_osso`. Recall that `mod_osso` sets a cookie, storing the retrieved attributes as HTTP headers. When deciding what content to offer up, the application may use function calls to retrieve any one of these attributes from `mod_osso` headers.

For detailed information about `mod_osso` headers and the methods used to access them, see the chapter about `mod_osso` in *Oracle Identity Management Application Developer's Guide*.

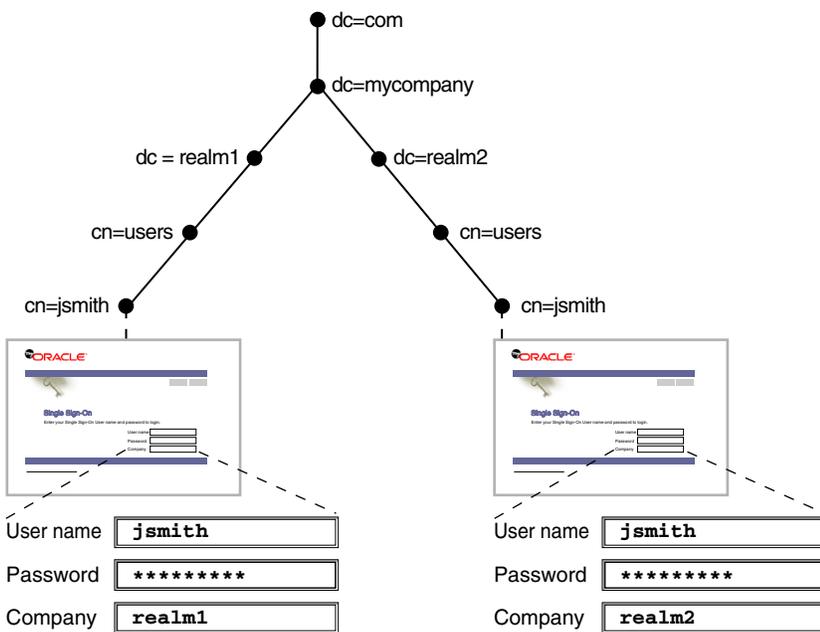
[Figure 10–2](#) on page 10-4 shows how applications running in `mod_osso` see HTTP headers for two users with the same nickname who are affiliated with two different realms. The application uses the headers that appear in bold face to distinguish between the two users. The host, or default realm, in this case is `mycompany.com`.

Figure 10-2 *mod_osso Headers for Users with the Same Name*

```

Realm1
REMOTE_USER = "jsmith"
HTTP_OSSO_USER_DN = "cn=jsmith,cn=users,dc=realm1,dc=mycompany,dc=com"
HTTP_OSSO_USER_GUID = "5D92F6E61F7A4CA7854BF59BA890EBFC"
HTTP_OSSO_SUBSCRIBER = "REALM1"
HTTP_OSSO_SUBSCRIBER_DN = "dc=realm1,dc=mycompany,dc=com"
HTTP_OSSO_SUBSCRIBER_GUID = "F76B7C1945AB4F8DB9391B45D3021334"

Realm2
REMOTE_USER = "jsmith"
HTTP_OSSO_USER_DN = "cn=jsmith,cn=users,dc=realm2,dc=mycompany,dc=com"
HTTP_OSSO_USER_GUID = "6786605E41604E18B74D5B90708F5CA4"
HTTP_OSSO_SUBSCRIBER = "REALM2"
HTTP_OSSO_SUBSCRIBER_DN = "dc=realm2,dc=mycompany,dc=com"
HTTP_OSSO_SUBSCRIBER_GUID = "D9D52D0DC8FF4B6FAF19A795B9B2EA23"
    
```



Configuring the Single Sign-On Server for Multiple Realms

Configuring the single sign-on server for multiple realms involves creating an entry for each realm in the single sign-on schema. Every realm that you create in Oracle Internet Directory must have a corresponding entry in the single sign-on schema.

Note:

- Create the realm in the directory before creating it in the single sign-on schema.
- The configuration scripts that follow work only on UNIX platforms. They cannot be run on Windows platforms.

To configure the single sign-on server for multiple realms, complete the steps that follow. Steps 1, 2, and 5 must be completed only once because these steps enable the

server for multiple realms. Steps 3 and 4 must be completed each time you add a realm.

1. Ensure that you have installed the OracleAS infrastructure and the single sign-on server.
2. Go to `ORACLE_HOME/sso/admin/plsql/wwhost`.

Run the `enblhstg.csh` script using the syntax that follows. See [Table 10-1](#) on page 10-6 for an explanation of script parameters:

```
enblhstg.csh -mode sso
              -sc sso_schema_connect_string
              -ss orasso
              -sw sso_schema_password
              -h oid_host_name
              -p oid_port
              -d "cn=orcladmin"
              -w oid_bind_password
```

Note: If the single sign-on server is part of a distributed deployment, make sure that you run the script on the computer that contains the metadata repository for OracleAS.

Here is an example:

```
enblhstg.csh -mode sso
              -sc webdbsvr2:1521:s901dev3
              -ss orasso
              -sw xyz
              -h dlsun670.us.oracle.com
              -p 389
              -d "cn=orcladmin"
              -w welcome123
```

3. Find a realm or add realms to Oracle Internet Directory. To do this, follow the instructions in *Oracle Internet Directory Administrator's Guide*.

To find an existing realm ID in the SSO server database, use the following SQL query:

```
sqlplus orasso/password
select subscriber_id from wwsub_model$;
```

4. Create an entry for the realm in the single sign-on database. Use the script `ORACLE_HOME/sso/admin/plsql/wwhost/addsub.csh`. Again, if your single sign-on server is part of a distributed deployment, run the script on the computer that contains the metadata repository for OracleAS.

Use the following syntax to execute the script:

```
addsub.csh -name realm_nickname
            -id realm_ID
            -mode sso
            -sc sso_schema_connect_string
            -ss sso_schema_name
            -sw sso_schema_password
            -h oid_host_name
            -p oid_port
            -d oid_bind_dn
            -w oid_bind_dn_password
```

```
-sp sys_schema_password
```

Where *realm_nickname* is the name of the realm that was created using OIDDAS and *realm_ID* is an integer value that does not conflict with any other existing realm value.

Table 10-1 on page 10-6 defines parameters for both `enblhstg.csh` and `addsub.csh`.

Table 10-1 Parameters for `enblhstg.csh` and `addsub.csh`

Parameter	Description
-mode	The value here must be <code>sso</code> .
-sc	The connect string for the single sign-on schema. Use the format <code>host:port:sid</code> .
-ss	The name of the single sign-on schema. This parameter must be <code>orasso</code> .
-sw	The password for the single sign-on schema. See Appendix B to learn how to obtain it.
-h	The host name for the Oracle Internet Directory server.
-p	The port number for the Oracle Internet Directory server.
-d	The bind DN for the Oracle Internet Directory server. The value of this parameter is <code>cn=orcladmin</code> . This is the directory super user.
-w	The password for the Oracle Internet Directory super user, <code>cn=orcladmin</code> .
-name	The realm nickname. This is the value that you enter into the company field on the login page.
-id	The realm ID. Choose any integer greater than 1 that was not previously passed to <code>addsub.sh</code> . (The value 1 is reserved for the default realm.) The single sign-on server uses realm IDs internally, as an index.
-sp	The <code>sys</code> schema password. This password is chosen during the installation of OracleAS.

Note:

- When the script asks you about the duplicated subscriber entry, choose the option to use the existing entry.
 - If you are creating a one-level realm, include the parameters `-sd default_realm_id` and `-type db` in the script.
-
-

5. Stop and then start the single sign-on middle tier:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

Granting Administrative Privileges for Multiple Realms

Oracle Internet Directory propagates the DIT structure of the default realm across realms when it creates these realms. Note, however, that the users, groups, and privileges that exist in the DIT of the default realm are not propagated. The directory

super user or realm administrator must assign, or reassign, privileges, using Oracle Directory Manager. To learn how to use the tool for this purpose, see "[Granting Administrative Privileges](#)" in [Chapter 2](#).

Monitoring the Single Sign-On Server

This chapter explains how to use Oracle Enterprise Manager, the Oracle system management console, to monitor the single sign-on server.

The chapter contains the following topics:

- [Setting the Database Monitoring Password](#)
- [Accessing the Monitoring Pages](#)
- [Interpreting and Using the Home Page on the Standalone Console](#)
- [Interpreting and Using the Details of Login Failures Page](#)
- [Updating the Port Property for the Single Sign-On Monitoring Target](#)
- [Using the OracleAS Web Cache Instance to Monitor the Server](#)
- [Monitoring a Single Sign-On Server Enabled for SSL](#)

Setting the Database Monitoring Password

The data used for monitoring OracleAS Single Sign-On is stored in an Oracle database, and the Oracle Enterprise Manager provides the user interface for monitoring. The Oracle Enterprise Manager connects to the Oracle database using a user name and password. For single sign-on monitoring to work properly, you must set a database monitoring password in the Oracle Enterprise Manager.

See the section on specifying new target monitoring credentials in *Oracle Enterprise Manager Advanced Configuration* for details.

Accessing the Monitoring Pages

The single sign-on monitoring UI on the standalone console consists of two pages: the home page and the Details of Login Failures page. The first provides general information about server load and user activity. The second provides a login failure profile for a particular user.

To access the home page for single sign-on monitoring:

1. Go to the standalone console for the instance of Oracle Enterprise Manager that you want to administer.

Enter the host name of the computer that hosts the OracleAS instance and the port number of Oracle Enterprise Manager. The default port number is 1156. You can find the instance-specific port number as follows:

UNIX: `ORACLE_HOME/install/setupinfo.txt`

Windows: `ORACLE_HOME\install\setupinfo.txt`

2. Log in using the credentials of an OracleAS administrator.
3. From the **Standalone Instances** section of the Farm page, choose the appropriate OracleAS instance.
4. From the **System Components** list of the Application Server page, choose the single sign-on server.

Interpreting and Using the Home Page on the Standalone Console

The home page, reproduced in [Figure 11-1](#) on page 11-3, displays the following metrics in the **General** section:

- **Status**
A green up arrow signifies that the single sign-on server is running. A red down arrow signifies that the server is not running.
- **Start Time**
The start time of the database serving the single sign-on schema.
- **Database**
SID/instance name of the database serving the single sign-on schema.
- **Database Version**
Version of the database serving the single sign-on schema.

The **Last 24 Hours Status Details** section contains the following metrics:

- **Logins**
- **Successful Logins**
- **Failed Logins**

As the heading implies, the statistics displayed are for the previous 24 hours.

The **Login Failures During the Last 24 Hours** section enables you to determine the number of login failures that have occurred during the previous 24 hours. You choose a name from the Login Failures During the Last 24 Hours table. You then choose the associated link under the **Failures** heading. When populated, this link contains the number of login failures for the user. Clicking it takes you to the Details of Login Failures page.

Figure 11–1 Monitoring Home Page for OracleAS Single Sign-On

ORACLE Enterprise Manager 10g
Application Server Control

Logs Topology Preferences Help

Farm > Application Server: infra.stadv11.us.oracle.com >

Single Sign-On: orasso

Page Refreshed Jan 31, 2006 10:37:37 AM

General

Status ↑
 Start Time Dec 19, 2005 3:12:12 AM
 Database infra1b
 Database Version 10.1.0.4.2

Last 24 Hours Status Details

Logins 0
 Successful Logins 87.3%
 Failed Logins 12.7%

Login Failures During The Last 24 Hours

Username	Failures
ORCLADMIN	1,251

Related Links

[Administer via Single Sign-On Web Application](#) [All Metrics](#) [HTTP Server](#)

Single Sign-On administration requires you to authenticate as a privileged user defined in Oracle Internet Directory. Log in as 'orcladmin' or another user belonging to the 'AS Administrators' group.

Logs | Topology | Preferences | Help

Copyright © 1996, 2005, Oracle. All rights reserved.
 About Oracle Enterprise Manager 10g Application Server Control

The **Related Links** section contains the following links:

- [HTTP Server](#)
Takes you to the monitoring home page for the Oracle HTTP Server
- [Administer via Single Sign-On Web Application](#)
Takes you to the home page for single sign-on administration

Interpreting and Using the Details of Login Failures Page

Clicking a link in the Login Failures During the Last 24 Hours table takes you to the Details of Login Failures page (Figure 11–2). This page contains a table that displays login failure times and associated IP addresses for a particular user.

Figure 11–2 Details of Login Failures Page

ORACLE Enterprise Manager 10g
Application Server Control

Logs Topology Preferences Help

Farm > Application Server: infra.stadv11.us.oracle.com > Single Sign-On: orasso >

Details of Login Failures: ORCLADMIN

Page Refreshed Jan 31, 2006 10:40:22 AM

Details of Login Failures:

I.P. Address	Failure Login Time
130.35.48.245	Jan 31, 2006 10:39:25 AM
130.35.48.245	Jan 31, 2006 10:39:24 AM
130.35.48.245	Jan 31, 2006 10:39:24 AM
130.35.48.245	Jan 31, 2006 10:39:24 AM
130.35.48.245	Jan 31, 2006 10:39:24 AM
130.35.48.245	Jan 31, 2006 10:39:24 AM
130.35.48.245	Jan 31, 2006 10:39:24 AM
130.35.48.245	Jan 31, 2006 10:29:16 AM
130.35.48.245	Jan 31, 2006 10:29:16 AM
130.35.48.245	Jan 31, 2006 10:29:16 AM

Copyright © 1996, 2005, Oracle. All rights reserved.
About Oracle Enterprise Manager 10g Application Server Control

Updating the Port Property for the Single Sign-On Monitoring Target

A change in the port number of the Oracle HTTP Server requires a change in the port property of the single sign-on monitoring target on that server. Perform these steps to effect the change:

1. Back up the `targets.xml` file:

```
cp ORACLE_HOME/sysman/emd/targets.xml ORACLE_HOME/sysman/emd/
targets.xml.backup
```

This file is the configuration file for the various "targets" that Oracle Enterprise Manager monitors, one of which is OracleAS Single Sign-On.

2. In `targets.xml`, find the target type `oracle_sso_server`; then locate and edit the HTTP port value associated with this target type:

```
<Property NAME="HTTPPort" VALUE="7777" />
```

3. Save and close the file.
4. Reload the OracleAS Console:

```
ORACLE_HOME/bin/emctl reload
```

Note: For more information about port dependency changes, see the appendix about port numbers in *Oracle Application Server Administrator's Guide*.

Using the OracleAS Web Cache Instance to Monitor the Server

If you are using OracleAS Web Cache as a load balancer for multiple single sign-on instances, you can monitor the single sign-on server from the OracleAS Web Cache computer. At the same time, you can use the monitoring pages on any one of the single sign-on instances to monitor that instance.

Follow these steps to add a single sign-on target to the OracleAS Web Cache instance:

1. Back up the file `ORACLE_HOME/sysman/emd/targets.xml` located on the OracleAS Web Cache instance.
2. Copy the single sign-on target definition from a `targets.xml` file located on a single sign-on instance. Paste the definition to the end of the `targets.xml` file on the OracleAS Web Cache instance, inserting it just before the closing tag `</Targets>`.
3. In the `Target TYPE` tag, replace the name of the `oracle_ias` target for single sign-on instance with the name of the `oracle_ias` target for the OracleAS Web Cache instance.
4. Replace the single sign-on `OracleHome` value with the OracleAS Web Cache `OracleHome` value.
5. Change `HTTPMachine`, `HTTPPort`, and `HTTPProtocol` to values that correspond to the OracleAS Web Cache instance.
6. Run this command to incorporate the changes:

```
ORACLE_HOME/bin/emctl reload
```

Monitoring a Single Sign-On Server Enabled for SSL

The following are guidelines if you are monitoring a single sign-on server enabled for SSL (whether or not you are using Grid Control monitoring):

- The `oracle_sso_server` target type in the `ORACLE_HOME/sysman/emd/targets.xml` file on the single sign-on middle tier must have the appropriate HTTP attributes.

If, for example, you connect to an SSL-enabled single sign-on server with this URL:

```
http://myhost.us.oracle.com:4443/sso
```

then `HTTPPort` is 4443 and `HTTPProtocol` is `https`.

For details, see ["Update targets.xml"](#) in [Chapter 7](#).

- The certificate configuration file for Oracle Enterprise Manager must contain the certificate of the infrastructure server.

To learn how to add the certificate to the configuration file, see the chapter about Oracle Enterprise Manager security in *Oracle Enterprise Manager Advanced Configuration*. See specifically the section about configuring beacons to monitor Web applications over HTTPS.

Creating Deployment-Specific Pages

Oracle Application Server Single Sign-On provides a framework for integrating deployment-specific login, change password, and single sign-off pages with the single sign-on server. This means that you can tailor these pages to your UI look and feel and globalization requirements.

Oracle recommends that you use JavaServer (JSP) pages. Other Web technologies may provide inconsistent results. PLSQL pages are not supported. Sample pages are provided with the product. The Oracle Application Server Single Sign-On product ships with sample pages that are designed for testing with the Oracle Application Server.

This chapter contains the following topics:

- [How the Single Sign-On Server Uses Deployment-Specific Pages](#)
- [How to Write Deployment-Specific Pages](#)
- [Page Error Codes](#)
- [Adding Globalization Support](#)
- [Guidelines for Deployment-Specific Pages](#)
- [Installing Deployment-Specific Pages](#)
- [Examples of Deployment-Specific Pages](#)

How the Single Sign-On Server Uses Deployment-Specific Pages

The process that enables single sign-on pages can be summarized as follows:

1. The user requests a partner application and is redirected to the single sign-on server.
2. If the user is not authenticated, the single sign-on server redirects the user to the sample login page or to a deployment-specific page. As part of the redirection, the server passes to the page the parameters contained in [Table 12-1](#) on page 12-3.
3. The user submits the login page, passing the parameters contained in [Table 12-2](#) on page 12-3 to the authentication URL:

```
http://sso_host:sso_port/sso/auth
```

or

```
https://sso_host:sso_ssl_port/sso/auth
```

At least two of these parameters, `ssousername` and `password`, appear on the page as modifiable fields.

4. If the user's password is not set to expire soon, and the single sign-on server successfully verifies the user name and password, the server redirects the user to the success URL of the application. If authentication fails, the server redirects the user back to the login page and displays an error message.
5. If the user's password is set to expire soon, the single sign-on server presents the change password page instead of the login page. Again, if the server is configured to use a deployment-specific change password page, it redirects the user to the URL for this page, passing to the page the parameters contained in [Table 12-3](#) on page 12-4.

Note: In step 5, the same conditions apply if the directory administrator forces the user to change the password, password expiration notwithstanding.

The user submits the change password page, entering her old password, new password, and new password confirmation. The page passes the parameters contained in [Table 12-4](#) on page 12-5 to the change password URL:

```
http://sso_host:sso_port/sso/ChangePwdServlet
```

or

```
https://sso_host:sso_ssl_port/sso/ChangePwdServlet
```

If an error occurs, the single sign-on server redirects the user to the change password page and displays an error message. See "[Change Password Page Behavior](#)" in [Chapter 3](#) for a detailed discussion of conditions under which errors may occur.

If the password change is successful, the user is redirected to the partner application URL that triggered the authentication request.

6. To finish the single sign-on session, the user clicks **Logout** in the partner application he or she is working in. This act calls application logout URLs in parallel, logging the user out from all accessed applications and ending the single sign-on session.
7. The user is redirected to the single sign-on server, which presents the single sign-off page. If the server is configured to use a deployment-specific page, it redirects the user to the URL for this page, passing to the page the parameters contained in [Table 12-5](#) on page 12-5.
8. The user can click **Return** on the single sign-off page to return to the application from which logout was initiated.

Note: The change password page can be used to change a password only when the password is about to expire. The UI for Oracle Delegated Administration Services can be used for this purpose at any time. See "[Change Password Page Behavior](#)" in [Chapter 3](#) for more about this topic.

How to Write Deployment-Specific Pages

The URLs for login, change password, and single sign-off pages must accept the parameters described in the tables that follow if these pages are to function properly.

This section contains the following topics:

- [Login Page Parameters](#)
- [Forgot My Password](#)
- [Change Password Page Parameters](#)
- [Single Sign-Off Page Parameters](#)

Login Page Parameters

The URL for the login page must accept the parameters listed in [Table 12–1](#) on page 12-3.

Table 12–1 Login Page Parameters Submitted to the Page by the Single Sign-On Server

Parameter	Description
site2pstoretoken	Contains the authentication request token for login processing.
ssusername	Contains the username.
p_error_code	Contains the error code in the form of a string. Passed when an error occurs during authentication.
p_cancel_url	Contains the URL to redirect to if the user clicks Cancel —if such a button exists on the login page. This URL points to the home URL of the partner application from which login was initiated.
locale	User’s language preference (optional). Must be in ISO format. For example, French is <code>fr-fr</code> . For more about this parameter, see "Adding Globalization Support" .

The login page must pass the parameters listed in [Table 12–2](#) to the authentication URL:

```
http://sso_host:sso_port/sso/auth
```

Table 12–2 Login Page Parameters Submitted by the Page to the Single Sign-On Server

Parameter	Description
site2pstoretoken	Contains the redirect URL information for login processing.
ssusername	Contains the username. Must be UTF-8 encoded.
password	Contains the password entered by the user. Must be UTF-8 encoded.
subscribername	The subscriber nickname when realms are enabled. Must be UTF-8 encoded. Note: This field is required on the login page only when multiple realms are enabled in the single sign-on server.
locale	User’s language preference (optional). Must be in ISO format. For example, French is <code>fr-fr</code> . For more about this parameter, see "Adding Globalization Support" .
v	Contains the page version. Recommended but optional. If the parameter is passed, its value must be <code>v1.4</code> .

The login page must have at least two fields: a text field with the parameter name `ssusername` and a password field with the parameter name `password`. The values are submitted to the authentication URL. The login page must also include

`site2pstoretoken` as a hidden parameter. It must submit this parameter to the login URL.

In addition to submitting these parameters, the login page is responsible for displaying appropriate error messages, as specified by `p_error_code`, redirecting to `p_cancel_url` if the user clicks **Cancel**.

Forgot My Password

When building your login page, you may want to configure it with a link that enables users to reset their passwords. This URL can go either to the home page for Oracle Delegated Administration Services or to the **Forgot My Password** link within Oracle Delegated Administration Services. Users who click the **Forgot My Password** link are challenged with a question. They must successfully answer this question before their password is reset.

Oracle Delegated Administration Services is generally available on the same computer as OracleAS Single Sign-On at a URL of the following form:

```
http://sso_host:sso_port/oiddas/
```

To learn how the Forgot My Password link is used to reset passwords, see the chapter about the Oracle Internet Directory Self-Service Console in *Oracle Identity Management Guide to Delegated Administration*.

Change Password Page Parameters

The URL for the change password page must accept the parameters listed in [Table 12-3](#).

Table 12-3 *Change Password Parameters Submitted to the Page*

Parameter	Description
<code>p_username</code>	Contains the user name to be displayed somewhere on the page.
<code>p_subscribername</code>	The subscriber nickname when hosting is enabled. Note: This field is required on the login page.
<code>p_error_code</code>	Contains the error code, in the form of a string, if an error occurred in the prior attempt to change the password.
<code>p_done_url</code>	Contains the URL of the appropriate page to return to after the password is saved.
<code>site2pstoretoken</code>	Contains the <code>site2pstoretoken</code> that is required by the <code>/sso/auth</code> login URL if the password has expired or is about to expire.
<code>p_pwd_is_exp</code>	Contains the flag value indicating whether the password has expired or is about to expire. The value can be either <code>WARN</code> or <code>FORCE</code> . See Table 12-8 for the associated error codes.
<code>locale</code>	User's language preference (optional). Must be in ISO format. For example, French is <code>fr-fr</code> . For more about this parameter, see "Adding Globalization Support" .

The change password page must pass the parameters listed in [Table 12-4](#) to the change password URL:

```
http://sso_host:sso_port/sso/ChangePwdServlet
```

Table 12–4 *Change Password Page Parameters Submitted by the Page*

Parameter	Description
p_username	Contains the user name to be displayed somewhere on the page. Should be posted as a hidden field by the change password page. Must be UTF-8 encoded.
p_old_password	Contains the user's old password. Must be UTF-8 encoded.
p_new_password	Contains the user's new password. Must be UTF-8 encoded.
p_new_password_confirm	Contains the confirmation of the user's new password. Must be UTF-8 encoded.
p_done_url	Contains the URL of the appropriate page to return to after the password is saved.
p_pwd_is_exp	Contains the flag value indicating whether the password has expired or is about to expire. The value can be either <code>WARN</code> or <code>FORCE</code> . See Table 12–8 for the associated error codes.
site2pstoretoken	Contains the redirect URL information for login processing.
p_action	Commits changes. The values must be either <code>OK</code> (commit) or <code>CANCEL</code> (ignore).
p_subscribername	Contains the user name to be displayed somewhere on the page.
p_request	Protected URL requested by the user.
locale	User's language preference (optional). Must be in ISO format. Example: French is <code>fr-fr</code> . See " Adding Globalization Support ".

The change password page must have at least three password fields: `p_old_password`, `p_new_password`, and `p_new_password_confirm`. The page should submit these fields to the change password URL.

The page should also submit `p_done_url` as a hidden parameter to the change password URL. In addition, it should display error messages according to the value of `p_error_code`.

Single Sign-Off Page Parameters

The URL for the single sign-off page must accept the parameters listed in [Table 12–5](#).

Table 12–5 *Parameters Submitted to the Single Sign-Off Page*

Parameter	Description
p_app_name[1. . .n]	Contains the application name to be displayed on the page. The variable <code>n</code> stands for the number of partner applications participating in single sign-off.
p_app_logout_url[1. . .n]	Contains the application logout URL. The variable <code>n</code> stands for the number of partner applications participating in single sign-off.
p_done_url	Contains the return URL. This URL returns users to the application from which they initiated logout.
locale	User's language preference in ISO format. Sent only if the user does not pass the same value during login.

External Application Login Page Parameters

The URL for external application login pages must accept the parameters listed in [Table 12–6](#).

Table 12–6 Parameters Submitted to the External Application Login Page

Parameter	Description
ID	The external application ID. This ID appears on the Administer External Application page. For each external application configured in OracleAS Single Sign-On, a unique ID is generated. This ID is the primary key in the external application-related tables. The external application login page must pass this ID back to the application.
p_app_name	Contains the application name to be displayed on the page. This is the name for the external application that was provided when the application was configured in OracleAS Single Sign-On.
extappfieldname1..9	Extra field names. Each external application can have up to nine extra fields associated with it. These fields can be visible or non-visible. Visible fields appear on the external application login page, and the user can change the default value of the field. The non-visible field values are also submitted to the external application, but the user cannot change their value. For example, for an application that has login, password, and locale fields, you can add a field named LO with a value of FR. See "Adding an External Application" on page 5-1 for details.
extappfieldvalue1..9	Extra field values.
extappfielddisplay1..9	Extra field visibility (true or false). Determines if the field is visible to the user and is modifiable (true) or if the field has a fixed value (false).
mode	This parameter may or may not be passed to the custom login page. If it is passed to the login page, it must be submitted with its value set to <code>modify</code> . This indicates to the single sign-on application controller that the external application login page has been called from the portal to update the user's credentials in the database.
p_error_code	Contains the error code, in the form of a string, if an error occurred in the prior attempt to change the password.
done	The URL to which the response must be redirected after the user's credentials have been updated. This is used with <code>modify</code> mode.

This page must be able to submit the parameters shown in [Table 12–7](#) using the POST method to the external application login controller:

Table 12–7 Parameters the External Application Login Page Submits to the Application

Parameter	Description
ID	The external application ID.
p_app_username	Contains the user name of the person logging in to the application.
p_app_pwd	The password that the user submits.

Table 12–7 (Cont.) Parameters the External Application Login Page Submits to the

Parameter	Description
p_remember_credentials	Flag that indicates to the external application login controller if the application user name and password must be saved to the database.
extappfieldname1..9	Extra field names. See Table 12–6 for details.
extappfieldvalue1..9	Extra field values.
extappfielddisplay1..9	Extra field visibility (true/false). See Table 12–6 for details.
p_change_password	A true/false flag that indicates to the external application login controller if the mode is set to <code>change password</code> .
mode	This parameter may or may not be passed to the custom login page. If it is passed to the login page, it must be submitted with its value set to <code>modify</code> . This indicates to the single sign-on application controller that the external application login page has been called from the portal to update the user's credentials in the database.
done	The URL to which the response must be redirected after the user's credentials have been updated.

Page Error Codes

URLs for login and change password pages must accept the process errors described in the tables that follow if these pages are to function properly.

Login Page Error Codes

The login page must process the error codes listed in [Table 12–8](#).

Table 12–8 Login Page Error Codes

Value of p_error_code	Corresponding message and description
acct_lock_err	Description: The user has committed too many login failures. Message: "Your account is locked. Please notify the system administrator."
pwd_exp_err	Description: The user's password has already expired. Message: "Your password has expired. Please contact the administrator to reset it."
null_uname_pwd_err	Description: The user left the user name field blank. Message: "You must enter a valid user name."
auth_fail_exception	Description: Authentication has failed. Message: "Authentication failed. Please try again."
null_password_err	Description: The user left the password field blank. Message: "You must enter your logon password."

Table 12–8 (Cont.) Login Page Error Codes

Value of p_error_code	Corresponding message and description
sso_forced_auth	<p>Description: The application requires authentication.</p> <p>Message: "The application you are trying to access requires you to sign in again even if you have signed in previously."</p>
unexpected_exception	<p>Description: An unexpected error occurred during authentication.</p> <p>Message: "An unexpected error occurred. Please try again."</p>
unexp_err	<p>Description: Unexpected error.</p> <p>"Unexpected Error. Please contact Administrator."</p>
internal_server_err	<p>Description: Internal server error report.</p> <p>Message: "Internal Server Error. Please contact Administrator."</p>
internal_server_try_again_err	<p>Description: Internal server error report with "try again" prompt.</p> <p>Message: "Internal Server Error. Please retry the operation."</p>
internal_server_try_later_err	<p>Description: Internal server error report with "try later" prompt.</p> <p>Message: "Internal Server Error. Please try the operation later."</p>
gito_err	<p>Description: Inactivity timeout. User must log in again.</p> <p>Message: "Your Single Sign_on session has expired. For your security, your session expires after some duration of inactivity. Please sign in again."</p>
cert_auth_err	<p>Description: Certificate sign-on has failed. User should check that the certificate is valid or should contact the administrator.</p> <p>Message: "Certificate-based sign in failed. Please ensure that you have a valid certificate or contact the administrator."</p>
session_exp_error	<p>Description: Single sign-on session time limit reached.</p> <p>Message: "Your Single Sign-On session has expired. For your security, your session expires after the specified amount of time. Please sign in again."</p>
userid_mismatch	<p>Description: The user ID presented during a forced authentication does not match the user ID in the current single sign-on session.</p> <p>Message: "The user name submitted for authentication does not match the user name present in the existing Single Sign-On session."</p>

Post-Login Messages

The messages listed in [Table 12-9](#) appear after the user authenticates. They are processed by the login page but may appear with the password change page.

Table 12-9 Post-Login Messages

Value of p_error_code	Corresponding message and description
pwd_expiry_warn_err	Description: The user's password will expire soon. Message: "Your password is about to expire. Please change it."
pwd_force_change_err	Description: The user's password has expired and the user is expected to change it. Message: "You must change your password before you can continue."
pwd_grace_login_err	Description: The user's password has expired, but a grace period is in effect for resetting it. Message: "Your password has expired. You are now in the grace login period. Please change your password."

Change Password Page Error Codes

The change password page must process the error codes listed in [Table 12-10](#).

Table 12-10 Change Password Page Error Codes

Value of p_error_code	Corresponding Error
confirm_pwd_fail_txt	The old and the new password do not match.
null_new_pwd_err	The user did not enter a new password.
null_old_pwd_err	The user did not enter the old password.
pwd_expiry_warn_err	The password is about to expire.
pwd_force_change_err	The password must be changed before the user can proceed.
pwd_grace_login_err	The password has expired, but a grace login is permitted.
account_deactivated_err	The user account is disabled.
acct_lock_err	The user account is locked.
pwd_illegal_value	The password contains an illegal value.
pwd_in_history_err	The password is in the password history.
pwd_min_length_err	The password does not meet the minimum length requirement.
pwd_numeric	The password does not meet the numeric character requirement.

Change External Application Login Page Error Codes

The external application login page must process the error codes listed in [Table 12-10](#).

Table 12-11 External Application Login Page Error Codes

Value of p_error_code	Corresponding Error
eapp_name_null	The user ID is missing.
eapp_pwd_null	The password is missing.

Table 12–11 (Cont.) External Application Login Page Error Codes

Value of p_error_code	Corresponding Error
ext_app_not_found	The external application cannot be identified.

Adding Globalization Support

The OracleAS Single Sign-On framework enables you to globalize deployment-specific pages to fit the needs of your deployment. When deciding what language to display the page in, you can adopt different strategies. Two strategies are presented in the following sections.

For a complete list of the language codes supported, see Appendix A in *Oracle Application Server Globalization Guide* at the following URL:

<http://www.oracle.com/technology/documentation/index.html>

From the landing page for the URL, click a link for the OracleAS Single-Sign on documentation, then click the View Library link to view the library for the appropriate release.

Deciding What Language to Display the Page In

This section explains how to use either the HTTP Accept-Language header or deployment page logic to choose a language to display.

Use the Accept-Language Header to Determine the Page

Browsers enable end users to decide the language (locale) they would like to view their Web content in. The browser sends the language that the user chooses to the server in the form of the HTTP Accept-Language header. The logic of the deployment-specific page must examine this header and render the page accordingly. When it receives this page, the single sign-on server takes note of the header value for Accept-Language and sends it to partner applications when it propagates the user's identity. Note that, although many partner applications enable users to override this header, the single sign-off page appears in the language established at sign-on. The net effect is a consistent session language for all partner applications.

The Accept-Language header is the preferred mechanism for determining the language preference. A major benefit of this approach is that end users have typically already set their language preference while browsing other Web sites. The result is browsing consistency between these pages and single sign-on pages.

Use Page Logic to Determine the Language

Although Oracle recommends the approach described in the preceding section, you may choose to implement globalization based on mechanisms that extend or override the language preference set in the browser. You may, for instance, do one of the following:

- Display a list of languages on the login page and allow the user to select from this list. As a convenience to the user, you can make this selection persistent by setting a persistent cookie.
- Render the page in one, fixed language. This method is appropriate when you know that the user population is monolingual.

- Obtain language preferences from a centralized application repository or a directory. A centralized store for user and system preferences and configuration data is ideal for storing language preferences.

If you use page logic to set language preferences, the page must propagate this information to the single sign-on server. The server must propagate this information to partner applications. The net result is a consistent globalization experience for the user. Your page must pass the language in ISO-639 format, using the `locale` parameter (Table 12–2) in the login form. A number of sites contain a full list of ISO-639 two-letter language codes. Here is one of them:

<http://www.ics.uci.edu/pub/ietf/http/related/iso639.txt>

Here is a site that contains a full list of ISO-3166 two-letter country codes:

http://www.chemie.fu-berlin.de/diverse/doc/ISO_3166.html

Note: In the event that the `locale` parameter is passed to the single sign-on server (Table 12–1), the parameter value is sent to `mod_osso`. `mod_osso` prefixes this value to the HTTP Accept-Language header before passing the header to partner applications.

Rendering the Page

Once it determines the end-user's locale, the deployment-specific page must use the corresponding translation strings to render the page. To learn how to store and retrieve these strings, see the chapter about locale awareness in *Oracle Application Server Globalization Guide*. You may also want to consult standard documents about Java development. Here are two links:

- Java Internationalization Guide:
<http://java.sun.com/j2se/1.4.2/docs/guide/intl/index.html>
- General link for Java documentation:
<http://java.sun.com/j2se/1.4.2/docs>

Guidelines for Deployment-Specific Pages

When implementing deployment-specific pages, observe the following guidelines:

- Oracle recommends that login and change password pages be protected by SSL.
- The login and change password pages must code against cross-site scripting attacks.
- The login and change password pages must have auto-fill and caching set to `off`. This prevents user credentials from being saved or cached in the browser. Here is an example of the `AutoComplete` tag:

```
<FORM NAME="foo" AutoComplete="off" METHOD="POST" ACTION="bar">
```

- Oracle recommends that you configure your login page to display a banner that warns against unauthorized access. You may, for example, want to use the following text or a variant thereof:

```
Unauthorized use of this site is prohibited and may subject you to civil and criminal prosecution.
```

- Deploy the login and change password pages on the computer that hosts the single sign-on server. This makes it easier to detect false versions of these pages.

Installing Deployment-Specific Pages

Use the `policy.properties` file to install deployment-specific login and change password pages.

Using `policy.properties` to Install Login, Single Sign-Off, and Change Password Pages

You can configure login, single sign-off, and change password pages.

To install your own login, single sign-off, and change password pages:

1. Edit the parameters in `ORACLE_HOME/sso/conf/policy.properties`. Substitute the paths to your login, logout, and password change pages for the values shown in the example:

```
#Deployment login page link
loginPageUrl = /sso/pages/login.jsp
logoutPageUrl = /sso/pages/logout.jsp

#Deployment change password page link
chgPasswordPageUrl = /sso/pages/password.jsp
```

2. Restart the single sign-on server:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

Using `policy.properties` to Install Wireless Login and Change Password Pages

OracleAS Wireless has its own framework for integrating deployment-specific wireless login and change password pages. The procedure for installing these pages is similar to that used to install standard pages (section immediately preceding).

To install wireless login and change password pages:

1. Open `ORACLE_HOME/sso/conf/policy.properties`.
2. Edit or add the following parameters:

```
#Wireless login page link
wirelessLoginPageUrl = wireless_login_page_url
wirelessChgPasswordPageUrl = change_password_page_URL
```

3. Restart the single sign-on server:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

Using `policy.properties` to Install External Application Login Pages

You can configure login pages that are presented to users when they log in to third-party applications.

To configure login pages for third-party applications:

1. Be sure these pages accept the page parameters and page error codes discussed in "[Login Page Parameters](#)" on page 12-3 and "[Page Error Codes](#)" on page 12-7.

2. After configuring the login pages, edit the `extAppLoginPageUrl` parameter in `ORACLE_HOME/sso/conf/policy.properties`, substituting the path to your login page for the path shown in the following example:

```
extAppLoginPageUrl = /sso/pages/ealgin.jsp
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

3. Optionally, you can configure the application page
4. Restart the single sign-on server:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

Examples of Deployment-Specific Pages

The `ipassample.jar` file contains the files `login-ex.jsp`, `password-ex.jsp`, and `signoff-ex.jsp`. You may customize these to suit your deployment. If you want to use these files, see ["Obtaining the Sample Files"](#) in [Chapter 2](#).

Using Custom Classes

In general, customized deployment-specific pages must operate with the current versions of component classes in use by `OC4J_SECURITY`. If your custom application needs to use a different version of a given class, you must deploy that class in a separate `OC4J` instance and *not* in the `OC4J_SECURITY` instance.

For example, if your deployment requires the use of custom `log4j` classes that conflict with the versions in use by `OC4J_SECURITY`, start a separate `OC4J_SECURITY` instance that uses a local `log4j.jar` file containing the custom classes.

WARNING: Replacing the classes used by `OC4J_SECURITY` with custom versions may render OracleAS Single Sign-On or other Oracle Application Server components unusable.

Integrating with Oracle Identity Federation

This chapter explains how to implement federated authentication using Oracle Application Server Single Sign-On and Oracle Identity Federation. Federated single sign-on permits users to access information on different corporate Web sites while authenticating to only one of those sites. You can configure either Oracle Application Server Single Sign-On or Oracle Identity Federation to be the authentication mechanism for users who want to access resources that are protected by either product.

The chapter contains the following topics:

- [How Federated Single Sign-On Works](#) on page 13-1
- [Configuring the Oracle Stack as the Service Provider](#) on page 13-2
- [Configuring the Oracle Stack as the Identity Provider](#) on page 13-4

Note: This chapter only describes how to configure single sign-on to Oracle Identity Federation from the standpoint of the Oracle Application Server Single Sign-On product. To complete the configuration, you also need to modify settings in the Oracle Identity Federation product. See the *Oracle Secure Federation Services Administration Guide* for details.

How Federated Single Sign-On Works

Users need a simple way to move back and forth between content that is provided on different corporate Web sites. Corporate Web sites need a way to authenticate and authorize users who are entering from different domains that use different security products. The Oracle Identity Federation product addresses these problems.

When a user tries to access a protected resource on a remote Web site, the Oracle Identity Federation product at the user's site transfers information about the user to the remote site for use in authorizing the user's request. For example:

- Users from an airline can access technical documentation in an airplane vendor's documentation database.
- Customers of a wireless company can access a bill-paying application that is outsourced from the vendor to a third-party supplier.
- Employees of an organization can access a 401(k) application through an internal HR portal that connects to the benefits provider.

Users might access a link on their own company's Web site to request access to content on a partner's Web site. The first time users request access, they are authenticated on

their own site with user profile information stored in their home site's user data repository. The user's home (or Identity Provider) domain forwards the user's access request to the destination (a Service Provider) site along with the credentials that the destination site needs to authorize the user's request.

Using the integration between OracleAS Single Sign-On and Oracle Identity Federation, the following is possible:

- When a user attempts to access a protected resource, the provider of the resource can send the query to Oracle Identity Federation, which can forward the query to OracleAS Single Sign-On.

Once the user is authenticated by OracleAS Single Sign-On, he or she can access resources at the destination.

- When a user attempts to access a resource protected by OracleAS Single Sign-On, the request can be forwarded to Oracle Identity Federation, which can locate an appropriate Identity Provider to perform authentication.

Once a user has been authenticated by the Identity Provider, he or she can access resources protected by OracleAS Single Sign-On.

For more information on Oracle Identity Federation, see the *Oracle Secure Federation Services Administration Guide*, available from the Oracle Documentation page on the Oracle Technology Network. The URL is as follows:

<http://www.oracle.com/technology/documentation>

Federated Single Sign-On From the User's Perspective

After completing configuration of federated single sign-on as described in this chapter, users perform a one-time authentication to both the Service Provider and the Identity Provider.

After this one-time authentication, the user only provides credentials to the Identity Provider. After authenticating, the user is able to access protected resources at the Service Provider.

Configuring the Oracle Stack as the Service Provider

When OracleAS Single Sign-On and Oracle Identity Federation perform the role of Service Provider, OracleAS Single Sign-On delegates user authentication to Oracle Identity Federation. In this scenario, you configure federated single sign-on so that Oracle Identity Federation is the intermediary that identifies an Identity Provider when users try to access resources that are protected by OracleAS Single Sign-On.

By default, the `MediumHighSecurity` authentication level is used for single sign-on between OracleAS Single Sign-On and Oracle Identity Federation. If you change this authentication level, Oracle recommends that you set the level to, or above, the default authentication level for OracleAS Single Sign-On. If you use a lower level, users will be challenged when they attempt to access any protected application that uses a higher security level.

The following task overview summarizes the steps for this configuration. Detailed procedures are provided after the task overview.

Note: You must stop the OracleAS Single Sign-On server before adding modifying the `policy.properties` file and restart it when you are done.

Task overview: Delegating authentication to an Oracle Identity Federation instance

1. Stop the OracleAS Single Sign-On server.
2. Configure Oracle Identity Federation as the authentication mechanism in the `policy.properties` file.
3. Add applications that are protected by Oracle Identity Federation to the list of protected applications in the `policy.properties` file.
4. Restart the Oracle Application Server Single Sign-On server.
5. Configure the Oracle Identity Federation to authenticate users who try to access the applications added to the `policy.properties` file.

See the *Oracle Secure Federation Services Administration Guide* for details.

To stop the Oracle Application Server Single Sign-On Server

1. From the Oracle Enterprise Manager 10g Application Server Control Console, click the instance of the application server that you want to stop.
2. From the details page for the application server, select `OC4J_SECURITY`.
If you also want to stop Oracle HTTP Server, click the HTTP Server link on the details page for the application server.
3. Click **Stop**.
A confirmation page appears.
4. Click **Yes** on the confirmation page.

To delegate authentication to an Oracle Identity Federation instance

1. Open the following file in a text editor:

```
OSSO_install_dir/sso/conf/policy.properties
```

Where `OSSO_install_dir` is the directory where Oracle Application Server Single Sign-On was installed.

2. Uncomment and edit the following lines:

`SASSOAuthnUrl`—Uncomment this line and change the host name and port to reflect the login URL for Oracle Identity Federation.

`SASSOLogoutUrl`—Uncomment this line and change the host name and port to reflect the logout URL for Oracle Identity Federation.

Note that the colon character (":") must be escaped by a backslash character ("\\"), for example:

```
SASSOAuthnUrl = http\://osfs_host.domain\:port/sso/authn
SASSOLogoutUrl = http\://osfs_
host.domain\:port/sso/jsp/sasso_logout_success.jsp
```

3. Uncomment the following line to set the security level for Oracle Identity Federation:
`SASSOAuthLevel = MediumHighSecurity`
4. In the `policy.properties` file, uncomment the plug-in and audit level for the `MediumHighSecurity` authentication level:

```
# MediumHighSecurity_AuthPlugin =
oracle.security.sso.server.auth.SASSOAuth
```

5. Locate the keystore file (the file name is "keystore") from the installation directory of the server hosting Oracle Identity Federation:

```
Oracle_Identity_Federation_installdir/sso/conf
```

Copy the keystore to the location specified in the SASSOConfigFile parameter in the `policy.properties` file. This location is the relative path from the local home directory for the OracleAS Single Sign-On server. For example:

```
SASSOConfigFile = /sso/conf/keystore
```

See the *Oracle Secure Federation Services Administration Guide* for details on generating the keystore.

6. From the Oracle Enterprise Manager 10g Application Server Control Console, click the instance of Oracle Enterprise Manager 10g that you want to modify.
7. Restart the Oracle HTTP Server and OC4J_SECURITY.

To add applications to be protected by the Oracle Identity Federation policies

1. Stop the server, as described in "To stop the Oracle Application Server Single Sign-On Server" on page 13-3.

2. Edit the `policy.properties` file in the following location:

```
install_dir/sso/conf/policy.properties
```

Where `install_dir` is the directory where Oracle Application Server Single Sign-On is installed.

3. In the Protected URL section of the `policy.properties` file, set the host and port for one or more applications that you want to be protected, for example:

```
host\:port = MediumHighSecurity
```

Where `host\:port` is the host and port of the application to be protected. The host and port are configured during or after installation. See the mid-tier documentation for details. `MediumHighSecurity` is the security level configured for single sign-on with Oracle Identity Federation. (See [Chapter 6, "Multilevel Authentication"](#) on page 6-1 for details on authentication levels.)

4. From the *Oracle Enterprise Manager 10g* Application Server Control Console, click the instance of application server that you want to start.
5. Restart the Oracle HTTP Server and OC4J_SECURITY.

Note: To complete the configuration, you also need to modify settings in the Oracle Identity Federation product. See the *Oracle Secure Federation Services Administration Guide* for details.

Configuring the Oracle Stack as the Identity Provider

When OracleAS Single Sign-On and Oracle Identity Federation perform the role of Identity Provider, Oracle Identity Federation delegates user authentication to OracleAS Single Sign-On. In this scenario, you configure federated single sign-on so that Oracle Identity Federation forwards user requests for resources to OracleAS Single Sign-On. In this case, OracleAS Single Sign-On becomes the authentication mechanism.

By default, the `MediumHighSecurity` authentication level is used for single sign-on between OracleAS Single Sign-On and Oracle Identity Federation. (See [Chapter 6, "Multilevel Authentication"](#) on page 6-1 for details.) If you change this authentication level, Oracle recommends that you set the level to, or above, the default authentication level for OracleAS Single Sign-On. If you use a lower level, users will be challenged when they attempt to access any protected application that uses a higher security level.

Note: To complete the configuration, you also need to modify settings in the Oracle Identity Federation product. See the *Oracle Secure Federation Services Administration Guide* for details.

To configure federated authentication using OracleAS Single Sign-On as the authentication mechanism:

1. Go to the Oracle Enterprise Manager 10g Application Server Control Console.
2. Click the instance of the application server that you want to stop.
3. To prepare for stopping OC4J_SECURITY, from the details page for the application server, select OC4J_SECURITY.
4. To prepare for stopping Oracle HTTP Server, click the HTTP Server link on the details page for the application server.
5. Click **Stop**.

A confirmation page appears.

6. Click **Yes** on the confirmation page.
7. Open the following file in a text editor:

```
OSSO_install_dir/sso/conf/policy.properties
```

Where `OSSO_install_dir` is the directory where Oracle Application Server Single Sign-On was installed.

8. Uncomment and edit the following lines:

SASSOAuthnUrl—Uncomment this line and change the host name and port to reflect the login URL for Oracle Identity Federation.

SASSOLogoutUrl—Uncomment this line and change the host name and port to reflect the logout URL for Oracle Identity Federation.

Note that the colon character (":") must be escaped by a backslash character ("\\"), for example:

```
SASSOAuthnUrl = http\://osfs_host.domain\:port/sso/authn
```

```
SASSOLogoutUrl = http\://osfs_
host.domain\:port/sso/jsp/sasso_logout_success.jsp
```

9. Locate the keystore file (the file name is "keystore") from the installation directory of the server hosting Oracle Identity Federation:

```
Oracle_Identity_Federation_install_dir/sso/conf
```

Copy the keystore to the location specified in the `SASSOConfigFile` parameter in the `policy.properties` file. This location is the relative path from the local home directory for the OracleAS Single Sign-On server. For example:

```
SASSOConfigFile = /sso/conf/keystore
```

See the *Oracle Secure Federation Services Administration Guide* for details on generating the keystore.

10. Restart OC4J_SECURITY and the Oracle HTTP Server.

Adding Federated Authentication URLs to a Web Portal

On a Web portal page, you may want to configure links to resources that each require a different authentication mechanism. The integration between Oracle Identity Federation and OracleAS Single Sign-On enables you to configure a link on a Web page that is protected by OracleAS Single Sign-On to do the following:

- Require OracleAS Single Sign-On to find an instance of Oracle Identity Federation when a user clicks the link.
- Direct Oracle Identity Federation to request authentication from a specific Identity Provider.

Note: See the *Oracle Secure Federation Services Administration Guide* for details on configuring Identity Providers.

To configure a federated authentication link on a Web portal page:

1. Set up a resource to be protected by OracleAS Single Sign-On.
2. In the HTML code for the portal page, provide the following link:

```
<a href="http(s)://<rest-of-URL>?providerid=xxx">
```

Where:

- *http(s)* is the protocol (http or https) to be used.
- *<rest-of-URL>* is the URL to the path to the protected resource.
- *providerid* is the keyword that signals to OracleAS Single Sign-On that Oracle Identity Federation must be queried for the Identity Provider.
- *xxx* is the Identity Provider ID configured in Oracle Identity Federation.

Integrating with Third-Party Access Management Systems

This chapter explains how to integrate OracleAS Single Sign-On with third-party access management products. It describes how third-party integration works; then it presents the integration APIs. Finally, it provides an example of how to integrate OracleAS Single Sign-On with a third-party access management system.

An enterprise that has a third-party system in place can gain access to the OracleAS suite by building an authentication adapter that enables the OracleAS Single Sign-On server to act as an authentication gateway between the third-party system and Oracle applications.

The chapter contains the following topics:

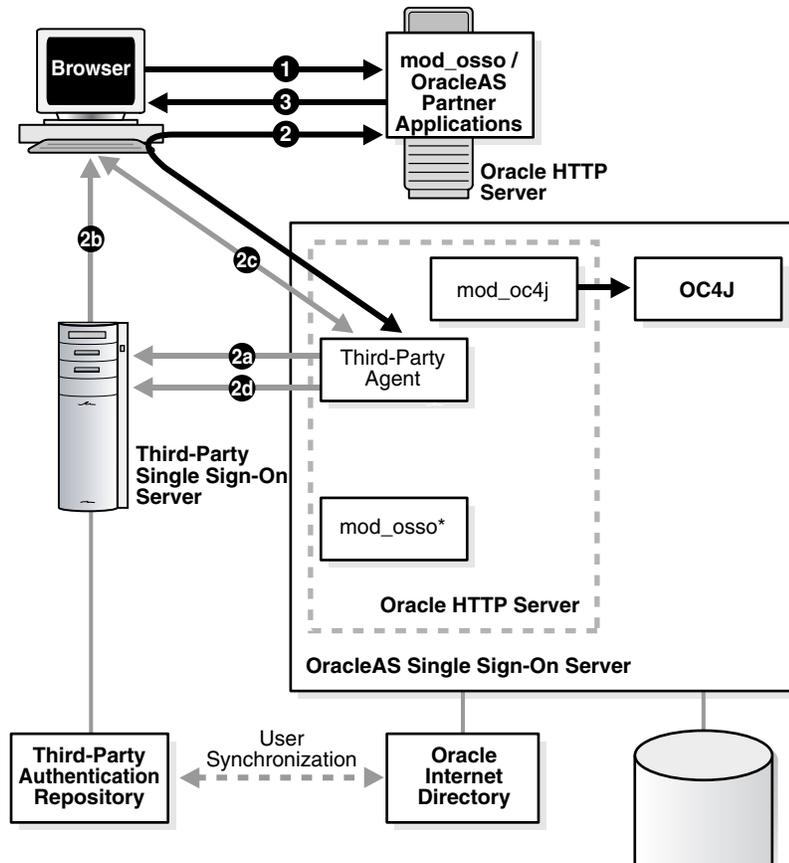
- [How Third-Party Access Management Works](#)
- [Synchronizing the Third-Party Repository with Oracle Internet Directory](#)
- [Third-Party Integration Modules](#)
- [Integrating with Windows Native Authentication](#)
- [Integration Case Study: SSOAcme](#)

How Third-Party Access Management Works

In third-party access management, the OracleAS Single Sign-On server, the third-party access management server, and the partner application form a chain of trust. The OracleAS Single Sign-On server delegates authentication to the third-party access management server, becoming a single sign-on-enabled application itself. Oracle applications continue to work only with the OracleAS Single Sign-On server and are unaware of the third-party access management server. Implicitly, however, they trust the third-party server.

For OracleAS Single Sign-On to issue users an authentication token under this arrangement, the third-party access management server must pass the OracleAS single sign-on server the user's identity by setting HTTP headers or by using some other mechanism. Once it obtains the user's identity, the OracleAS Single Sign-On server functions as before, authenticating and redirecting users to its partner applications. [Figure 14-1](#) on page 14-2 illustrates the process.

Figure 14–1 Accessing Oracle Partner Applications Using a Third-Party Server



The illustration captures two possible scenarios:

Scenario 1: The user has not yet authenticated to the third-party server

1. The unauthenticated user attempts to access an application protected by OracleAS Single Sign-On.
2. The application redirects the user to the OracleAS Single Sign-On server for authentication. As part of this redirection, the following occurs:
 - a. The OracleAS Single Sign-On server has the third-party agent, typically a module on the Oracle HTTP Server, authenticate the user. You install this module when you install the third-party adapter. Note that this module resides only on the single sign-on server. It does not reside on the application server.

Note: See "[Integration Case Study: SSOAcme](#)" for more about the third-party agent.

 - b. The third-party server sets a token in the user's browser.
 - c. The OracleAS Single Sign-On server retrieves the token from the browser.
 - d. The OracleAS Single Sign-On server verifies the token with the third-party server.

After token verification, the OracleAS Single Sign-On server returns the user—and the authenticated user information—to the requested application.

3. The application provides content to the user.

Scenario 2: The user has already authenticated to the third-party server

1. The authenticated user attempts to access an application protected by OracleAS Single Sign-On.
2. The application redirects the user to the OracleAS Single Sign-On server for authentication. As part of this redirection, the following occurs:
 - a. The OracleAS Single Sign-On server retrieves the token from the browser (step 2c in scenario 1).
 - b. The OracleAS Single Sign-On server verifies the token with the third-party server (step 2d in scenario 1).

After token verification, the OracleAS Single Sign-On server returns the user to the requested application.

3. The application provides content to the user.

Note: If the single sign-on systems involved are to be accessible to all authorized users, the user repository must be centralized in one place. This means that, before deployment, users must be synchronized between Oracle Internet Directory and the external repository if this repository is not also Oracle Internet Directory.

Synchronizing the Third-Party Repository with Oracle Internet Directory

The authentication scenario presented in the preceding steps assumes either that the user repository is Oracle Internet Directory or that the repository is a third-party directory or database. If the repository is the latter, the user name information must be synchronized with the user entry in Oracle Internet Directory. This synchronization enables the single sign-on server to retrieve the user attributes required by applications enabled for single sign-on.

Note: Third-party access management integration cannot proceed if the synchronization mechanism is not in place.

To synchronize the third-party repository with Oracle Internet Directory, use either Oracle Directory Integration and Provisioning or bulk load tools. For details, see the chapters about directory synchronization in *Oracle Identity Management Integration Guide*.

Third-Party Integration Modules

There are two ways to achieve third-party integration: you can use existing, vendor-supplied packages, or you can build your own third-party adapter, using interfaces provided by Oracle.

Using Vendor-Supplied Packages

Several third-party access management vendors provide authentication adapters for the OracleAS Single Sign-On server. These products enable you to integrate a third-party system with the Oracle system without having to write your own code. The link that follows provides information about these vendors' products. All of the vendors listed certify that their products work with OracleAS Single Sign-On. See the section Single Sign-On under the heading Documentation, which appears near the bottom of the page. Note that this material cannot be found under the Services menu.

http://www.oracle.com/technology/products/id_mgmt/partners/index.html

If you decide to use a third-party adapter, be aware that the instructions for implementing the adapter are contained not in this document, but in vendor documents. If you need help implementing the adapter, you must contact the vendor directly. The link provided includes contact information.

Building Your Own Package

You can use the Java toolkit `oracle.security.sso.ias904.toolkit` to build your own third-party integration adapter. The toolkit consists of two interfaces, one for performing authentication, the other for setting deployment-specific cookies. The OracleAS Single Sign-On server invokes the first interface during authentication. It invokes the second, the cookie adapter, after it has successfully determined the user's identity.

This section contains the following topics describing the interfaces and related classes in `oracle.security.sso.ias904.toolkit`:

- [Guidelines for Using the Interfaces](#)
- [The Classes and Interfaces](#)
- [Configuration Steps](#)

Guidelines for Using the Interfaces

Use authentication interface if you want to build your own third-party integration adapter. The OracleAS single sign-on server uses the interface implementation to authenticate the user's identity.

The cookie interface is optional. It is provided for environments or applications that require specialized cookies. For example, you may want to replicate the authentication cookie that is set by a popular user application. Or you may want to set user preferences using a cookie. You can set one or more cookies once the user is authenticated by the OracleAS single sign-on server. If you choose to use the cookie interface, you can include it in your own adapter or in an adapter provided by a vendor.

The Classes and Interfaces

The classes and interfaces in the kit perform the following functions:

- [Authentication Using a Token](#)
- [User Information Constructors](#)
- [Setting External Cookies](#)
- [Exception Handling](#)

Authentication Using a Token The `IPASAuthInterface.java` package is invoked by the OracleAS Single Sign-On server during authentication. If authentication using a token is to be supported, the implementer of this interface must return the user name to the OracleAS Single Sign-On server by retrieving the user identity in a secure fashion—from a securely set HTTP header, for instance, or from a secure cookie. Here is the interface:

The IPASAuthInterface.java Interface

```
package oracle.security.sso.ias904.toolkit;

/**
 * Oracle Single Sign-On server authentication interface. This package can
 * be used to integrate with custom authentication mechanism or third-party
 * access management system.
 */
public interface IPASAuthInterface
{
    /**
     * This method returns IPASUserInfo object that contains either user name,
     * subscriber name, and requested URL, or full user and subscriber
     * attribute mappings, including DN, GUID, and requested URL.
     * @param request - HTTP request object
     * @return IPASUserInfo object that contains
     * @authenticated user information
     * @see oracle.security.sso.ias904.toolkit.IPASUserInfo
     */
    IPASUserInfo authenticate(HttpServletRequest request)
        throws IPASAuthException, IPASInsufficientCredException;

    /**
     * This method returns a page URL - user will be redirected to
     * the page to enter login credentials
     * @param request - HTTP request object
     * @param message - Message to be displayed in the page
     * @return The page URL for collecting user login credential
     */
    java.net.URL getUserCredentialPage(HttpServletRequest request,
        String message);
}

```

User Information Constructors The user information class `IPASUserInfo.java` provides constructors for user logins.

The IPASUserInfo.java Class

```
package oracle.security.sso.ias904.toolkit;
/**
 * User information class
 */
public class IPASUserInfo
{
    /**
     * Constructor with user login name that belongs to default subscriber
     * @param userNickName - User login name
     */
    IPASUserInfo(String userNickName);

    /**

```

```
* Constructor with user login name that belongs to default subscriber
* @param userNickName - User login name
* @param subscriberName - The user's subscriber name
*/
IPASUserInfo(String userNickName, String subscriberName);

/**
 * Constructor with user login name that belongs to default subscriber
 * @param userNickName - User login name
 * @param userDN - User directory distinguished name
 * @param userGUID - User directory GUID value
 * @param subscriberName - The subscriber name for this user
 * @param subscriberDN - The subscriber's directory distinguished name
 * for this user
 * @param subscriberGUID - The subscriber's directory GUID value
 * for this user
 */
IPASUserInfo(String userNickName, String userDN, String userGUID,
             String subscriberName, String subscriberDN, String subscriberGUID);

/**
 * This method returns subscriber distinguished name
 * @return subscriber distinguished name
 */
String getSubscriberDN();

/**
 * This method sets subscriber distinguished name
 * @param subDn - subscriber distinguished name
 */
void setSubscriberDN(String subDn);

/**
 * This method returns subscriber GUID value
 * @return subscriber GUID value
 */
String getSubscriberGUID();

/**
 * This method sets subscriber GUID value
 * @param subGuid - subscriber GUID value
 */
void setSubscriberGUID(String subGuid);

/**
 * This method returns subscriber name
 * @return subscriber name
 */
String getSubscriberName();

/**
 * This method sets subscriber name
 * @param subscriber name
 */
void setSubscriberName(String subName);

/**
 * This method returns user login name
 * @return user login name
```

```

    */
    String getUsername();

    /**
     * This method sets user login name
     * @param user login name
     */
    void setUsername(String userName);

    /**
     * This method returns user distinguished name
     * @return user distinguished name
     */
    String getUserDN();

    /**
     * This method sets user distinguished name
     * @param user distinguished name
     */
    void setUserDN(String userDN);

    /**
     * This method returns user GUID value
     * @return user GUID value
     */
    String getUserGUID();

    /**
     * This method sets user GUID value
     * @param user GUID value
     */
    void setUserGUID(String userGUID);
}

```

Setting External Cookies To use cookies from a third-party application, the `IPASCustomCookieInterface.java` interface enables you to set one or more additional cookies after the user authenticates to the OracleAS single sign-on server. For example, you can add a cookie that is set by another single sign-on vendor to the set of cookies that are managed by the Oracle AS Single Sign-On server. These cookies are set if authentication is successful and the cookie adapter corresponds to the appropriate authentication level.

To implement a cookie that is set by a third-party application, you must write a java class to define the cookie.

The `IPASCustomCookieInterface.java` Interface

```

package oracle.security.sso.ias904.toolkit;

/**
 * Oracle Single Sign-On server invokes this method to obtain
 * user-defined custom cookies which will be sent to the user
 * upon successful login.
 */
public interface IPASCustomCookieInterface
{
    /**
     * Oracle Single Sign-On server invokes this method to obtain
     * user-defined custom cookies which will be sent
     * to the user upon successful login.
     * @param user - IPASUserInfo object that contains

```

```
    * the authenticated user information
    * @param request - HTTP request object
    * @return Array of javax.servlet.http.Cookie objects
    * @see javax.servlet.http.Cookie
    */
    public javax.servlet.http.Cookie[] getCustomCookie(IPASUserInfo user,
        HttpServletRequest request);
}
```

Exception Handling This section lists the exception handling classes in `oracle.security.sso.ias904.toolkit`.

The IPASException.java Class

```
package oracle.security.sso.ias904.toolkit;

/**
 * Generic exception class
 */
public class IPASException
    extends Exception
{
    /**
     * Default constructor with no error message
     */
    public IPASException()
    {
        super();
    }

    /**
     * Constructor with an error message
     */
    public IPASException(String message)
    {
        super(message);
    }
}
```

The IPASAuthException.java Class

```
package oracle.security.sso.ias904.toolkit;

/**
 * Authentication failure exception class
 */
public class IPASAuthException
    extends IPASException
{
    /**
     * Default constructor with no error message
     */
    public IPASAuthException()
    {
        super();
    }

    /**
     * Constructor with an error message
     */
}
```

```

    public IPASAuthException(String message)
    {
        super(message);
    }
}

```

The IPASInsufficientCredException.java Class

```

package oracle.security.sso.ias904.toolkit;

/**
 * Authentication failure exception due to insufficient user credentials
 */
public class IPASInsufficientCredException
    extends IPASException
{
    /**
     * Constructor with an error message
     */
    public IPASInsufficientCredException (String message)
    {
        super(message);
    }
}

```

Configuration Steps

To create your own third-party integration adapter using the interfaces, follow these steps:

1. In the third-party access management system, create rules that protect this URI:

```
/sso/auth/*
```

2. Register this logout URI with the third-party access management system:

```
/sso/logout
```

Note: In the remaining steps and in the sample package that follows, change all instances of `acme` and `SSOAcme` to your company name.

3. Create a Java file for your package. For help, see the sample file in "[Integration Case Study: SSOAcme](#)". The sample file is called `SSOAcmeAuth.java`. Before it is compiled, this package directive must be added to it:

```
package acme.security.ssoplugin;
```

4. Compile the file, including `ORACLE_HOME/sso/lib/ipastoolkit.jar` in the class path. The sample file `SSOAcmeAuth.java` is compiled this way:

```
ORACLE_HOME/jdk/bin/javac -classpath ORACLE_HOME/sso/lib/ipastoolkit.jar:
ORACLE_HOME/lib/servlet.jar -d ORACLE_HOME/sso/plugin SSOAcmeAuth.java
```

This command creates `SSOAcmeAuth.class` and places it in the directory `ORACLE_HOME/sso/plugin/acme/security/ssoplugin`.

5. In the `policy.properties` file, replace the simple authentication plugin with the plugin that you created in step 3. The simple authentication plugin looks like this:

```
MediumSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOAcmeAuth
```

The sample plugin looks like this:

```
MediumSecurity_AuthPlugin = acme.security.ssoplugin.SSOAcmeAuth
```

Note: When editing `policy.properties`, take care not to insert blank space at the end of a line.

- If you want to implement the custom cookie interface, add the class name of the implementation of each cookie to `policy.properties`, along with the minimum authentication level at which the custom cookie is set if the user authenticates successfully:

```
# Custom Cookie Provider Class names
# -----
# Sample custom cookie tester provider class

CustomCookie_ProviderPlugin = class_name
CustomCookieAuthLevel = authentication_level

CustomCookie_ProviderPlugin1 = class_name1
CustomCookieAuthLevel = authentication_level1

CustomCookie_ProviderPlugin2 = class_name2
CustomCookieAuthLevel = authentication_level2
```

Where `class_name` is the name of the java class that implements the cookie and `authentication_level` is the value NoSecurity, LowSecurity, LowMediumSecurity, MediumSecurity, MediumHighSecurity, or HighSecurity.

For example, you can implement three plug-ins. The first, `CustomCookieProviderPlugin`, may be associated with the `test.custom.MyCookieProvider` class. The second, `CustomCookieProviderPlugin1`, may be associated with the `com.custom.CustomCookieProvider` class.

If you are not using multilevel authentication and are using default settings for authentication adapter levels, you can set this value to `MediumSecurity`.

- Restart the single sign-on middle tier:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

- Test the integrated system.

Logging Out of the Integrated System

Before proceeding with this section, make sure that you understand the concept of single sign-off and know how implement it. Read the section ["Single Sign-Off"](#) in [Chapter 1](#).

Third-party logout takes two forms:

- The user initiates a logout request using the third-party access management system.

In this scenario, the user clicks a logout link that invokes a logout handler in the third-party system. The third-party logout flow cleans up its own session. After cleanup, The third-party system must invoke the OracleAS Single Sign-On logout

handler. Invoking the OracleAS Single Sign-On logout handler ensures that the user is logged out of all applications protected by the OracleAS Single Sign-On server. To perform single sign-on logout, the third-party system must redirect the user to the following URL:

```
http://single_sign-on_host:single_sign-on_port/sso/logout
```

or, if SSL is enabled, to this URL:

```
https://single_sign-on_host:single_sign-on_ssl_port/sso/logout
```

done_url is the URL to which the user is redirected after logout.

- The user initiates a logout request using the OracleAS Single Sign-On system

In this scenario, the user clicks a logout link in an Oracle partner application. This invokes the OracleAS Single Sign-On logout handler. When logout is finished, the user should also be logged out from the third-party system. Concurrent logout is effected by registering the Oracle logout handler (*ls_logout* in the URL immediately preceding) with the third-party system. The third-party system cleans up the third-party session when it detects that the Oracle logout handler is being invoked.

If you have chosen to use an adapter from a third party, see that vendor's documentation to learn how logout is actually implemented.

Integrating with Windows Native Authentication

OracleAS Single Sign-On interoperates with Windows Native Authentication (WNA). See the section on integrating with Active Directory in the *Oracle Identity Management Integration Guide* for details.

Note that if you use WNA with a virtual host, only one host name can be configured. To use a virtual host, you must define the virtual host's server IP address in the */etc/hosts* file.

Note: You can only have one virtual host per server for WNA-enabled single sign-on installations. Even if you configure multiple virtual hosts in the */etc/hosts* file, only the first one in the list for the server IP address will work for WNA-enabled single sign-on.

Integration Case Study: SSOAcme

Consider the case of SSOAcme, a product that offers single sign-on authentication to protected resources. SSOAcme consists of two components: the SSOAcme policy server and the SSOAcme agent. The first provides users with a variety of services including user and session management, authentication, and authorization. The second is located on Web servers and Web application servers. It screens requests for resources and determines whether a resource is protected by SSOAcme.

Customers who have SSOAcme already installed may want to use it to gain access to OracleAS applications. They can achieve this access by using APIs that enable SSOAcme to talk to Oracle applications by way of OracleAS Single Sign-On.

Note: SSOAcme is a fictitious product, used for the purposes of illustration only.

This section contains the following topics:

- [Sample Integration Package](#)
- [Migrating the Release 9.0.2 Sample Implementation to Release 10.1.3](#)

Sample Integration Package

The `SSOAcme.java` package, presented here, can be used to integrate an existing SSOAcme implementation with OracleAS Single Sign-On.

```
/* Copyright (c) 2002, 2003, Oracle Corporation. All rights reserved. */

/*
DESCRIPTION
    Sample class for SSOAcme integration with SSO Server

PRIVATE CLASSES

NOTES
    This class implements the SSOServerAuthInterface.
    To enable this integration, replace:
        oracle.security.sso.server.auth.SSOServerAuth
    with
        acme.security.ssoplugin.SSOAcmeAuth
    for the desired security level in policy.properties.
*/

import java.io.PrintWriter;

import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

import oracle.security.sso.ias904.toolkit.IPASAuthInterface;
import oracle.security.sso.ias904.toolkit.IPASAuthException;
import oracle.security.sso.ias904.toolkit.IPASUserInfo;
import oracle.security.sso.ias904.toolkit.IPASInsufficientCredException;

public class SSOAcmeAuth implements IPASAuthInterface {

    private static String CLASS_NAME = "SSOAcmeAuth";
    private static String ACME_USER_HEADER = "ACME_USER";

    public SSOAcmeAuth() {

    }

    public IPASUserInfo authenticate(HttpServletRequest request)
        throws IPASAuthException, IPASInsufficientCredException {

        String AcmeUserName = null;

        try
        {
            AcmeUserName = request.getHeader(ACME_USER_HEADER);
        }
    }
}
```

```

        catch (Exception e)
        {
            throw new IPASInsufficientCredException("No Acme Header");
        }

        if (AcmeUserName == null)
            throw new IPASInsufficientCredException("No Acme Header");

        IPASUserInfo authUser = new IPASUserInfo(AcmeUserName);

        return authUser;
    }

    public java.net.URL getUserCredentialPage(HttpServletRequest request,
        String msg) {

        // This function will never have been reached in the case of SSOAcme
        // because the SSOAcme Agent will intercept all requests
        return "http://error_url";
    }
}

```

Migrating the Release 9.0.2 Sample Implementation to Release 10.1.3

This section is provided for the benefit of those who used the release 9.0.2 external authentication package to perform third-party authentication. The release 9.0.2 package was written in PL/SQL. The release 10.1.3 package is written in Java. In the lines that follow, the pertinent sections of the two packages appear together.

New Authentication Interface

Release 10.1.3:

```

package acme.security.ssoplugin;

import java.io.PrintWriter;

import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import oracle.security.sso.server.util.SSODebug;
import oracle.security.sso.ias904.toolkit.IPASAuthInterface;
import oracle.security.sso.ias904.toolkit.IPASAuthException;
import oracle.security.sso.ias904.toolkit.IPASUserInfo;
import oracle.security.sso.ias904.toolkit.IPASInsufficientCredException;

public class SSOAcmeAuth implements IPASAuthInterface {

    private static String CLASS_NAME = "SSOAcmeAuth";
    private static String ACME_USER_HEADER = "ACME_USER";

    public SSOAcmeAuth() {
    }

    public IPASUserInfo authenticate(HttpServletRequest request)
    throws IPASAuthException, IPASInsufficientCredException {

```

Release 9.0.2:

```
FUNCTION authenticate_user
(
  p_user OUT VARCHAR2
)
return PLS_INTEGER
IS
  l_http_header varchar(1000);
  l_ssouser wwsec_person.user_name&type := NULL;
BEGIN
```

Get User Name from HTTP Header

Release 10.1.3:

```
String AcmeUserName = null;

try
{
  AcmeUserName = request.getHeader(ACME_USER_HEADER)
```

Release 9.0.2:

```
l_http_header := owa_util.get_cgi_env('HTTP_Acme_USER');
debug_print('Acme ID : ' || l_http_header);
```

Error Handling if User Name Not Present

Release 10.1.3:

```
}
catch (Exception e)
{
  DebugUtil.debug(SSODebug.ERROR, "exception: " + CLASS_NAME, e);
  throw new IPASInsufficientCredException("No Acme Header");
}

if (AcmeUserName == null)
throw new IPASInsufficientCredException("No Acme Header");
```

Release 9.0.2:

```
IF ( (l_ssouser IS NULL) or
  ( INSTR(l_ssouser, GLOBAL_SEPARATOR) != 0) ) THEN
  debug_print('malformed user id: '
    || l_ssouser
    || ' returned by wssso_auth_external.authenticate_user');
  RAISE EXT_AUTH_FAILURE_EXCEPTION;
ELSE
```

Return User Name to Single Sign-On Server

Release 10.1.3:

```
IPASUserInfo authUser = new IPASUserInfo(AcmeUserName);

return authUser;

}
```

Release 9.0.2:

```
p_user := NLS_UPPER(l_ssouser); -- p-user is the out parameter
return 0; -- SUCCESS error code
```

END IF;

Exporting and Importing Data

This chapter explains how to move data between two or more single sign-on servers. Various conditions dictate whether you export and import data. Perhaps you want to stage data on a test server before transferring it to a production server. Or maybe you want to consolidate multiple servers as one server. Or you may simply want to back up an existing server.

The chapter contains the following topics:

- [What's Exported and Imported?](#)
- [Export and Import Script: Syntax and Parameters](#)
- [Exporting Data from One Server to Another](#)
- [Consolidating Multiple Servers](#)
- [Verifying That Export and Import Succeeded](#)
- [Error Messages](#)

What's Exported and Imported?

The export and import script, `ssomig`, moves three categories of data:

- Definitions and user data for external applications
- Registration URLs and tokens for partner applications
- Connection information used by OracleAS Discoverer to access various data sources

If you need to move user accounts, use LDAP command-line scripts such as `ldapsearch` to extract data from the source directory. Use `ldapadd` or `ldapmodify` to load data into the target directory. To learn how to use these scripts, see the syntax chapter in *Oracle Identity Management Application Developer's Guide*.

Export and Import Script: Syntax and Parameters

The `ssomig` script uses Perl, Oracle SQL*Plus, and the database export and import tools `exp` and `imp` to move data between two release 10.1.3 servers. You must run the export and import modes separately. You can find `ssomig` at `ORACLE_HOME/sso/bin`.

Script Syntax

Use this syntax to run `ssomig`:

```

ssomig -s sso_schema
      -p sso_password
      -c net_service_name
      -log_d log_dir
      {
        -export [-prompt]
                [-noextappusrs]

        -import {-merge | -overwrite}
                [-discoforce | -disconoforce]
      }
      [-log_f log_file]
      [-d dump_file_name]
      [-help]

```

Script Parameters

Table 15–1 defines the parameters passed to `ssomig`.

Table 15–1 Parameters Passed to `ssomig`

Parameter	Description	Additional Information
-s	Database schema name for OracleAS Single Sign-On.	The default is ORASSO.
-p	Database schema password for OracleAS Single Sign-On.	The password is randomized during installation of the OracleAS infrastructure. To obtain the password, see Appendix B .
-c	Net service name for the OracleAS Single Sign-On database.	-
-log_d	Name of the log directory.	This directory must be writable. The log file, the export configuration file, and the dump file are written here. Use the absolute path for the directory when running the script. The default is <code>ORACLE_HOME/sso/log</code> .
-export	Extracts data from single sign-on tables and places it into a dump file.	-
-prompt	Exports partner and external applications selectively.	Use with <code>export</code> .
-noextappusrs	Specifies that external application users not be exported.	Use with <code>export</code> . Choose this mode if you are moving data from a staged server to a production server and do not want to move test users.
-import	Extracts data from a dump file and places it into single sign-on tables.	-
-merge	Imports only partner and external applications that do not already exist in the target server.	Choose this mode after you have imported the first of multiple servers. Use with <code>import</code> .
-overwrite	Imports all partner and external applications, regardless of whether some already exist in the target server.	Choose this mode when migrating the first of multiple servers. Use with <code>import</code> .
-discoforce	Imports OracleAS Discoverer information, replacing Discoverer information in the target server.	-

Table 15–1 (Cont.) Parameters Passed to *ssomig*

Parameter	Description	Additional Information
-disconoforce	Imports OracleAS Discoverer information only if the target server contains no Discoverer data.	-
-log_f	Log file name.	This file provides export results and the runtime status of tools such as SQL*Plus, exp, and imp. The default file name is <code>ssomig.log</code> .
-d	Dump file name.	The default is <code>ssomig.dmp</code> .
-help	Describes the syntax and parameters for <code>ssomig</code> .	-

Exporting Data from One Server to Another

The scenarios under which the export and import script is run fall into two categories: export from a single server and export from multiple servers. The choice of one category or the other dictates whether the script is run in overwrite mode or merge mode. It also dictates whether partner and external applications are exported selectively. This section examines single-server export and import. For multiple-server export and import, see "[Consolidating Multiple Servers](#)".

This section contains the following topics:

- [Export and Import Scenarios and Script Examples](#)
- [Running the Script](#)

Export and Import Scenarios and Script Examples

What follows are scenarios that you are likely to encounter when moving data from one single sign-on server to another. The command appropriate for each scenario is provided.

Note: The following examples are described with UNIX in mind, but they work with Windows as well. Simply substitute a backslash for the forward slash in the log directory path.

Export Scenarios

- Export all partner and external applications. Export OracleAS Discoverer data entirely. This command is appropriate when you want to back up a server:


```
ssomig -export -s orasso -p password -c net_service_name -log_d /tmp
```
- Selectively export partner and external applications. Export OracleAS Discoverer data entirely. Run this command when you want to move staged data to a production server:


```
ssomig -export -prompt -s orasso -p password -c net_service_name -log_d /tmp
```
- Selectively export partner applications. Selectively export definitions for external applications. Do not export user data for external applications. Export OracleAS Discoverer data entirely. Run this command when you want to move staged data to a production server, but do not want to move external application information for test users:

```
ssomig -export -prompt -noextappusrs -s orasso -p password -c net_service_name  
-log_d /tmp
```

Import Scenarios

- Import partner and external applications. Overwrite only entries that are the same as the entries that you are importing. Exclude OracleAS Discoverer data. This command is useful if you are not deploying Discoverer:

```
ssomig -import -overwrite -s orasso -p password -c net_service_name -log_d /tmp
```

- Import partner and external applications and OracleAS Discoverer data. Overwrite all entries, regardless of whether they are the same as the entries you are importing. Run this command if you need to refresh data in the target server:

```
ssomig -import -overwrite -s orasso -p password -c net_service_name -log_d /tmp  
-discoforce
```

- Import partner and external applications. Overwrite all entries, regardless of whether they are the same as the entries you are importing. Import OracleAS Discoverer information only if none is present in the target server:

```
ssomig -import -overwrite -s orasso -p password -c net_service_name -log_d /tmp  
-disconoforce
```

Running the Script

To export data:

1. Log in to the computer that you are exporting from.
2. Set the Oracle home environment variable, `ORACLE_HOME`, to point to the Oracle home of the release 10.1.3 single sign-on server.
3. Run the script. (See "[Export and Import Scenarios and Script Examples](#)".)

This action creates the dump file `ssomig.dmp`, the log file `ssoconf.log`, and the single sign-on configuration file `ssoconf.log`. All three are created in the log directory.

Note: When you run `ssomig` in export mode with the prompt option, the script asks you to identify applications that you do not want to export. At the same time, it asks you to press any key when you are finished making your selections. Press the **Return** or **Enter** key instead. The script ignores other keys.

To import data:

1. Log in to the computer that you are importing data to.
2. Set the environment variable `ORACLE_HOME` to point to the Oracle home for the release 10.1.3 single sign-on server.
3. Make sure that the `log_d` parameter points to the log directory where the log files for export are located. The script must reference the files `ssomig.dmp` and `ssoconf.log` when it runs in import mode. You may have to copy these files from the computer on which the export server is located.
4. Run the script, choosing `import` mode. (See "[Export and Import Scenarios and Script Examples](#)".)

Verifying That Export and Import Succeeded

After completing export and import operations, open `ssomig.log` and check for errors. To interpret the messages that you encounter in the file, see ["Error Messages"](#).

Consolidating Multiple Servers

This scenario is applicable if several departments in your enterprise maintain departmental single sign-on servers. You may want to consolidate these servers into a unified identity management service.

Use the following approach to export and import multiple servers:

1. Export data from all of the servers involved except the target server. To learn how to run the script, see ["Exporting Data from One Server to Another"](#).
2. Run the script in `import` mode, `overwrite` option, for the first single sign-on server that you migrate. For help, see the section ["Import Scenarios"](#).
3. For subsequent servers, run the script in `merge` mode. Import partner and external applications to the target server, importing the servers one at a time:

```
ssomig -import -merge -s orasso -p password -c net_service_name -log_d /tmp -d
ssomig.dmp
```

This command merges only partner and external applications.

Note: when importing multiple servers, you can run the script in `overwrite` mode to cancel the result of a previous run.

Error Messages

Any one of the following messages may appear during the course of export and import. [Table 15–2](#) defines these messages to aid problem resolution.

Table 15–2 Error Codes for Export and Import

Error	Cause	Action
SSO-80000: The operation was unsuccessful.	Import or export or both failed because of one or more errors.	Determine the error from the log file or from screen output.
SSO-80001: The environment variable <code>ORACLE_HOME</code> is not set.	The variable has not been set for the release 10.1.3 Oracle home.	Follow the instructions in "Running the Script" .
SSO-80002: Invalid <code>ORACLE_HOME</code> specified.	The directory represented by <code>ORACLE_HOME</code> does not exist or required scripts under it are unavailable.	Set the Oracle home to a valid Oracle instance.
SSO-80004: Invalid log directory. String is not writable.	You lack write permission for the log directory specified.	Specify a directory for which you have write permission.
SSO-80005: Invalid log directory. String is not directory.	The log directory specified does not exist.	Specify a valid directory.

Table 15–2 (Cont.) Error Codes for Export and Import

Error	Cause	Action
SSO-80008: Duplicate option string.	The command-line parameter string is repeated or both options that compose a set of complementary options are provided.	Avoid repeating the command-line parameter string. Avoid including both options that compose a set of complementary options— <code>export</code> and <code>import</code> , for instance.
SSO-80009: Mandatory parameter missing: string.	A mandatory command-line parameter string is missing	Specify the parameter string, including any relevant values.
SSO-80010: Invalid SSO Server version detected.	The script does not support the version of the source or destination server.	Make sure that you are using release 10.1.3 servers to perform export and import operations.
SSO-80011: Invalid option string.	The parameter string is not a recognized command-line parameter	Use the option <code>help</code> to obtain a list of valid parameters.
SSO-80012: Invalid SSO schema information.	The schema name, password, or net service name is invalid.	Reenter the command.
SSO-80014: Invalid log file. String is not writable.	You lack write permission for the log file that you specified.	Specify a log file for which you have write permission.
SSO-80015: Failed to drop temporary tables.	An expected script file was missing, or an operating system error or database error was encountered.	View the log files for details. Correct any errors that you find.
SSO-80050: Data export unsuccessful.	The export operation failed because of one or more errors.	Determine the error from the log file or from screen output.
SSO-80051: Copying data into the temporary tables failed.	A script file is missing or an operating system error or database error was encountered.	View the log file for details. Correct errors that you find.
SSO-80052: Invalid dump file. String not writable.	You lack write permission for the dump file specified.	Specify a dump file for which you have write permission.
SSO-80076: Cannot determine NLS information.	A script file is missing or an operating system error or database error was encountered.	View the log file for details. Correct errors that you find.
SSO-80077: The file string does not exist.	The file string has been deleted or renamed externally.	Ensure that the file string is not touched externally during execution of the script.
SSO-80078: Creating the table that represents the config file failed.	A script file is missing or an operating system error or database error was encountered.	View the log file for details. Correct errors that you find.
SSO-80100: Data import unsuccessful.	The import operation failed because of one or more errors.	Determine the error from the log file or from screen output. Correct errors that you find.
SSO-80101: Cannot read the import dump file: string.	You lack read permission for the dump file string.	Obtain read permission for the specified dump file.
SSO-80102: The dump file string is of size zero.	An error occurred during export.	View the log file. Correct errors that you find.

Table 15–2 (Cont.) Error Codes for Export and Import

Error	Cause	Action
SSO-80103: Config file not found: string.	This error appears if required configuration files such as dump and log are missing during import.	Ensure that the configuration files are present in the log directory.
SSO-80104: Corrupted or invalid config file.	The configuration file has been altered.	Ensure that the configuration file is not altered when transferred from the source to the destination.
SSO-80150: Package loading into the SSO schema failed.	A script file is missing or an operating system error or database error was encountered.	View the log file for details. Correct errors that you find.

Troubleshooting OracleAS Single Sign-On

This appendix describes common problems that you might encounter when using Oracle Application Server Single Sign-On and explains how to solve them. It also provides information for diagnosing and solving problems with your OracleAS Single Sign-On environment, such as reviewing log files and enabling debugging.

It contains the following topics:

- [Problems and Solutions for General Single Sign-On Server Errors](#)
- [Problems and Solutions for Certificate Authentication Errors](#)
- [Problems and Solutions for Windows Native Authentication Errors](#)
- [Problems and Solutions for Password Policy Errors](#)
- [Diagnosing OracleAS Single Sign-On Problems](#)
- [Maintenance Tasks for OracleAS Single Sign-On](#)
- [A Word About Non-GET Authentication](#)
- [Need More Help?](#)

Problems and Solutions for General Single Sign-On Server Errors

This section describes common problems and solutions encountered when starting or accessing the single sign-on server. It contains the following topics:

- [Internal Server Error](#)
- [Unexpected Error](#)
- [File Not Found Error](#)
- [Authentication Failed](#)
- [The User Name Submitted for Authentication Does Not Match the User Name Present in the Existing Single Sign-On Session](#)
- [White Page Displayed When Accessing OracleAS Single Sign-On Administration](#)
- [Administrator Cannot See OracleAS Single Sign-On Administration Pages](#)
- [The "SSO Server Administration" Link is Missing from the OracleAS Single Sign-On Administration Page](#)
- [Audit Log Insertion Exception: ORA-00018: Maximum Number of Sessions Exceeded](#)
- [Connection Limit Exceeded](#)

- [Failed Login Message when System has been Idle](#)
- [Error due to Idle LDAP or Database Connection Timeouts](#)

URL Exceeds Maximum Length

On some browsers a user's attempt to access a protected resource may exceed the maximum URL length, even if the requested URL is shorter than the maximum allowed by the browser. This problem occurs because, by default, `mod_osso` uses the GET directive to pass information to the OracleAS Single Sign-On Server. When using the GET directive, encryption keys, a site ID, site token, the IP address of the client, timestamps, and so are added to the URL in the course of processing the request.

Problem

The user attempts to access a protected URL, but the OracleAS Single Sign-On Server returns a 302 status code and the requested resource is not served to the user.

Solution

You can configure `mod_osso` to use POST by adding the `OsoRedirectByForm` directive to the `mod_osso.conf` file, located in the `$ORACLE_HOME/Apache/Apache/conf` directory.

Internal Server Error

When accessing OracleAS Single Sign-On, you may encounter an "Internal Server Error" message if the single sign-on server was started incorrectly or is unable to connect to infrastructure components.

Problem 1

Users see the following error message when contacting the single sign-on server:

```
Internal Server Error. Please contact administrator.
```

This error message usually appears when the single sign-on server is started incorrectly.

Solution 1

Use the following sequence to solve the problem:

1. Verify that the single sign-on server was started correctly by checking the startup log file: `ORACLE_HOME/opmn/logs/OC4J~OC4J_SECURITY~default_island~1`.
2. If the log file reports errors for the database or for Oracle Internet Directory, make sure that both are up and running before starting the single sign-on server. If you see the message `SSOLoginServlet.init: SSO server started`, the single sign-on server has been started correctly.
3. Next, check the log file for the single sign-on server: `ORACLE_HOME/sso/log/ssoServer.log`.
4. If the log file contains the error message `NumberFormatException` or a specific configuration parameter not found, check `policy.properties` for blank spaces. Remove spaces that occur at the end of the line containing the questionable configuration; then restart the OC4J_SECURITY instance:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

5. If the file `ORACLE_HOME/opmn/logs/OC4J~OC4J_SECURITY~default_island~1` reports the error message `Orion Launcher SSO Server initialization failed`, do the following:

- Make sure that the database is available; then restart the single sign-on server:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

- If the database is available, the problem may be the directory connection. Check the opmn log. If you see the error message that follows, run `ssoconf.sql` to ensure that directory access is properly configured in the single sign-on database.

```
java.lang.NumberFormatException: null
    at java.lang.Integer.parseInt(Integer.java:442)
    at java.lang.Integer.parseInt(Integer.java:524)
    at oracle.security.sso.server.conf.DatabaseConfigReader.
    setSSOServerConfig(DatabaseConfigReader.java:322)
```

6. To learn how to run `ssoconf.sql`, see ["Changing Single Sign-On Server Settings for Directory Access"](#) in Chapter 3.

Problem 2

Users see the following error message when contacting the single sign-on server:

```
Internal Server Error. Please try the operation later.
```

This error message appears when either the infrastructure database or Oracle Internet Directory is unavailable or is down.

Solution 2

Check `ORACLE_HOME/sso/log/ssoServer.log` for a detailed description of the message; then try restarting the database or the directory, depending upon what you find.

Unexpected Error

Users see the following error when contacting the single sign-on server:

```
Unexpected Error. Please contact administrator.
```

Problem

This message may indicate a server-side error. The `policy.properties` file may be misconfigured, or Java classes may not be loaded. Another cause may be that the partner application is registered incorrectly.

Solution

Try the following steps to determine the cause of the problem:

1. Check the following log files for error messages:

The single sign-on server log: `ORACLE_HOME/sso/log/ssoServer.log`

The Oracle HTTP Server error log: `ORACLE_HOME/Apache/Apache/logs/error_log`

2. Try to log on to the OracleAS Single Sign-On administration pages. Be sure to log in as `orcladmin`, not as `cn=orcladmin`.

```
http://single_sign-on_host:single_sign-on_port/sso
```

3. If you are able to log in, the problem is not with the single sign-on server, but with the partner application registration or with the application itself.

File Not Found Error

When accessing the single sign-on server, users see the following error message:

```
File Not Found.
```

Problem

Check the Oracle HTTP Server error log (*ORACLE_HOME*/Apache/Apache/logs/error_log).

If you find the message `file not found`, Oracle HTTP Server is not delegating the authentication request to OC4J.

Solution

Perform the following checks:

1. Check `mod_oc4j.conf` for single sign-on application mappings. The mount configuration `Oc4jMount/sso OC4J_SECURITY` should be present.
2. Check `default-web-access.log` to determine whether the authentication request was received by the servlet.

Authentication Failed

Users may see an `Authentication Failed` error after logging on to OracleAS Single Sign-On.

Problem

The user's password is incorrect, or the server does not have the permissions necessary to authenticate the user.

Solution

1. Try binding to the directory as the user, making sure that the user DN corresponds to the appropriate realm:

```
ORACLE_HOME/bin/ldapbind
-h directory_server
-p directory_ssl_port
-D user_dn
-w user_password
-u 1
```

If the bind fails, the user's password is incorrect. Reset the password. If the bind succeeds, proceed to step 2.

2. Try binding to the directory as the single sign-on server:

```
ORACLE_HOME/bin/ldapbind
-h directory_server
-p directory_ssl_port
-D orclApplicationCommonName=ORASSO_
SSOSERVER,cn=SSO,cn=Products,cn=OracleContext
-w single_sign-on_server_password
```

If the bind fails, the server password that you are trying to bind with may be incorrect. To set the correct password, run `ssoconf.sql` as explained in ["Changing Single Sign-On Server Settings for Directory Access"](#) in [Chapter 3](#). If the bind succeeds, proceed to step 3.

3. Check whether the single sign-on application is a member of the SecurityAdmins group. If it is not a member of this group, it cannot authenticate the user:

```
ORACLE_HOME/bin/ldapcompare
-h directory_host
-p directory_ssl_port
-D orclApplicationCommonName=ORASSO_
  SSOSEVER, cn=SSO, cn=Products, cn=OracleContext
-w orasso_password
-b "cn=user_dn, cn=users, realm_dn"
-a userpassword
-v user_password
```

If the application is not a member, add it to the SecurityAdmins group (`cn=OracleUserSecurityAdmins, cn=Groups, cn=OracleContext`) and have the user reauthenticate. If the application is a member, the problem may be directory based.

The User Name Submitted for Authentication Does Not Match the User Name Present in the Existing Single Sign-On Session

Problem

Users encounter this error only during a forced authentication request. They see the error because they fail to enter the same user ID and, optionally, realm that they entered when they first authenticated.

Solution

The user ID and, optionally, realm entered during forced authentication must match the user ID and realm in the current single sign-on session. Users who want to use different credentials to log in must log out of the current session first.

White Page Displayed When Accessing OracleAS Single Sign-On Administration

When logging on to OracleAS Single Sign-On administration pages the administrator sees a blank white page.

Problem 1

The `PUBLIC` user entry is missing from Oracle Internet Directory, or the user nickname attribute was changed in the directory, but the new attribute was not added to the `PUBLIC` entry.

Solution 1

Add the `PUBLIC` user entry under the user search base in the directory. If, instead, the user nickname attribute was changed, add the attribute to the `PUBLIC` user entry.

Problem 2

The single sign-on server is configured with the wrong information for the directory.

Solution 2

Run `ssooconf.sql` to configure the single sign-on server with the correct directory information. To learn how to run the script, see ["Changing Single Sign-On Server Settings for Directory Access"](#) in [Chapter 3](#).

Problem 3

There may be installation problems, namely, a missing Enabler entry or faulty SSL registration.

Solution 3

Run `ssooconf.sql` to update the single sign-on server with the enabler entry or to modify single sign-on URLs for SSL.

Problem 4

The directory DIT has changed and the single sign-on server has not been updated with the changes.

Solution 4

Run `ssoreoid.sql` to update the single sign-on server with directory DIT changes.

Administrator Cannot See OracleAS Single Sign-On Administration Pages

The administrator does not see the OracleAS Single Sign-On administration pages when logging in to `.../sso`.

Problem

The administrator is not a member of the iASAdmins group:

```
cn=iASAdmin,cn=Groups,cn=OracleContext, realm_dn
```

Solution

Check the `uniquemember` attribute of the iASAdmins entry in the directory:

```
ldapsearch -h directory_host
            -p directory_port
            -D orclApplicationCommonName=ORASSO_
              SSOSERVER,cn=SSO,cn=Products,cn=OracleContext
            -w orasso_password
            -b "cn=iasadmins,cn=groups,cn=oraclecontext, realm_dn"
              "uniquemember=cn=user,cn=users, realm_dn"
```

If the `user` in the command is not a unique member of iASAdmins, follow the instructions in ["Granting Administrative Privileges"](#) in [Chapter 2](#).

The "SSO Server Administration" Link is Missing from the OracleAS Single Sign-On Administration Page

Problem

Only administrators see this link. The user who is missing the link is logged in as an end user.

Solution

Make sure that the user is a member of the iASAdmins group:

```
cn=iASAdmins,cn=Groups,cn=OracleContext,dc=default_identity_management_realm
```

If you have changed the OracleAS Single Sign-On administration group, make sure that the user is a member of this group.

Audit Log Insertion Exception: ORA-00018: Maximum Number of Sessions Exceeded

This message appears when the load on the single sign-on server is heavy.

Problem

The number of database sessions required has exceeded the number specified in the `init.ora` file.

Solution

Change the properties of the identity management infrastructure database. Specifically, increase the `processes` and `sessions` parameters to match anticipated load. Use a database-specific configuration file such as `init.ora` to make the change. `init.ora` is found at `ORACLE_HOME/dbs`.

Connection Limit Exceeded**Problem**

This message is a variation of the message: Audit Log Insertion Exception: ORA-00018: Maximum Number of Sessions Exceeded.

Solution

The end user should retry the operation, or the administrator can increase the connection limit.

Failed Login Message when System has been Idle

Users may see a login failure error when OracleAS Single Sign-On is operating behind a firewall and has been idle for some time. The following text appears in `ssoserver.log`:

```
AJPRequestHandler-ApplicationServerThread-11 DB connection error
java.sql.SQLException: Closed Connection
at oracle.jdbc.dbaccess.DBError.throwSQLException(DBError.java:189)
at oracle.jdbc.dbaccess.DBError.throwSQLException(DBError.java:231)
at oracle.jdbc.dbaccess.DBError.throwSQLException(DBError.java:294)
```

Problem

In most production environments, a firewall protects the OracleAS Single Sign-On and Oracle Internet Directory servers. The firewall tracks connection activity and drops inactive database or directory connections after a period controlled by the firewall timeout value.

If the single sign-on server has not been notified about a dropped database connection, it may try to perform an operation using the stale connection, resulting in this error.

Solution

Follow the solution described in "[Error due to Idle LDAP or Database Connection Timeouts](#)" on page A-8.

Error due to Idle LDAP or Database Connection Timeouts

OracleAS Single Sign-On server may display an internal server error while logging in, if the system is configured with an LDAP firewall and the firewall drops idle LDAP or database connections.

Problem

When there is a firewall between Oracle Application Server Single Sign-On and the LDAP or database server, you may encounter login errors when the firewall drops an inactive LDAP or database connection.

Solution

You can set a parameter to control the duration of OracleAS Single Sign-On server's LDAP or database connections. This is known as the `connectionIdleTimeout` parameter; you can specify its value, in minutes, in the `policy.properties` configuration file. The parameter is useful in deployments that utilize a firewall between OracleAS Single Sign-On and the LDAP or database server. If an LDAP or database connection is idle for a period longer than this parameter value, then OracleAS Single Sign-On server will remove that connection from the pool and try to use a fresh connection from the pool.

Take the following steps to set the LDAP or database connection timeout:

1. Edit the `ORACLE_HOME/sso/conf/policy.properties` file to add or update the `connectionIdleTimeout` parameter value. This value is an integer that represents a specific number of minutes. In the following example, the idle timeout value is set to 120 minutes.

```
connectionIdleTimeout = 120
```

2. Restart OracleAS Single Sign-On by restarting OC4J.

Login to Portal Fails

When users try to log in to Portal or an application that is protected by OracleAS Single Sign-On, they see one of the following errors:

- Unexpected error encountered in `wwsec_app_priv.process_signon` (User-Defined Exception) (WWC-41417)
- An entry was not found in the Oracle Internet Directory (error status: -5: The specified user does not exist in the directory)
- Details Operation: `dbms_ldap_utl.get_group_membership`). (WWC-41745)

Problem

This occurs because the single sign-on server caches user entries by default. If a user has been deleted and re-created in Oracle Internet Directory, the user entry's `orclGUID` attribute has changed, thus causing the cache to be out of synch with the directory data. When the application then tries to access the user entry in Oracle Internet Directory, the `orclGUID` value that is returned by the single sign-on server does not match the `orclGUID` of the entry.

This can also happen when adding and deleting users to a realm that has multiple search bases configured (`orclcommonusersearchbase` attribute in the `cn=Common, cn=Products, cn=OracleContext` entry). If, for example, a user with

the same nickname exists in more than one search base and then the user entry in the first listed search base is deleted, this can cause a mismatch between the cache and the directory data.

Solution

Disable the cache by performing the following steps:

1. Take back up of `/sso/conf/policy.properties`.
2. Edit the `policy.properties` file and change `cacheSize=1000` to `cacheSize=-1`.
3. Restart the single sign-on server:

```
opmnctl restartproc process-type=OC4J_SECURITY
```

Problems and Solutions for Certificate Authentication Errors

To perform general debugging for certificate authentication, follow these steps:

1. Set the debug level in `policy.properties` to `DEBUG`; then restart the single sign-on middle tier:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY
```

2. To view browser certificate information while debugging, extract the file `certinfo.jsp` file from `ORACLE_HOME/sso/lib/ipassample.jar`.
3. Place the file into `ORACLE_HOME/j2ee/applications/sso/web/jsp`.
4. View the file at this URL:

```
https://host:port/sso/certinfo.jsp
```

The following issues may occur when using certificate authentication with OracleAS Single Sign-On:

- [Network Error: Connection Refused](#)
- [The Single Sign-On Server Fails to Prompt the User for a Certificate](#)
- [Certificate Authentication Fails - User Is Presented with the Login Page](#)
- [User's Browser Certificate Not Found](#)
- [Mapping Module Class Name Not Found](#)
- [Mapping Module Instance Creation Failed](#)
- [Cannot Create the Mapping Module Object](#)
- [Exception in Creating Mapping Module](#)
- [Certificate Match Failed](#)

Network Error: Connection Refused

Problem

This message appears when the user tries to access a partner application over SSL. The parameter `SSLEngine` on may be missing from `httpd.conf` or may not have been entered correctly.

Solution

Add the missing parameter as specified in "[Setting SSL Parameters](#)" in [Chapter 8](#). If the parameter is present and is entered correctly, the Oracle HTTP Server log file may identify the problem.

The Single Sign-On Server Fails to Prompt the User for a Certificate

Problem

The optional parameter `SSLVerifyClient` is missing from `httpd.conf` or has not been entered correctly.

Solution

Add the missing parameter as specified in "[Setting SSL Parameters](#)" in [Chapter 8](#). If the parameter is present and is entered correctly, the Oracle HTTP Server log file may identify the problem.

Certificate Authentication Fails - User Is Presented with the Login Page

Problem

The user's certificate is missing from the directory or has been entered incorrectly. Check `ssoServer.log` for details.

Solution

Reenter the user's certificate in the directory. See the instructions in "[Oracle Internet Directory](#)" in [Chapter 8](#).

User's Browser Certificate Not Found

Problem 1

The user's certificate is not in the browser.

Solution 1

Install a valid certificate in the user's browser.

Problem 2

The SSL wallet on the Oracle HTTP Server may not contain the trusted certificate of the CA that issued the client certificate.

Solution 2

Use Oracle Wallet Manager to determine whether the SSL wallet contains the trusted certificate. To learn how to use the tool, see the chapter about managing wallets and certificates in *Oracle Application Server Administrator's Guide*.

Mapping Module Class Name Not Found

Problem

The class name for the mapping module is missing from `x509CertAuth.properties` or is incorrect.

Solution

Make sure that a value is assigned to the parameter `CertificateMappingModule`. If it is assigned, check that this value is correct.

Mapping Module Instance Creation Failed

Problem

The customized mapping module has been incorrectly implemented.

Solution

Ensure that the custom module has a default constructor.

Cannot Create the Mapping Module Object

Problem

The customized mapping module has been incorrectly implemented.

Solution

Ensure that the customized module implements the interface prescribed in "[Customize the User Name Mapping Module \(Optional\)](#)" in [Chapter 8](#).

Exception in Creating Mapping Module

Problem

The customized mapping module has been incorrectly implemented.

Solution

Ensure that the customized module implements the interface prescribed in "[Customize the User Name Mapping Module \(Optional\)](#)" in [Chapter 8](#).

Certificate Match Failed

Problem

The user's certificate is missing from the directory or has been entered incorrectly. Check `ssoServer.log` for details.

Solution

Reenter the user's certificate in the directory. See the instructions in "[Oracle Internet Directory](#)" in [Chapter 8](#).

Problems and Solutions for Windows Native Authentication Errors

The following issues may occur when using Windows native authentication (WNA) with OracleAS Single Sign-On.

- [A User Cannot Access a URL After Authenticating in Windows](#)
- [A User Who Is Already Authenticated in Windows Cannot Authenticate in the Browser](#)
- [single sign-on server Fails to Start with a Credential Not Found Error](#)

- [Single Sign-On Server Displays Internal Server Error](#)
- [Single Sign-On Users Unable to Authenticate to KDC](#)
- [Windows Login Dialog Appears When Accessing a Partner Application](#)

Most of these issues involve a misconfiguration of the external authentication plug-in or synchronization profile for Microsoft Active Directory. The *Oracle Identity Management Integration Guide* provides more troubleshooting information for Microsoft Active Directory integration issues.

Also refer to note 283268.1 on Oracle *MetaLink*, <http://metalink.oracle.com>, for general troubleshooting tips for OracleAS Single Sign-On and Windows native authentication.

A User Cannot Access a URL After Authenticating in Windows

A user who is able to authenticate in their Windows environment with Microsoft Active Directory cannot access a URL through OracleAS Single Sign-On. The user may see one of the following error messages:

```
Access Forbidden
```

```
HTTP error code 403
```

```
Windows Native Authentication Failed. Please contact your  
administrator.
```

Problem

This can be caused by one of the following problems:

- The required user entry cannot be found in Oracle Internet Directory, preventing the user from accessing the URL through OracleAS Single Sign-On.
- If a user is only logged in to the local domain, for example if the user logged in as administrator on their local machine, the enterprise identity of that user is not known to OracleAS Single Sign-On.

Solution

Try the following to make sure the user identity is recognized in both Microsoft Active Directory and Oracle Internet Directory:

1. Log in to the Windows desktop environment as a user identity that is known in Microsoft Active Directory. Make sure you log in as an actual user and log in to an Microsoft Active Directory domain (not just the local machine).
2. Once you are sure that the user identity is valid in the Microsoft Active Directory domain, verify that the user identity exists in Oracle Internet Directory. If the user does not exist, use the `oditest` utility to troubleshoot any problems with your Microsoft Active Directory synchronization profile.

See the Troubleshooting appendix in the *Oracle Identity Management Integration Guide* for more information about the `oditest` utility.

3. If the user does exist in Oracle Internet Directory, determine whether the Kerberos principal attributes for the user have been properly synchronized from Microsoft Active Directory into Oracle Internet Directory. You can use the `oditest` and `diptester` utilities to troubleshoot any problems with your Microsoft Active Directory synchronization profile.

See the Troubleshooting appendix in the *Oracle Identity Management Integration Guide* for more information about the `oditest` and `diptester` utilities.

A User Who Is Already Authenticated in Windows Cannot Authenticate in the Browser

The user's browser does not authenticate a user who has already authenticated in their Windows environment with Microsoft Active Directory.

Problem

The user's browser does not support Windows Kerberos authentication or is not configured properly.

Solution

See the *Oracle Identity Management Integration Guide* for instructions on configuring the browser to use Windows native authentication.

single sign-on server Fails to Start with a Credential Not Found Error

The single sign-on server fails to start and its startup log file, `ORACLE_HOME/opmn/logs/OC4J~OC4J_SECURITY~default_island~1`, contains the following error message:

```
Credential not found.
```

Problem

The parameter `kerberos-servicename` may not be configured correctly.

Solution

See the *Oracle Identity Management Integration Guide* for details.

Single Sign-On Server Displays Internal Server Error

The single sign-on server displays the following error message when using Windows native authentication:

```
Internal Server error. Please contact your administrator.
```

Problem

Windows native authentication is not configured correctly on the OracleAS Single Sign-On middle tier.

Solution

See the *Oracle Identity Management Integration Guide* for details.

Single Sign-On Users Unable to Authenticate to KDC

Users who are using Windows native authentication see the following error:

```
Could not authenticate to KDC.
```

Problem

The realm name in the Kerberos configuration file, `krb5.conf`, is not configured correctly.

Solution

See the *Oracle Identity Management Integration Guide* for details.

Windows Login Dialog Appears When Accessing a Partner Application

A user who has already authenticated in the Windows environment with Microsoft Active Directory is prompted with the Windows login dialog (username, password, and domain prompt) when trying to access an OracleAS Single Sign-On partner application.

Problem

The single sign-on server is not able to authenticate the Kerberos token because the corresponding user entry cannot be found in Oracle Internet Directory.

Solution

Add the user entry to Oracle Internet Directory, preferably by synchronizing user entries from Microsoft Active Directory into Oracle Internet Directory. You can use the `oditest` and `diptester` utilities to troubleshoot any problems with your Microsoft Active Directory synchronization profile.

See the Troubleshooting appendix in the *Oracle Identity Management Integration Guide* for more information about the `oditest` and `diptester` utilities.

Problems and Solutions for Password Policy Errors

Users may encounter the following issues related to password policy:

- [A Disabled User Can Still Log In](#)
- [A Disabled User Sees "Authentication Failed" Instead of "Account Disabled" Message](#)
- [The User Receives a Password Expiration Message at Login](#)
- [Password Expiration Message Does Not Appear on Command-Line Tools](#)

A Disabled User Can Still Log In

The administrator disabled a user using the `orclIsEnabled` attribute in Oracle Internet Directory, but the user can still log in.

Problem

The `orclIsEnabled` attribute is incorrect.

Solution

Execute `ldapbind` from the command line as the user. If this act invokes an "account disabled error," reenter the attribute value.

A Disabled User Sees "Authentication Failed" Instead of "Account Disabled" Message

Problem

The administrator disabled a user using the `orclIsEnabled` attribute in Oracle Internet Directory, but the user receives an "authentication failed error" instead of an "account disabled" error.

Solution

None. This is the expected behavior. If the user's account is disabled, she receives an "authentication failed error."

The User Receives a Password Expiration Message at Login

Problem

The user's password has expired.

Solution

The administrator has to reset the password. The administrator can enable password expiration warnings in the directory. These warnings prompt users to change their passwords before they expire.

Password Expiration Message Does Not Appear on Command-Line Tools

Problem

The user logs in to the single sign-on server and is told that her password is about to expire and is prompted to change it. When, however, she does a command-line bind, the message does not appear, and the bind succeeds.

Solution

None. Certain extended directory messages are not visible through the command-line tools. These messages are visible only through the LDAP client-side APIs.

Diagnosing OracleAS Single Sign-On Problems

This section provides information to help you diagnose problems with your OracleAS Single Sign-On environment. It contains the following topics:

- [Viewing the Log Files](#)
- [Increasing the Debug Log Level](#)
- [Enabling the Debug Option in the Single Sign-On Database](#)
- [Enabling LDAP Tracing for UI Operations](#)

Note: Do not delete or edit log files while OC4J is running.

Viewing the Log Files

These OracleAS log files record data about single sign-on operations.

- General log file for the single sign-on server:

`ORACLE_HOME/sso/log/ssoServer.log`

Usage Notes:

The single sign-on server writes all errors to this file. You can change the default location by editing `ORACLE_HOME/sso/conf/policy.properties`. You can also use this file to change the logging level.

- Startup error log for single sign-on server:

`ORACLE_HOME/opmn/logs/OC4J-OC4J_SECURITY~default_island-1`

Usage Notes:

This OC4J-generated file reports any errors that occur when the single sign-on server is started. Check the file for error messages if the `opmnctl` command hangs or if it reports errors on the command line when the OC4J_SECURITY instance is started.

- Web application log:

`ORACLE_HOME/j2ee/OC4J_SECURITY/application-deployments/sso/OC4J_SECURITY_default_island_1/application.log`

Usage Notes:

This file reports run-time errors for OC4J applications.

- OC4J servlet access log:

`ORACLE_HOME/j2ee/OC4J_SECURITY/log/OC4J_SECURITY_default_island_1/default-web-access.log`

Usage Notes:

Another OC4J-generated file. The file contains the servlet access logs for single sign-on. Check the file to determine whether the authentication request was received by the authentication servlet.

- Error log for Oracle HTTP Server

`ORACLE_HOME/Apache/Apache/logs/error_log`

Usage Notes:

If the Oracle HTTP Server is configured to rotate its log files, it appends a timestamp to these files. Use this timestamp to find the latest file.

- Access log for Oracle HTTP Server:

`ORACLE_HOME/Apache/Apache/logs/access_lo`

Usage Notes:

If the Oracle HTTP Server is configured to rotate its log files, it appends a timestamp to these files. Use this timestamp to find the latest file.

Increasing the Debug Log Level

OracleAS Single Sign-On provides four levels of debugging. They are listed here in ascending order of detail provided.

- ERROR—log errors only
- WARN—log both errors and warning messages
- INFO—log informational messages—current date and time, for instance—as well as errors and warnings
- DEBUG—log details about program execution as well as errors, warnings, and informational messages

In the course of debugging, you may have to increase the level of debugging to, say, DEBUG. You do this by modifying the file `ORACLE_HOME/sso/conf/policy.properties`.

After changing the debug level, restart the OC4J_SECURITY instance:

`ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY`

Enabling the Debug Option in the Single Sign-On Database

Occasionally you may need to debug the `mod_plsql` code used to access external applications. This task requires that you enable debugging on the single sign-on database and then view detail logs. Note that this procedure does not apply to the debugging of partner applications. Debugging information for these applications is stored only in `ORACLE_HOME/sso/log/ssoServer.log`.

To turn on `mod_plsql` debugging, log in to the `ORASSO` schema and run the `ssolsdbg.sql` script. See [Appendix B](#) to obtain the schema password. Be sure to uncomment the commented lines in the script before running it. A copy of the script is located at `ORACLE_HOME/sso/admin/plsql/sso`.

Here is the script:

```
set scan off;
set feedback ON;
set verify ON;
set pages 50000;
set serveroutput ON;

CREATE OR replace PROCEDURE debug_print (str VARCHAR2) AS
BEGIN

    INSERT INTO wwsso_log$ VALUES (wwsso_log_pk_seq.nextval,
        substr(str, 1, 1000),
        sysdate, dbms_session.unique_session_id);

    commit;

END debug_print;
/

show errors;
```

To query the debug logs, issue this command:

```
SELECT * FROM WWSO_LOG$ ORDER BY ID;
```

To turn off debugging, log in to the `ORASSO` schema and create the PL/SQL script that follows. Be sure to include this step when you finish debugging. If you skip it, superfluous records are created in the database table. See [Appendix B](#) to obtain the schema password.

```
set scan off;
set feedback ON;
set verify ON;
set pages 50000;
set serveroutput ON;

CREATE OR replace PROCEDURE debug_print (str VARCHAR2) AS
-- PRAGMA autonomous_transaction;
BEGIN

    null;

END debug_print;
/
```

```
show errors;
```

Enabling LDAP Tracing for UI Operations

The administration pages for single sign-on use the `DBMS_LDAP` package to perform directory operations. You can obtain details about these operations in the debug logs for the single sign-on database. To pinpoint the error though, you must enable client-side LDAP tracing. In trying, for example, to determine why an administrator cannot see administration links on the single sign-on home page, you can determine the exact point at which an error is being returned by the LDAP client-side APIs. You can then find the trace results in the RDBMS trace files.

Follow these steps to perform client-side tracing:

1. Enable tracing by loading the `debugonldap.sql` package into the `ORASSO` schema:

```
SQL> connect orasso/password
```

See [Appendix B](#) to obtain the schema password.

2. Run the script:

```
SQL> @debugonldap.sql
```

`debugonldap.sql` looks like this:

```
set scan off;
set feedback ON;
set verify ON;
set pages 50000;
set serveroutput ON;

CREATE OR replace PROCEDURE debug_print (str VARCHAR2) AS
BEGIN

    dbms_ldap.set_trace_level(65535);

    INSERT INTO wssso_log$ VALUES
        (wssso_log_pk_seq.nextval, substr(str, 1, 1000), sysdate,
        dbms_session.unique_session_id);

    commit;

END debug_print;
/

show errors;
```

3. Perform a single sign-on operation that raises an error or that requires debugging, for example, log in to the home page as an administrator.
4. Examine the LDAP client logs in the RDBMS trace directory.

You can determine the location of this directory by connecting as `SYS` to the identity management infrastructure database and then issuing this command:

```
SQL> show parameter user_dump_dest
```

The value returned is the directory where trace files are written. Once in the directory, examine the file timestamps to find the relevant file.

If the client-side trace files fail to reveal the problem, perform client-side tracing, then enable server-side tracing. To enable server-side tracing, see the chapter about logging, auditing, and monitoring in *Oracle Internet Directory Administrator's Guide*.

To disable tracing, load and run this package:

```
set scan OFF;
set feedback ON;
set verify ON;
set pages 50000;
set serveroutput ON;

CREATE OR replace PROCEDURE debug_print (str VARCHAR2) AS BEGIN
null;
END debug_print;
/
show errors;
```

Maintenance Tasks for OracleAS Single Sign-On

This section provides information on various maintenance tasks for OracleAS Single Sign-On. It includes the following topics:

- [Managing Single Sign-On Audit Records](#)
- [Refreshing the LDAP Connection Cache](#)
- [Restarting OC4J After Modifying Oracle Internet Directory](#)

Managing Single Sign-On Audit Records

The single sign-on server records authentication failures and successes in the Oracle Identity Management database. In time, the audit table, `ORASSO.WWSSO_AUDIT_LOG_TABLE_T`, runs out of space. When this happens, this error message appears in database alert logs:

```
ORA-1654: unable to extend index ORASSO.AUDIT_INDEX1 by 128 in tablespace IAS_META
```

In addition, further authentication requests fail.

Be sure to monitor `ORASSO.WWSSO_AUDIT_LOG_TABLE_T` regularly. When it becomes full, either back up the table and free up space or add space. Note that this is an internal, product-specific table. This means that you can use SQL*Plus to clean up the table, but you cannot use this tool or any other tool to build reporting or monitoring scripts based on the table.

Refreshing the LDAP Connection Cache

For performance reasons, the single sign-on server caches connections to Oracle Internet Directory. If the directory server has a scheduled or unscheduled outage, the single sign-on server is left holding bad directory connections, and users may encounter directory setup errors when they try to access external applications. If the LDAP connection cache is invalid, the Oracle HTTP Server must be restarted:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
```

Use the following steps to determine whether the LDAP connection cache must be refreshed:

1. Connect to the single sign-on schema. See [Appendix B](#) to obtain the schema password.

2. Issue the following command:

```
SELECT * FROM WSSO_LOG$
```

3. Restart the HTTP server if you see the following error in the log:

```
'INVALID LDAP CONNECTION CACHE: RESTART ORACLE HTTP SERVER'
```

4. Delete the error message from WSSO_LOG\$.

Restarting OC4J After Modifying Oracle Internet Directory

If you change values in Oracle Internet Directory, you must update the single sign-on server with the changes. If, for example, you change a user, subscriber, or group search base in the directory and fail to notify the single sign-on server, users under the modified container are unable to log in. The `ssoreoid.sql` script updates the single sign-on server with directory changes. To learn how to run the script, see "[Updating the Single Sign-On Server with Directory Changes](#)" in [Chapter 3](#).

After running the script, make sure that you restart the single sign-on server:

```
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server  
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

A Word About Non-GET Authentication

The first page of a `mod_osso`-protected application must be a URL that uses the GET authentication method. If the POST method is used, the data that the user provides when logging in is lost during redirection to the single sign-on server. When deciding whether to enable the global user inactivity timeout, note that users are redirected after timing out and logging in again.

Need More Help?

You can find more solutions on Oracle *MetaLink*, <http://metalink.oracle.com>. If you do not find a solution for your problem, log a service request.

To help Oracle Support troubleshoot the problem, perform the steps outlined in MetaLink note 248870.1.

See Also:

- *Oracle Application Server Release Notes*, available on the Oracle Technology Network:
<http://www.oracle.com/technology/documentation/index.html>

Obtaining the Single Sign-On Schema Password

The single sign-on schema password is randomized when the Oracle Application Server infrastructure is installed. You can use either the command-line tool `ldapsearch` or Oracle Directory Manager to obtain the password.

Using the Command Line

Use this syntax to obtain the schema password with `ldapsearch`:

```
ldapsearch -h directory_host_name
           -p directory_ssl_port
           -D directory_bind_dn
           -w directory_bind_dn_password
           -b "orclReferenceName=infrastructure_database"
              "orclresourcename=ORASSO"
              orclpasswordattribute
           -u 1
```

The table that follows defines the parameters passed to `ldapsearch`.

Parameter	Description
<i>directory_host_name</i>	Host name of the directory server.
<i>directory_ssl_port</i>	Port number of the directory server.
<i>directory_bind_dn</i>	Distinguished name of the user authenticating to the directory.
<i>directory_bind_dn_password</i>	Password of the user authenticating to the directory.
<i>infrastructure_database</i>	Distinguished name of the directory entry under which the password attribute (<code>orclpasswordattribute</code>) is located.
<code>-u</code>	Changes the directory port to an SSL port globally.

Here is an example:

```
ldapsearch -h oid.acme.com
           -p 636
           -D "cn=orcladmin"
           -w welcome1
           -b "orclReferenceName=disco.us.acme.com,cn=IAS Infrastructure"
```

```
Databases,cn=IAS,cn=Products,cn=oraclecontext"  
"orclresourcename=ORASSO"  
orclpasswordattribute  
-u 1
```

Using Oracle Directory Manager

Follow these steps to obtain the schema password with Oracle Directory Manager:

1. Launch the tool:

```
ORACLE_HOME/bin/oidadmin
```

2. In the **System Objects** frame, expand in succession the following entries:

- Entry Management
- cn=OracleContext
- cn=Products
- cn=IAS
- cn=IAS Infrastructure Databases
- orclReferenceName=*database_service_name_for_infrastructure_database*
- OrclResourceName=ORASSO

The orclpasswordattribute text box on the OrclResourceName=ORASSO tab contains the schema password.

policy.properties

The `policy.properties` file, provided here, is a multipurpose configuration file that contains basic parameters required by the single sign-on server. The file is also used to implement advanced features such as multilevel authentication.

```
# SSO Server policy configurations

#####
# Authentication Levels
# -----
# Set the auth levels from lower value to higher value.
# 10 being the lowest authentication level
# The auth level names (on the left hand side) can be changed to
# some other names if desired as long as the change is consistent
# in other usages within the policy file.

NoSecurity = 10
LowSecurity = 20
LowMediumSecurity = 30
MediumSecurity = 40
MediumHighSecurity = 50
HighSecurity = 60

#####
# DefaultAuthLevel
# -----
# DefaultAuthLevel entry must have a value assigned.

DefaultAuthLevel = MediumSecurity

#####
# Authentication plugins
# -----
# Assign a class name that implements SSOServerAuthInterface
# for each auth level referenced.
#
# The Authentication level name must be appended with
# "_AuthPlugin" keyword.

MediumSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOServerAuth
#####
# Custom Cookie Provider Class name
# -----
# Sample custom cookie tester provider class
# CustomCookie_ProviderPlugin = oracle.security.sso.server.auth.CustomCookieTester
```

```

# Custom Cookie auth level
# -----
# This is a mandatory attribute. If custom cookies are not needed it should
# be set to a higher value than any of the authentication levels used.

CustomCookieAuthLevel = HighSecurity

#####
# Protected URL configurations
# -----
# Assign a auth level to each protected (partner) application that is
# participating in SSO. If any of the partner apps are not listed with
# a specific auth level, then the DefaultAuthLevel will be used.
#
# Protected application URL configuration format:
# "Partner Application Root URL" = "AuthenticationLevel"
# host.company.com\:port = AuthLevelName
# NOTE: The required backslash(escape character) before the
# colon (:) character immediately preceding.
# There should be a corresponding auth plugin configured for the
# "AuthenticationLevel" used.
#
# Examples:
# The following example configures a SSO partner application hosted
# on host1.company.com:7777 machine using LowSecurity authentication level.
# This configuration will secure all URLs hosted on this host/port.
# host1.company.com\:7777 = LowSecurity
#
# The following example configures a SSO partner application hosted
# on host2.company.com:7777 machine using MediumSecurity authentication level
# This configuration will secure all URLs hosted on this host/port.
# host2.company.com\:7777 = MediumSecurity

#####
#SSO Server specific configurations

# set the cache size in kbytes
#default is 250
cacheSize = -1

#set the minimum number of connections in the connection pool
#default is 5
minConnectionsInPool = 5

#set the maximum number of connections in the connection pool
#default is 150
maxConnectionsInPool = 150

#LDAP and database connection pool timeout in minutes
connectionIdleTimeout = 120

#Debug level {ERROR, WARN, INFO, DEBUG}
# default debug level is set to ERROR
debugLevel = ERROR

#Debug file location
#This is a mandatory property that needs to be passed

```

```
#the SSO server. A valid file location should be specified here
debugFile = /private/vshriram/infra1012/sso/log/ssoServer.log

#Deployment login page link
loginPageUrl = /sso/pages/login.jsp

#Deployment logout page link
logoutPageUrl = /sso/pages/logout.jsp

#Deployment external application login page link
extAppLoginPageUrl = /sso/pages/ealgin.jsp

#Deployment change password page link
chgPasswordPageUrl = /sso/pages/password.jsp

#Wireless login page link
wirelessLoginPageUrl = /wirelessso/wirelesslogin.jsp
wirelessChgPasswordPageUrl = /wirelessso/wirelesscpwd.jsp

SASSOAuthnUrl = http://stads41.us.oracle.com:/sso/authn
SASSOLogoutUrl = http://stads41.us.oracle.com:/sso/jsp/sasso_logout_success.jsp
SASSOAuthLevel = HighSecurity

#SASSO keyfile
SASSOConfigFile = %s_ssoLogOH%/sso/conf/keystore

#SASSO key rollover interval
ROLLOVER_INTERVAL = 600
```

Glossary

3DES

See [Triple Data Encryption Standard \(3DES\)](#).

access control item (ACI)

Access control information represents the permissions that various entities or subjects have to perform operations on a given object in the directory. This information is stored in Oracle Internet Directory as user-modifiable operational [attributes](#), each of which is called an access control item (ACI). An ACI determines user access rights to directory data. It contains a set of rules for controlling access to entries (structural access items) and attributes (content access items). Access to both structural and content access items may be granted to one or more users or groups.

access control list (ACL)

A list of resources and the user names of people who are permitted access to those resources within a computer system. In Oracle Internet Directory, an ACL is a list of [access control item \(ACI\) attribute values](#) that is associated with directory objects. The attribute values on that list represent the permissions that various directory user entities (or subjects) have on a given object.

access control policy point (ACP)

A directory entry that contains access control policy information that applies downward to all entries at lower positions in the [directory information tree \(DIT\)](#). This information affects the entry itself and all entries below it. In Oracle Internet Directory, you can create ACPs to apply an access control policy throughout a [subtree](#) of your directory.

account lockout

A security feature that locks a user account if repeated failed logon attempts occur within a specified amount of time, based on security policy settings. Account lockout occurs in OracleAS Single Sign-On when a user submits an account and password combination from any number of workstations more times than is permitted by Oracle Internet Directory. The default lockout period is 24 hours.

ACI

See [access control item \(ACI\)](#).

ACL

See [access control list \(ACL\)](#).

ACP

See [access control policy point \(ACP\)](#).

administrative area

A [subtree](#) on a directory server whose entries are under the control of a single administrative authority. The designated administrator controls each [entry](#) in that administrative area, as well as the directory [schema](#), [access control list \(ACL\)](#), and [attributes](#) for those entries.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a [symmetric cryptography](#) algorithm that is intended to replace [Data Encryption Standard \(DES\)](#). AES is a Federal Information Processing Standard (FIPS) for the encryption of commercial and government data.

advanced replication

See [Oracle Database Advanced Replication](#).

advanced symmetric replication (ASR)

See [Oracle Database Advanced Replication](#).

AES

See [Advanced Encryption Standard \(AES\)](#).

anonymous authentication

The process by which a directory authenticates a user without requiring a user name and password combination. Each anonymous user then exercises the privileges specified for anonymous users.

API

See [application programming interface \(API\)](#).

application programming interface (API)

A series of software routines and development tools that comprise an interface between a computer application and lower-level services and functions (such as the operating system, device drivers, and other software applications). APIs serve as building blocks for programmers putting together software applications. For example, LDAP-enabled clients access Oracle Internet Directory information through programmatic calls available in the LDAP API.

application service provider

Application Service Providers (ASPs) are third-party entities that manage and distribute software-based services and solutions to customers across a wide area network from a central data center. In essence, ASPs are a way for companies to outsource some or almost all aspects of their information technology needs.

artifact profile

An [authentication](#) mechanism which transmits data using a compact reference to an [assertion](#), called an artifact, instead of sending the full assertion. This [profile](#) accommodates browsers which handle a limited number of characters.

ASN.1

Abstract Syntax Notation One (ASN.1) is an International Telecommunication Union (ITU) notation used to define the syntax of information data. ASN.1 is used to describe

structured information, typically information that is to be conveyed across some communications medium. It is widely used in the specification of Internet protocols.

ASR

See [Oracle Database Advanced Replication](#).

assertion

An assertion is a statement used by providers in security domains to exchange information about a subject seeking access to a resource. Identity providers, as well as service providers, exchange assertions about identities to make [authentication](#) and [authorization](#) decisions, and to determine and enforce security policies protecting the resource.

asymmetric algorithm

A [cryptographic algorithm](#) that uses different [keys](#) for [encryption](#) and [decryption](#).

See also: [public key cryptography](#).

asymmetric cryptography

See [public key cryptography](#).

attribute

Directory attributes hold a specific data element such as a name, phone number, or job title. Each directory [entry](#) is comprised of a set of attributes, each of which belongs to an [object class](#). Moreover, each attribute has both a *type*, which describes the kind of information in the attribute, and a *value*, which contains the actual data.

attribute configuration file

In an Oracle Directory Integration Platform environment, a file that specifies attributes of interest in a connected directory.

attribute type

Attribute types specify information about a data element, such as the data type, maximum length, and whether it is single-valued or multivalued. The attribute type provides the real-world meaning for a value, and specifies the rules for creating and storing specific pieces of data, such as a name or an e-mail address.

attribute uniqueness

An Oracle Internet Directory feature that ensures that no two specified [attributes](#) have the same value. It enables applications synchronizing with the enterprise directory to use attributes as unique keys.

attribute value

Attribute values are the actual data contained within an [attribute](#) for a particular [entry](#). For example, for the attribute type `email`, an attribute value might be `sally.jones@oracle.com`.

authentication

The process of verifying the identity claimed by an entity based on its credentials. Authentication of a user is generally based on something the user knows or has (for example, a password or a certificate).

Authentication of an electronic message involves the use of some kind of system (such as [public key cryptography](#)) to ensure that a file or message which claims to originate

from a given individual or company actually does, and a check based on the contents of a message to ensure that it was not modified in transit.

authentication level

An OracleAS Single Sign-On parameter that enables you to specify a particular authentication behavior for an application. You can link this parameter with a specific [authentication plugin](#).

authentication plugin

An implementation of a specific authentication method. OracleAS Single Sign-On has Java plugins for password authentication, digital certificates, Windows native authentication, and third-party access management.

authorization

The process of granting or denying access to a service or network resource. Most security systems are based on a two step process. The first stage is authentication, in which a user proves his or her identity. The second stage is authorization, in which a user is allowed to access various resources based on his or her identity and the defined [authorization policy](#).

authorization policy

Authorization policy describes how access to a protected resource is governed. Policy maps identities and objects to collections of rights according to some system model. For example, a particular authorization policy might state that users can access a sales report only if they belong to the sales group.

basic authentication

An [authentication](#) protocol supported by most browsers in which a Web server authenticates an entity with an encoded user name and password passed using data transmissions. Basic authentication is sometimes called plaintext authentication because the base-64 encoding can be decoded by anyone with a freely available decoding utility. Note that encoding is not the same as [encryption](#).

Basic Encoding Rules (BER)

Basic Encoding Rules (BER) are the standard rules for encoding data units set forth in [ASN.1](#). BER is sometimes incorrectly paired with ASN.1, which applies only to the abstract syntax description language, not the encoding technique.

BER

See [Basic Encoding Rules \(BER\)](#).

binding

In networking, binding is the establishment of a logical connection between communicating entities.

In the case of Oracle Internet Directory, binding refers to the process of authenticating to the directory.

The formal set of rules for carrying a [SOAP](#) message within or on top of another protocol (underlying protocol) for the purpose of exchange is also called a binding.

block cipher

Block ciphers are a type of [symmetric algorithm](#). A block cipher encrypts a message by breaking it down into fixed-size blocks (often 64 bits) and encrypting each block with a key. Some well known block ciphers include [Blowfish](#), [DES](#), and [AES](#).

See also: [stream cipher](#).

Blowfish

Blowfish is a [symmetric cryptography](#) algorithm developed by Bruce Schneier in 1993 as a faster replacement for [DES](#). It is a [block cipher](#) using 64-bit blocks and keys of up to 448 bits.

CA

See [Certificate Authority \(CA\)](#).

CA certificate

A [Certificate Authority \(CA\)](#) signs all certificates that it issues with its [private key](#). The corresponding Certificate Authority's [public key](#) is itself contained within a certificate, called a CA Certificate (also referred to as a root certificate). A browser must contain the CA Certificate in its list of trusted root certificates in order to trust messages signed by the CA's private key.

cache

Generally refers to an amount of quickly accessible memory in your computer. However, on the Web it more commonly refers to where the browser stores downloaded files and graphics on the user's computer.

CBC

See [cipher block chaining \(CBC\)](#).

central directory

In an Oracle Directory Integration Platform environment, the directory that acts as the central repository. In an Oracle Directory Integration Platform environment, Oracle Internet Directory is the central directory.

certificate

A certificate is a specially formatted data structure that associates a [public key](#) with the identity of its owner. A certificate is issued by a [Certificate Authority \(CA\)](#). It contains the name, serial number, expiration dates, and public key of a particular entity. The certificate is digitally signed by the issuing CA so that a recipient can verify that the certificate is real. Most digital certificates conform to the [X.509](#) standard.

Certificate Authority (CA)

A Certificate Authority (CA) is a trusted third party that issues, renews, and revokes digital [certificates](#). The CA essentially vouches for an entity's identity, and may delegate the verification of an applicant to a [Registration Authority \(RA\)](#). Some well known Certificate Authorities (CAs) include Digital Signature Trust, Thawte, and VeriSign.

certificate chain

An ordered list of certificates containing one or more pairs of a user [certificate](#) and its associated [CA certificate](#).

certificate management protocol (CMP)

Certificate Management Protocol (CMP) handles all relevant aspects of certificate creation and management. CMP supports interactions between [public key infrastructure \(PKI\)](#) components, such as the [Certificate Authority \(CA\)](#), [Registration Authority \(RA\)](#), and the user or application that is issued a certificate.

certificate request message format (CRMF)

Certificate Request Message Format (CRMF) is a format used for messages related to the life-cycle management of [X.509](#) certificates, as described in the [RFC 2511](#) specification.

certificate revocation list (CRL)

A Certificate Revocation List (CRL) is a list of digital [certificates](#) which have been revoked by the [Certificate Authority \(CA\)](#) that issued them.

change logs

A database that records changes made to a directory server.

cipher

See [cryptographic algorithm](#).

cipher block chaining (CBC)

Cipher block chaining (CBC) is a mode of operation for a [block cipher](#). CBC uses what is known as an initialization vector (IV) of a certain length. One of its key characteristics is that it uses a chaining mechanism that causes the decryption of a block of ciphertext to depend on all the preceding ciphertext blocks. As a result, the entire validity of all preceding blocks is contained in the immediately previous ciphertext block.

cipher suite

In [Secure Sockets Layer \(SSL\)](#), a set of authentication, encryption, and data integrity algorithms used for exchanging messages between network nodes. During an SSL handshake, the two nodes negotiate to see which cipher suite they will use when transmitting messages back and forth.

ciphertext

Ciphertext is the result of applying a [cryptographic algorithm](#) to readable data (plaintext) in order to render the data unreadable by all entities except those in possession of the appropriate [key](#).

circle of trust

A trust relationship among a set of identity providers and service providers that allows a [principal](#) to use a single federated identity and [single sign-on \(SSO\)](#) when conducting business transactions with providers within that set.

Businesses federate or affiliate together into circles of trust based on Liberty-enabled technology and on operational agreements that define trust relationships between the businesses.

See also: [federated identity management \(FIM\)](#), [Liberty Alliance](#).

claim

A claim is a declaration made by an entity (for example, a name, identity, key, group, and so on).

client SSL certificates

A type of [certificate](#) used to identify a client machine to a server through [Secure Sockets Layer \(SSL\)](#) (client authentication).

cluster

A collection of interconnected usable whole computers that is used as a single computing resource. Hardware clusters provide high availability and scalability.

CMP

See [certificate management protocol \(CMP\)](#).

CMS

See [Cryptographic Message Syntax \(CMS\)](#).

code signing certificates

A type of [certificate](#) used to identify the entity who signed a Java program, Java Script, or other signed file.

cold backup

In Oracle Internet Directory, this refers to the procedure of adding a new [directory system agent \(DSA\)](#) node to an existing replicating system by using the database copy procedure.

concurrency

The ability to handle multiple requests simultaneously. Threads and processes are examples of concurrency mechanisms.

concurrent clients

The total number of clients that have established a session with Oracle Internet Directory.

concurrent operations

The number of operations that are being executed on Oracle Internet Directory from all of the [concurrent clients](#). Note that this is not necessarily the same as the concurrent clients, because some of the clients may be keeping their sessions idle.

confidentiality

In cryptography, confidentiality (also known as privacy) is the ability to prevent unauthorized entities from reading data. This is typically achieved through [encryption](#).

configset

See [configuration set entry](#).

configuration set entry

An Oracle Internet Directory entry holding the configuration parameters for a specific instance of the directory server. Multiple configuration set entries can be stored and referenced at runtime. The configuration set entries are maintained in the subtree specified by the `subConfigsubEntry` attribute of the [directory-specific entry \(DSE\)](#), which itself resides in the associated [directory information base \(DIB\)](#) against which the servers are started.

connect descriptor

A specially formatted description of the destination for a network connection. A connect descriptor contains destination service and network route information.

The destination service is indicated by using its service name for the Oracle Database or its Oracle System Identifier (SID) for Oracle release 8.0 or version 7 databases. The

network route provides, at a minimum, the location of the listener through use of a network address.

connected directory

In an Oracle Directory Integration Platform environment, an information repository requiring full synchronization of data between Oracle Internet Directory and itself—for example, an Oracle human resources database.

consumer

A directory server that is the destination of replication updates. Sometimes called a slave.

contention

Competition for resources.

context prefix

The **distinguished name (DN)** of the root of a **naming context**.

CRL

See **certificate revocation list (CRL)**.

CRMF

See **certificate request message format (CRMF)**.

cryptographic algorithm

A cryptographic algorithm is a defined sequence of processes to convert readable data (plaintext) to unreadable data (ciphertext) and vice versa. These conversions require some secret knowledge, normally contained in a **key**. Examples of cryptographic algorithms include **DES**, **AES**, **Blowfish**, and **RSA**.

Cryptographic Message Syntax (CMS)

Cryptographic Message Syntax (CMS) is a syntax defined in **RFC 3369** for signing, digesting, authenticating, and encrypting digital messages.

cryptography

The process of protecting information by transforming it into an unreadable format. The information is encrypted using a **key**, which makes the data unreadable, and is then decrypted later when the information needs to be used again. See also **public key cryptography** and **symmetric cryptography**.

dads.conf

A configuration file for Oracle HTTP Server that is used to configure a **database access descriptor (DAD)**.

DAS

See **Oracle Delegated Administration Services**. (DAS).

Data Encryption Standard (DES)

Data Encryption Standard (DES) is a widely used **symmetric cryptography** algorithm developed in 1974 by IBM. It applies a 56-bit key to each 64-bit block of data. DES and 3DES are typically used as encryption algorithms by **S/MIME**.

data integrity

The guarantee that the contents of the message received were not altered from the contents of the original message sent.

See also: [integrity](#).

database access descriptor (DAD)

Database connection information for a particular Oracle Application Server component, such as the OracleAS Single Sign-On schema.

decryption

The process of converting the contents of an encrypted message (ciphertext) back into its original readable format (plaintext).

default identity management realm

In a hosted environment, one enterprise—for example, an application service provider—makes Oracle components available to multiple other enterprises and stores information for them. In such hosted environments, the enterprise performing the hosting is called the default identity management realm, and the enterprises that are hosted are each associated with their own identity management realm in the [directory information tree \(DIT\)](#).

default knowledge reference

A [knowledge reference](#) that is returned when the base object is not in the directory, and the operation is performed in a [naming context](#) not held locally by the server. A default knowledge reference typically sends the user to a server that has more knowledge about the directory partitioning arrangement.

default realm location

An attribute in the [root Oracle Context](#) that identifies the root of the [default identity management realm](#).

defederation

The act of unlinking a user's account from an [identity provider](#) or [service provider](#).

Delegated Administration Services

See [Oracle Delegated Administration Services](#).

delegated administrator

In a hosted environment, one enterprise—for example, an application service provider—makes Oracle components available to multiple other enterprises and stores information for them. In such an environment, a global administrator performs activities that span the entire directory. Other administrators—called delegated administrators—may exercise roles in specific identity management realms, or for specific applications.

DER

See [Distinguished Encoding Rules \(DER\)](#).

DES

See [Data Encryption Standard \(DES\)](#).

DIB

See [directory information base \(DIB\)](#).

Diffie-Hellman

Diffie-Hellman (DH) is a public key cryptography protocol that allows two parties to establish a shared secret over an unsecure communications channel. First published in 1976, it was the first workable public key cryptographic system.

See also: [symmetric algorithm](#).

digest

See [message digest](#).

digital certificate

See [certificate](#).

digital signature

A digital signature is the result of a two-step process applied to a given block of data. First, a [hash function](#) is applied to the data to obtain a result. Second, that result is encrypted using the signer's [private key](#). Digital signatures can be used to ensure integrity, message authentication, and non-repudiation of data. Examples of digital signature algorithms include [DSA](#), [RSA](#), and [ECDSA](#).

Digital Signature Algorithm (DSA)

The Digital Signature Algorithm (DSA) is an [asymmetric algorithm](#) that is used as part of the Digital Signature Standard (DSS). It cannot be used for encryption, only for digital signatures. The algorithm produces a pair of large numbers that enable the authentication of the signatory, and consequently, the integrity of the data attached. DSA is used both in generating and verifying digital signatures.

See also: [Elliptic Curve Digital Signature Algorithm \(ECDSA\)](#).

directory

See [Oracle Internet Directory](#), [Lightweight Directory Access Protocol \(LDAP\)](#), and [X.500](#).

directory information base (DIB)

The complete set of all information held in the directory. The DIB consists of entries that are related to each other hierarchically in a [directory information tree \(DIT\)](#).

directory information tree (DIT)

A hierarchical tree-like structure consisting of the [DNs](#) of the entries.

directory integration and provisioning server

In an Oracle Directory Integration Platform environment, the server that drives the synchronization of data between Oracle Internet Directory and a [connected directory](#).

directory integration profile

In an Oracle Directory Integration Platform environment, an entry in Oracle Internet Directory that describes how Oracle Directory Integration Platform communicates with external systems and what is communicated.

Directory Manager

See [Oracle Directory Manager](#).

directory naming context

See [naming context](#).

directory provisioning profile

A special kind of [directory integration profile](#) that describes the nature of provisioning-related notifications that Oracle Directory Integration Platform sends to the directory-enabled applications.

directory replication group (DRG)

The directory servers participating in a [replication agreement](#).

directory server instance

A discrete invocation of a directory server. Different invocations of a directory server, each started with the same or different configuration set entries and startup flags, are said to be different directory server instances.

directory synchronization profile

A special kind of [directory integration profile](#) that describes how synchronization is carried out between Oracle Internet Directory and an external system.

directory system agent (DSA)

The [X.500](#) term for a directory server.

directory-specific entry (DSE)

An entry specific to a directory server. Different directory servers may hold the same [directory information tree \(DIT\)](#) name, but have different contents—that is, the contents can be specific to the directory holding it. A DSE is an entry with contents specific to the directory server holding it.

directory user agent (DUA)

The software that accesses a directory service on behalf of the directory user. The directory user may be a person or another software element.

DIS

See [directory integration and provisioning server](#).

Distinguished Encoding Rules (DER)

Distinguished Encoding Rules (DER) are a set of rules for encoding [ASN.1](#) objects in byte-sequences. DER is a special case of [Basic Encoding Rules \(BER\)](#).

distinguished name (DN)

A [X.500](#) distinguished name (DN) is a unique name for a node in a directory tree. A DN is used to provide a unique name for a person or any other directory entry. A DN is a concatenation of selected [attributes](#) from each node in the tree along the path from the root node to the named entry's node. For example, in LDAP notation, the DN for a person named John Smith working at Oracle's US office would be: "cn=John Smith, ou=People, o=Oracle, c=us".

DIT

See [directory information tree \(DIT\)](#).

DN

See [distinguished name \(DN\)](#).

Document Type Definition (DTD)

A Document Type Definition (DTD) is a document that specifies constraints on the tags and tag sequences that are valid for a given [XML](#) document. DTDs follow the rules of Simple Generalized Markup Language (SGML), the parent language of XML.

domain

A domain includes the Web site and applications that enable a [principal](#) to utilize resources. A federated site acts as an [identity provider](#) (also known as the source domain), a [service provider](#) (also known as the destination domain), or both.

domain component attribute

The domain component (dc) attribute can be used in constructing a [distinguished name \(DN\)](#) from a domain name. For example, using a domain name such as "oracle.com", one could construct a DN beginning with "dc=oracle, dc=com", and then use this DN as the root of its subtree of directory information.

DRG

See [directory replication group \(DRG\)](#).

DSA

See [Digital Signature Algorithm \(DSA\)](#) or [directory system agent \(DSA\)](#).

DSE

See [directory-specific entry \(DSE\)](#).

DTD

See [Document Type Definition \(DTD\)](#).

ECC

See [Elliptic Curve Cryptography \(ECC\)](#).

ECDSA

See [Elliptic Curve Digital Signature Algorithm \(ECDSA\)](#).

EJB

See [Enterprise Java Bean \(EJB\)](#).

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is an alternative to the [RSA](#) encryption system which is based on the difficulty of solving elliptic curve discrete logarithm problems rather than on factoring large numbers. Developed and marketed by Certicom, ECC is especially suitable for environments, such as wireless devices and PC cards, where computational power is limited and high speed is required. For any given key size (measured in bits) ECC provides more security (is harder to decrypt without the key) than RSA.

Elliptic Curve Digital Signature Algorithm (ECDSA)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analog of the [Digital Signature Algorithm \(DSA\)](#) standard. The advantages of ECDSA compared to RSA-like schemes are shorter key lengths and faster signing and decryption. For example, a 160 (210) bit ECC key is expected to give the same security as a 1024 (2048) bit RSA key, and the advantage increases as level of security is raised.

encryption

Encryption is the process of converting plaintext to ciphertext by applying a [cryptographic algorithm](#).

encryption certificate

An encryption certificate is a [certificate](#) containing a [public key](#) that is used to encrypt electronic messages, files, documents, or data transmission, or to establish or exchange a session key for these same purposes.

end-to-end security

This is a property of message-level security that is established when a message traverses multiple applications within and between business entities and is secure over its full route through and between the business entities.

Enterprise Java Bean (EJB)

Enterprise JavaBeans (EJBs) are a Java API developed by Sun Microsystems that defines a component architecture for multi-tier client/server systems. Because EJB systems are written in Java, they are platform independent. Being object oriented, they can be implemented into existing systems with little or no recompiling and configuring.

Enterprise Manager

See [Oracle Enterprise Manager](#).

entry

An entry is a unique record in a directory that describes an object, such as a person. An entry consists of [attributes](#) and their associated [attribute values](#), as dictated by the [object class](#) that describes that entry object. All entries in an LDAP directory structure are uniquely identified through their [distinguished name \(DN\)](#).

export agent

In an Oracle Directory Integration Platform environment, an agent that exports data out of Oracle Internet Directory.

export data file

In an Oracle Directory Integration Platform environment, the file that contains data exported by an [export agent](#).

export file

See [export data file](#).

external agent

A directory integration agent that is independent of Oracle Directory Integration Platform server. Oracle Directory Integration Platform server does not provide scheduling, mapping, or error handling services for it. An external agent is typically used when a third party metadirectory solution is integrated with Oracle Directory Integration Platform.

external application

Applications that do not delegate authentication to the OracleAS Single Sign-On server. Instead, they display HTML login forms that ask for application user names and passwords. At the first login, users can choose to have the OracleAS Single

Sign-On server retrieve these credentials for them. Thereafter, they are logged in to these applications transparently.

failover

The process of failure recognition and recovery. In an Oracle Application Server Cold Failover Cluster (Identity Management), an application running on one cluster node is transparently migrated to another cluster node. During this migration, clients accessing the service on the cluster see a momentary outage and may need to reconnect once the failover is complete.

fan-out replication

Also called a point-to-point replication, a type of replication in which a supplier replicates directly to a consumer. That consumer can then replicate to one or more other consumers. The replication can be either full or partial.

Federal Information Processing Standards (FIPS)

Federal Information Processing Standards (FIPS) are standards for information processing issued by the US government Department of Commerce's National Institute of Standards and Technology (NIST).

federated identity management (FIM)

The agreements, standards, and technologies that make identity and entitlements portable across autonomous domains. FIM makes it possible for an authenticated user to be recognized and take part in personalized services across multiple domains. It avoids pitfalls of centralized storage of personal information, while allowing users to link identity information between different accounts. Federated identity requires two key components: trust and standards. The trust model of federated identity management is based on [circle of trust](#). The standards are defined by the [Liberty Alliance](#) Project.

federation

See [identity federation](#).

filter

A filter is an expression that defines the entries to be returned from a request or search on a directory. Filters are typically expressed as DNs, for example: `cn=susie smith,o=acme,c=us`.

FIM

See [federated identity management \(FIM\)](#).

FIPS

See [Federal Information Processing Standards \(FIPS\)](#).

forced authentication

The act of forcing a user to reauthenticate if he or she has been idle for a preconfigured amount of time. Oracle Application Server Single Sign-On enables you to specify a global user inactivity timeout. This feature is intended for installations that have sensitive applications.

GET

An authentication method whereby login credentials are submitted as part of the login URL.

global administrator

In a hosted environment, one enterprise—for example, an application service provider—makes Oracle components available to multiple other enterprises and stores information for them. In such an environment, a global administrator performs activities that span the entire directory.

global unique identifier (GUID)

An identifier generated by the system and inserted into an entry when the entry is added to the directory. In a multimaster replicated environment, the GUID, not the DN, uniquely identifies an entry. The GUID of an entry cannot be modified by a user.

global user inactivity timeout

An optional feature of Oracle Application Server Single Sign-On that forces users to reauthenticate if they have been idle for a preconfigured amount of time. The global user inactivity timeout is much shorter than the single sign-out session timeout.

globalization support

Multilanguage support for graphical user interfaces. Oracle Application Server Single Sign-On supports 29 languages.

globally unique user ID

A numeric string that uniquely identifies a user. A person may change or add user names, passwords, and distinguished names, but her globally unique user ID always remains the same.

grace login

A login occurring within the specified period before password expiration.

group search base

In the Oracle Internet Directory default [directory information tree \(DIT\)](#), the node in the identity management realm under which all the groups can be found.

guest user

One who is not an anonymous user, and, at the same time, does not have a specific user entry.

GUID

See [global unique identifier \(GUID\)](#).

handshake

A protocol two computers use to initiate a communication session.

hash

A number generated from a string of text with an algorithm. The hash value is substantially smaller than the text itself. Hash numbers are used for security and for faster access to data.

See also: [hash function](#).

hash function

In cryptography, a hash function or one-way hash function is an algorithm that produces a given value when applied to a given block of data. The result of a hash function can be used to ensure the integrity of a given block of data. For a hash

function to be considered secure, it must be very difficult, given a known data block and a known result, to produce another data block that produces the same result.

Hashed Message Authentication Code (HMAC)

Hashed Message Authentication Code (HMAC) is a hash function technique used to create a secret hash function output. This strengthens existing hash functions such as MD5 and SHA. It is used in transport layer security (TLS).

HMAC

See [Hashed Message Authentication Code \(HMAC\)](#).

HTTP

The Hyper Text Transfer Protocol (HTTP) is the protocol used between a Web browser and a server to request a document and transfer its contents. The specification is maintained and developed by the World Wide Web Consortium.

HTTP Redirect Profile

A [federation](#) profile which indicates that the requested resource resides under a different URL.

HTTP Server

See [Oracle HTTP Server](#).

httpd.conf

The file used to configure [Oracle HTTP Server](#).

iASAdmins

The administrative group responsible for user and group management functions in Oracle Application Server. The OracleAS Single Sign-On administrator is a member of the group iASAdmins.

identity federation

The linking of two or more accounts a [principal](#) may hold with one or more identity providers or service providers within a given [circle of trust](#).

When users federate the otherwise isolated accounts they have with businesses, known as their local identities, they create a relationship between two entities, an association comprising any number of service providers and identity providers.

See also: [identity provider](#), [service provider](#).

identity management

The process by which the complete security lifecycle for network entities is managed in an organization. It typically refers to the management of an organization's application users, where steps in the security life cycle include account creation, suspension, privilege modification, and account deletion. The network entities managed may also include devices, processes, applications, or anything else that needs to interact in a networked environment. Entities managed by an identity management process may also include users outside of the organization, for example customers, trading partners, or Web services.

identity management infrastructure database

The database that contains data for OracleAS Single Sign-On and Oracle Internet Directory.

identity management realm

A collection of identities, all of which are governed by the same administrative policies. In an enterprise, all employees having access to the intranet may belong to one realm, while all external users who access the public applications of the enterprise may belong to another realm. An identity management realm is represented in the directory by a specific **entry** with a special **object class** associated with it.

identity management realm-specific Oracle Context

An Oracle Context contained in each identity management realm. It stores the following information:

- User naming policy of the identity management realm—that is, how users are named and located.
- Mandatory authentication attributes.
- Location of groups in the identity management realm.
- Privilege assignments for the identity management realm—for example: who has privileges to add more users to the realm.
- Application specific data for that realm including authorizations.

identity provider

One of the three primary roles defined in the **identity federation** protocols supported by OSFS. The other primary roles are **service provider** and **principal**. The identity provider is responsible for managing and authenticating a set of identities within a given **circle of trust**.

A service provider, in turn, provides services or goods to a principal based on the identity provider's authentication of a principal's identity.

Identity providers are service providers offering business incentives so that other service providers affiliate with them. An identity provider typically authenticates and asserts a principal's identity.

import agent

In an Oracle Directory Integration Platform environment, an agent that imports data into Oracle Internet Directory.

import data file

In an Oracle Directory Integration Platform environment, the file containing the data imported by an **import agent**.

infrastructure tier

The Oracle Application Server components responsible for identity management. These components are OracleAS Single Sign-On, Oracle Delegated Administration Services, and Oracle Internet Directory.

inherit

When an **object class** has been derived from another class, it also derives, or inherits, many of the characteristics of that other class. Similarly, an attribute subtype inherits the characteristics of its supertype.

instance

See **directory server instance**.

integrity

In cryptography, integrity is the ability to detect if data has been modified by entities that are not authorized to modify it.

Internet Directory

See [Oracle Internet Directory](#).

Internet Engineering Task Force (IETF)

The principal body engaged in the development of new Internet standard specifications. It is an international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Internet Message Access Protocol (IMAP)

A protocol allowing a client to access and manipulate electronic mail messages on a server. It permits manipulation of remote message folders, also called mailboxes, in a way that is functionally equivalent to local mailboxes.

J2EE

See [Java 2 Platform, Enterprise Edition \(J2EE\)](#).

Java 2 Platform, Enterprise Edition (J2EE)

Java 2 Platform, Enterprise Edition (J2EE) is an environment for developing and deploying enterprise applications, defined by Sun Microsystems Inc. The J2EE platform consists of a set of services, application programming interfaces (APIs), and protocols that provide the functionality for developing multitiered, Web-based applications.

Java Server Page (JSP)

JavaServer Pages (JSP), a server-side technology, are an extension to the Java servlet technology that was developed by Sun Microsystems. JSPs have dynamic scripting capability that works in tandem with HTML code, separating the page logic from the static elements (the design and display of the page). Embedded in the HTML page, the Java source code and its extensions help make the HTML more functional, being used in dynamic database queries, for example.

JSP

See [Java Server Page \(JSP\)](#).

key

A key is a data structure that contains some secret knowledge necessary to successfully encrypt or decrypt a given block of data. The larger the key, the harder it is to crack a block of encrypted data. For example, a 256-bit key is more secure than a 128-bit key.

key pair

A [public key](#) and its associated [private key](#).

See also: [public/private key pair](#).

knowledge reference

The access information (name and address) for a remote [directory system agent \(DSA\)](#) and the name of the [directory information tree \(DIT\)](#) subtree that the remote DSA holds. Knowledge references are also called referrals.

latency

The time a client has to wait for a given directory operation to complete. Latency can be defined as wasted time. In networking discussions, latency is defined as the travel time of a packet from source to destination.

LDAP

See [Lightweight Directory Access Protocol \(LDAP\)](#).

LDAP connection cache

To improve throughput, the OracleAS Single Sign-On server caches and then reuses connections to Oracle Internet Directory.

LDAP Data Interchange Format (LDIF)

A common, text-based format for exchanging directory data between systems. The set of standards for formatting an input file for any of the LDAP command-line utilities.

LDIF

See [LDAP Data Interchange Format \(LDIF\)](#).

legacy application

Older application that cannot be modified to delegate authentication to the OracleAS Single Sign-On server. Also known as an [external application](#).

Liberty Alliance

The Liberty Alliance Project is a consortium of companies, non-profits, and non-government organizations around the globe. It is committed to developing an open standard for [federated identity management \(FIM\)](#) and identity-based Web services supporting current and emerging network devices.

Liberty ID-FF

Liberty Identity Federation Framework (Liberty ID-FF) provides an architecture for Web-based [single sign-on \(SSO\)](#) with federated identities.

Lightweight Directory Access Protocol (LDAP)

A set of protocols for accessing information in directories. LDAP supports TCP/IP, which is necessary for any type of Internet access. Its framework of design conventions supports industry-standard directory products, such as Oracle Internet Directory. Because it is a simpler version of the [X.500](#) standard, LDAP is sometimes called X.500 light.

load balancer

Hardware devices and software that balance connection requests between two or more servers, either due to heavy load or failover. BigIP, Alteon, or Local Director are all popular hardware devices. Oracle Application Server Web Cache is an example of load balancing software.

logical host

In an Oracle Application Server Cold Failover Cluster (Identity Management), one or more disk groups and pairs of host names and IP addresses. It is mapped to a physical host in the cluster. This physical host impersonates the host name and IP address of the logical host.

MAC

See [message authentication code \(MAC\)](#).

man-in-the-middle

A security attack characterized by the third-party, surreptitious interception of a message. The third-party, the *man-in-the-middle*, decrypts the message, re-encrypts it (with or without alteration of the original message), and retransmits it to the originally-intended recipient—all without the knowledge of the legitimate sender and receiver. This type of security attack works only in the absence of [authentication](#).

mapping rules file

In an Oracle Directory Integration Platform environment, the file that specifies mappings between Oracle Internet Directory attributes and those in a [connected directory](#).

master definition site (MDS)

In replication, a master definition site is the Oracle Internet Directory database from which the administrator runs the configuration scripts.

master site

In replication, a master site is any site other than the [master definition site \(MDS\)](#) that participates in LDAP replication.

matching rule

In a search or compare operation, determines equality between the attribute value sought and the attribute value stored. For example, matching rules associated with the `telephoneNumber` attribute could cause "(650) 123-4567" to be matched with either "(650) 123-4567" or "6501234567" or both. When you create an [attribute](#), you associate a matching rule with it.

MD2

Message Digest Two (MD2) is a message digest [hash function](#). The algorithm processes input text and creates a 128-bit [message digest](#) which is unique to the message and can be used to verify data integrity. MD2 was developed by Ron Rivest for RSA Security and is intended to be used in systems with limited memory, such as smart cards.

MD4

Message Digest Four (MD4) is similar to [MD2](#) but designed specifically for fast processing in software.

MD5

Message Digest Five (MD5) is a message digest [hash function](#). The algorithm processes input text and creates a 128-bit [message digest](#) which is unique to the message and can be used to verify data integrity. MD5 was developed by Ron Rivest after potential weaknesses were reported in [MD4](#). MD5 is similar to MD4 but slower because more manipulation is made to the original data.

MDS

See [master definition site \(MDS\)](#).

message authentication

The process of verifying that a particular message came from a particular entity.

See also: [authentication](#).

message authentication code (MAC)

The Message Authentication Code (MAC) is a result of a two-step process applied to a given block of data. First, the result of a [hash function](#) is obtained. Second, that result is encrypted using a [secret key](#). The MAC can be used to authenticate the source of a given block of data.

message digest

The result of a [hash function](#).

See also: [hash](#).

metadirectory

A directory solution that shares information between all enterprise directories, integrating them into one virtual directory. It centralizes administration, thereby reducing administrative costs. It synchronizes data between directories, thereby ensuring that it is consistent and up-to-date across the enterprise.

middle tier

That portion of a OracleAS Single Sign-On instance that consists of the Oracle HTTP Server and OC4J. The OracleAS Single Sign-On middle tier is situated between the identity management infrastructure database and the client.

mod_osso

A module on the Oracle HTTP Server that enables applications protected by OracleAS Single Sign-On to accept HTTP headers in lieu of a user name and password once the user has logged into the OracleAS Single Sign-On server. The values for these headers are stored in the [mod_osso cookie](#).

mod_osso cookie

User data stored on the HTTP server. The cookie is created when a user authenticates. When the same user requests another application, the Web server uses the information in the mod_osso cookie to log the user in to the application. This feature speeds server response time.

mod_proxy

A module on the Oracle HTTP Server that makes it possible to use [mod_osso](#) to enable single sign-on to legacy, or [external applications](#).

MTS

See [shared server](#).

multimaster replication

Also called peer-to-peer or *n*-way replication, a type of replication that enables multiple sites, acting as equals, to manage groups of replicated data. In a multimaster replication environment, each node is both a supplier and a consumer node, and the entire directory is replicated on each node.

name identifier profile

A [federation](#) profile which allows a provider to inform it's peers when assigning or updating a name identifier for one of their common users.

naming attribute

The attribute used to compose the RDN of a new user entry created through Oracle Delegated Administration Services or Oracle Internet Directory Java APIs. The default value for this is `cn`.

naming context

A subtree that resides entirely on one server. It must be contiguous, that is, it must begin at an entry that serves as the top of the subtree, and extend downward to either leaf entries or [knowledge references](#) (also called referrals) to subordinate naming contexts. It can range in size from a single entry to the entire [directory information tree \(DIT\)](#).

native agent

In an Oracle Directory Integration Platform environment, an agent that runs under the control of the [directory integration and provisioning server](#). It is in contrast to an [external agent](#).

net service name

A simple name for a service that resolves to a connect descriptor. Users initiate a connect request by passing a user name and password along with a net service name in a connect string for the service to which they wish to connect, for example:

```
CONNECT username/password@net_service_name
```

Depending on your needs, net service names can be stored in a variety of places, including:

- Local configuration file, `tnsnames.ora`, on each client
- Directory server
- Oracle Names server
- External naming service, such as NDS, NIS or CDS

Net Services

See [Oracle Net Services](#).

nickname attribute

The attribute used to uniquely identify a user in the entire directory. The default value for this is `uid`. Applications use this to resolve a simple user name to the complete distinguished name. The user nickname attribute cannot be multi-valued—that is, a given user cannot have multiple nicknames stored under the same attribute name.

non-repudiation

In cryptography, the ability to prove that a given [digital signature](#) was produced with a given entity's [private key](#), and that a message was sent untampered at a given point in time.

OASIS

Organization for the Advancement of Structured Information Standards. OASIS is a worldwide not-for-profit consortium that drives the development, convergence and adoption of e-business standards.

object class

In LDAP, object classes are used to group information. Typically an object class models a real-world object such as a person or a server. Each directory entry belongs to one or more object classes. The object class determines the attributes that make up an entry. One object class can be derived from another, thereby inheriting some of the characteristics of the other class.

OC4J

See [Oracle Containers for J2EE \(OC4J\)](#).

OCA

See [Oracle Certificate Authority](#).

OCI

See [Oracle Call Interface \(OCI\)](#).

OCSP

See [Online Certificate Status Protocol \(OCSP\)](#).

OEM

See [Oracle Enterprise Manager](#).

OID

See [Oracle Internet Directory](#).

OID Control Utility

A command-line tool for issuing run-server and stop-server commands. The commands are interpreted and executed by the [OID Monitor](#) process.

OID Database Password Utility

The utility used to change the password with which Oracle Internet Directory connects to an Oracle Database.

OID Monitor

The Oracle Internet Directory component that initiates, monitors, and terminates the Oracle Internet Directory Server processes. It also controls the replication server if one is installed, and Oracle Directory Integration Platform Server.

Online Certificate Status Protocol (OCSP)

Online Certificate Status Protocol (OCSP) is one of two common schemes for checking the validity of digital certificates. The other, older method, which OCSP has superseded in some scenarios, is [certificate revocation list \(CRL\)](#). OCSP is specified in [RFC 2560](#).

one-way function

A function that is easy to compute in one direction but quite difficult to reverse compute, that is, to compute in the opposite direction.

one-way hash function

A [one-way function](#) that takes a variable sized input and creates a fixed size output.

See also: [hash function](#).

Oracle Application Server Single Sign-On

OracleAS Single Sign-On consists of program logic that enables you to log in securely to applications such as expense reports, mail, and benefits. These applications take two forms: [partner applications](#) and [external applications](#). In both cases, you gain access to several applications by authenticating only once.

Oracle Call Interface (OCI)

An application programming interface (API) that enables you to create applications that use the native procedures or function calls of a third-generation language to access an Oracle Database server and control all phases of SQL statement execution.

Oracle Certificate Authority

Oracle Application Server Certificate Authority is a [Certificate Authority \(CA\)](#) for use within your Oracle Application Server environment. OracleAS Certificate Authority uses Oracle Internet Directory as the storage repository for certificates. OracleAS Certificate Authority integration with OracleAS Single Sign-On and Oracle Internet Directory provides seamless certificate provisioning mechanisms for applications relying on them. A user provisioned in Oracle Internet Directory and authenticated in OracleAS Single Sign-On can choose to request a digital certificate from OracleAS Certificate Authority.

Oracle CMS

Oracle CMS implements the IETF [Cryptographic Message Syntax \(CMS\)](#) protocol. CMS defines data protection schemes that allow for secure message envelopes.

Oracle Containers for J2EE (OC4J)

A lightweight, scalable container for [Java 2 Platform, Enterprise Edition \(J2EE\)](#).

Oracle Context

See [identity management realm-specific Oracle Context](#) and [root Oracle Context](#).

Oracle Crypto

Oracle Crypto is a pure Java library that provides core cryptography algorithms.

Oracle Database Advanced Replication

A feature in the Oracle Database that enables database tables to be kept synchronized across two Oracle databases.

Oracle Delegated Administration Services

A set of individual, pre-defined services—called Oracle Delegated Administration Services units—for performing directory operations on behalf of a user. Oracle Internet Directory Self-Service Console makes it easier to develop and deploy administration solutions for both Oracle and third-party applications that use Oracle Internet Directory.

Oracle Directory Integration and Provisioning

A collection of interfaces and services for integrating multiple directories by using Oracle Internet Directory and several associated plug-ins and connectors. A feature of Oracle Internet Directory that enables an enterprise to use an external user repository to authenticate to Oracle products.

Oracle Directory Integration and Provisioning Server

In an Oracle Directory Integration Platform environment, a daemon process that monitors Oracle Internet Directory for change events and takes action based on the information present in the [directory integration profile](#).

Oracle Directory Integration Platform

A component of [Oracle Internet Directory](#). It is a framework developed to integrate applications around a central LDAP directory like Oracle Internet Directory.

Oracle Directory Manager

A Java-based tool with a graphical user interface for administering Oracle Internet Directory.

Oracle Enterprise Manager

A separate Oracle product that combines a graphical console, agents, common services, and tools to provide an integrated and comprehensive systems management platform for managing Oracle products.

Oracle HTTP Server

Software that processes Web transactions that use the Hypertext Transfer Protocol (HTTP). Oracle uses HTTP software developed by the Apache Group.

Oracle Identity Management

An infrastructure enabling deployments to manage centrally and securely all enterprise identities and their access to various applications in the enterprise.

Oracle Internet Directory

A general purpose directory service that enables retrieval of information about dispersed users and network resources. It combines [Lightweight Directory Access Protocol \(LDAP\)](#) Version 3 with the high performance, scalability, robustness, and availability of the Oracle Database.

Oracle Liberty SDK

Oracle Liberty SDK implements the [Liberty Alliance](#) Project specifications enabling federated single sign-on between third-party Liberty-compliant applications.

Oracle Net Services

The foundation of the Oracle family of networking products, allowing services and their client applications to reside on different computers and communicate. The main function of Oracle Net Services is to establish network sessions and transfer data between a client application and a server. Oracle Net Services is located on each computer in the network. Once a network session is established, Oracle Net Services acts as a data courier for the client and the server.

Oracle PKI certificate usages

Defines Oracle application types that a [certificate](#) supports.

Oracle PKI SDK

Oracle PKI SDK implements the security protocols that are necessary within [public key infrastructure \(PKI\)](#) implementations.

Oracle SAML

Oracle SAML provides a framework for the exchange of security credentials among disparate systems and applications in an XML-based format as outlined in the [OASIS](#) specification for the [Security Assertions Markup Language \(SAML\)](#).

Oracle Security Engine

Oracle Security Engine extends Oracle Crypto by offering X.509 based certificate management functions. Oracle Security Engine is a superset of Oracle Crypto.

Oracle S/MIME

Oracle S/MIME implements the [Secure/Multipurpose Internet Mail Extension \(S/MIME\)](#) specifications from the [Internet Engineering Task Force \(IETF\)](#) for secure e-mail.

Oracle Wallet Manager

A Java-based application that security administrators use to manage public-key security credentials on clients and servers.

See also: *Oracle Advanced Security Administrator's Guide*.

Oracle Web Services Security

Oracle Web Services Security provides a framework for authentication and authorization using existing security technologies as outlined in the [OASIS](#) specification for Web Services Security.

Oracle XML Security

Oracle XML Security implements the W3C specifications for XML Encryption and XML Signature.

OracleAS Portal

An OracleAS Single Sign-On [partner application](#) that provides a mechanism for integrating files, images, applications, and Web sites. The External Applications portlet provides access to external applications.

other information repository

In an Oracle Directory Integration Platform environment, in which Oracle Internet Directory serves as the [central directory](#), any information repository except Oracle Internet Directory.

OWM

See [Oracle Wallet Manager](#).

partition

A unique, non-overlapping directory naming context that is stored on one directory server.

partner application

An Oracle Application Server application or non-Oracle application that delegates the authentication function to the OracleAS Single Sign-On server. This type of application spares users from reauthenticating by accepting [mod_osso](#) headers.

peer-to-peer replication

Also called multimaster replication or *n*-way replication. A type of replication that enables multiple sites, acting as equals, to manage groups of replicated data. In such a

replication environment, each node is both a supplier and a consumer node, and the entire directory is replicated on each node.

PKCS#1

The Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories. PKCS#1 provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering the following aspects: cryptographic primitives; encryption schemes; signature schemes; ASN.1 syntax for representing keys and for identifying the schemes.

PKCS#5

The Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories. PKCS#5 provides recommendations for the implementation of password-based cryptography.

PKCS#7

The Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories. PKCS #7 describes general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes.

PKCS#8

The Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories. PKCS #8 describes syntax for private key information, including a private key for some public key algorithms and a set of attributes. The standard also describes syntax for encrypted private keys.

PKCS#10

The Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories. PKCS #10 describes syntax for a request for certification of a public key, a name, and possibly a set of attributes.

PKCS#12

The Public Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories. PKCS #12 describes a transfer syntax for personal identity information, including private keys, certificates, miscellaneous secrets, and extensions. Systems (such as browsers or operating systems) that support this standard allow a user to import, export, and exercise a single set of personal identity information—typically in a format called a [wallet](#).

PKI

See [public key infrastructure \(PKI\)](#).

plaintext

Plaintext is readable data prior to a transformation to ciphertext using encryption, or readable data that is the result of a transformation from ciphertext using decryption.

point-to-point replication

Also called fan-out replication is a type of replication in which a supplier replicates directly to a consumer. That consumer can then replicate to one or more other consumers. The replication can be either full or partial.

policy precedence

In Oracle Application Server Certificate Authority (OCA), policies are applied to incoming requests in the order that they are displayed on the main policy page. When

the OCA policy processor module parses policies, those that appear toward the top of the policy list are applied to requests first. Those that appear toward the bottom of the list are applied last and take precedence over the others. Only enabled policies are applied to incoming requests.

policy.properties

A multipurpose configuration file for Oracle Application Server Single Sign-On that contains basic parameters required by the single sign-on server. Also used to configure advanced features of OracleAS Single Sign-On, such as multilevel authentication.

POSIX

Portable Operating System Interface for UNIX. A set of programming interface standards governing how to write application source code so that the applications are portable between operating systems. A series of standards being developed by the [Internet Engineering Task Force \(IETF\)](#).

POST Profile

An [authentication](#) method whereby login credentials are submitted within the body of the login form.

predicates

In Oracle Application Server Certificate Authority (OCA), a policy predicate is a logical expression that can be applied to a policy to limit how it is applied to incoming certificate requests or revocations. For example, the following predicate expression specifies that the policy in which it appears can have a different effect for requests or revocations from clients with DNs that include "ou=sales,o=acme,c=us":

```
Type=="client" AND DN=="ou=sales,o=acme,c=us"
```

principal

One of the three primary roles defined in the [identity federation](#) protocols supported by OSFS. The other roles are [identity provider](#) and [service provider](#).

A principal is any entity capable of using a service and capable of acquiring a federated identity. Typically, a principal is a person or user, or a system entity whose identity can be authenticated.

primary node

In an Oracle Application Server Cold Failover Cluster (Identity Management), the cluster node on which the application runs at any given time.

See also: [secondary node](#).

private key

A private key is the secret key in a [public/private key pair](#) used in [public key cryptography](#). An entity uses its private key to decrypt data that has been encrypted with its [public key](#). The entity can also use its private key to create [digital signatures](#). The security of data encrypted with the entity's public key as well as signatures created by the private key depends on the private key remaining secret.

private key cryptography

See [symmetric cryptography](#).

profile

See [directory integration profile](#).

Project Liberty

See [Liberty Alliance](#).

provisioned applications

Applications in an environment where user and group information is centralized in Oracle Internet Directory. These applications are typically interested in changes to that information in Oracle Internet Directory.

provisioning

The process of providing users with access to applications and other resources that may be available in an enterprise environment.

provisioning agent

An application or process that translates Oracle-specific provisioning events to external or third-party application-specific events.

provisioning integration profile

A special kind of [directory integration profile](#) that describes the nature of provisioning-related notifications that Oracle Directory Integration Platform sends to the directory-enabled applications.

proxy server

A server between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfil the requests itself. If not, it forwards the request to the real server. In OracleAS Single Sign-On, proxies are used for load balancing and as an extra layer of security.

See also: [load balancer](#).

proxy user

A kind of user typically employed in an environment with a middle tier such as a firewall. In such an environment, the end user authenticates to the middle tier. The middle tier then logs into the directory on the end user's behalf. A proxy user has the privilege to switch identities and, once it has logged into the directory, switches to the end user's identity. It then performs operations on the end user's behalf, using the authorization appropriate to that particular end user.

public key

A public key is the non-secret key in a [public/private key pair](#) used in [public key cryptography](#). A public key allows entities to encrypt data that can only then be decrypted with the public key's owner using the corresponding [private key](#). A public key can also be used to verify digital signatures created with the corresponding private key.

public key certificate

See [certificate](#).

public key cryptography

Public key cryptography (also known as asymmetric cryptography) uses two keys, one public and the other private. These keys are called a key pair. The private key must be kept secret, while the public key can be transmitted to any party. The private key and the public key are mathematically related. A message that is signed by a private key can be verified by the corresponding public key. Similarly, a message encrypted by the

public key can be decrypted by the private key. This method ensures privacy because only the owner of the private key can decrypt the message.

public key encryption

The process in which the sender of a message encrypts the message with the public key of the recipient. Upon delivery, the message is decrypted by the recipient using the recipient's private key.

public key infrastructure (PKI)

A public key infrastructure (PKI) is a system that manages the issuing, distribution, and authentication of **public keys** and **private keys**. A PKI typically comprises the following components:

- A **Certificate Authority (CA)** that is responsible for generating, issuing, publishing and revoking digital certificates.
- A **Registration Authority (RA)** that is responsible for verifying the information supplied in requests for certificates made to the CA.
- A directory service where a **certificate** or **certificate revocation list (CRL)** gets published by the CA and where they can be retrieved by relying third parties.
- Relying third parties that use the certificates issued by the CA and the **public keys** contained therein to verify **digital signatures** and encrypt data.

public/private key pair

A mathematically related set of two numbers where one is called the private key and the other is called the public key. Public keys are typically made widely available, while private keys are available only to their owners. Data encrypted with a public key can only be decrypted with its associated private key and vice versa. Data encrypted with a public key cannot be decrypted with the same public key.

RC2

Rivest Cipher Two (RC2) is a 64-bit **block cipher** developed by Ronald Rivest for RSA Security, and was designed as a replacement for **Data Encryption Standard (DES)**.

RC4

Rivest Cipher Four (RC4) is a **stream cipher** developed by Ronald Rivest for RSA Security. RC4 allows variable key lengths up to 1024 bits. RC4 is most commonly used to secure data communications by encrypting traffic between Web sites that use the **Secure Sockets Layer (SSL)** protocol.

RDN

See **relative distinguished name (RDN)**.

readable data

Data prior to a transformation to ciphertext using encryption or data that is the result of a transformation from ciphertext using decryption.

realm

See **identity management realm**.

realm search base

An attribute in the **root Oracle Context** that identifies the entry in the **directory information tree (DIT)** that contains all **identity management realms**. This attribute is used when mapping a simple realm name to the corresponding entry in the directory.

referral

Information that a directory server provides to a client and which points to other servers the client must contact to find the information it is requesting.

See also: [knowledge reference](#).

Registration Authority (RA)

The Registration Authority (RA) is responsible for verifying and enrolling users before a certificate is issued by a [Certificate Authority \(CA\)](#). The RA may assign each applicant a relative distinguished value or name for the new certificate applied. The RA does not sign or issue certificates.

registry entry

An entry containing runtime information associated with invocations of Oracle Internet Directory servers, called a [directory server instance](#). Registry entries are stored in the directory itself, and remain there until the corresponding directory server instance stops.

relational database

A structured collection of data that stores data in tables consisting of one or more rows, each containing the same set of columns. Oracle makes it very easy to link the data in multiple tables. This is what makes Oracle a relational database management system, or RDBMS. It stores data in two or more tables and enables you to define relationships between the tables. The link is based on one or more fields common to both tables.

relative distinguished name (RDN)

The local, most granular level entry name. It has no other qualifying entry names that would serve to uniquely address the entry. In the example, `cn=Smith, o=acme, c=US`, the RDN is `cn=Smith`.

remote master site (RMS)

In a replicated environment, any site, other than the [master definition site \(MDS\)](#), that participates in [Oracle Database Advanced Replication](#).

replica

Each copy of a [naming context](#) that is contained within a single server.

replication agreement

A special directory entry that represents the replication relationship among the directory servers in a [directory replication group \(DRG\)](#).

response time

The time between the submission of a request and the completion of the response.

RFC

The Internet Request For Comments (or RFC) documents are the written definitions of the protocols and policies of the Internet. The Internet Engineering Task Force (IETF) facilitates the discussion, development, and establishment of new standards. A standard is published using the RFC acronym and a reference number. For example, the official standard for e-mail is RFC 822.

root CA

In a hierarchical [public key infrastructure \(PKI\)](#), the root [Certificate Authority \(CA\)](#) is the CA whose [public key](#) serves as the most trusted datum for a security domain.

root directory specific entry (DSE)

An entry storing operational information about the directory. The information is stored in a number of attributes.

root DSE

See [root directory specific entry \(DSE\)](#).

root Oracle Context

In the Oracle Identity Management infrastructure, the root Oracle Context is an entry in Oracle Internet Directory containing a pointer to the default identity management realm in the infrastructure. It also contains information on how to locate an identity management realm given a simple name of the realm.

RSA

RSA is a [public key cryptography](#) algorithm named after its inventors (Rivest, Shamir, and Adelman). The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Netscape and Microsoft, and many other products.

RSAES-OAEP

The RSA Encryption Scheme - Optimal Asymmetric Encryption Padding (RSAES-OAEP) is a public key encryption scheme combining the [RSA](#) algorithm with the OAEP method. Optimal Asymmetric Encryption Padding (OAEP) is a method for encoding messages developed by Mihir Bellare and Phil Rogaway.

S/MIME

See [Secure/Multipurpose Internet Mail Extension \(S/MIME\)](#).

SAML

See [Security Assertions Markup Language \(SAML\)](#).

SASL

See [Simple Authentication and Security Layer \(SASL\)](#).

scalability

The ability of a system to provide throughput in proportion to, and limited only by, available hardware resources.

schema

The collection of [attributes](#), [object classes](#), and their corresponding [matching rules](#).

secondary node

In an Oracle Application Server Cold Failover Cluster (Identity Management), the cluster node to which an application is moved during a failover.

See also: [primary node](#).

secret key

A secret key is the **key** used in a **symmetric algorithm**. Since a secret key is used for both encryption and decryption, it must be shared between parties that are transmitting ciphertext to one another but must be kept secret from all unauthorized entities.

secret key cryptography

See **symmetric cryptography**.

Secure Hash Algorithm (SHA)

Secure Hash Algorithm (SHA) is a **hash function** algorithm that produces a 160-bit **message digest** based upon the input. The algorithm is used in the Digital Signature Standard (DSS). With the introduction of the Advanced Encryption Standard (AES) which offers three key sizes: 128, 192 and 256 bits, there has been a need for a companion hash algorithm with a similar level of security. The newer SHA-256, SHA-284 and SHA-512 hash algorithms comply with these enhanced requirements.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is a protocol designed by Netscape Communications to enable encrypted, authenticated communications across networks (such as the Internet). SSL uses the **public key encryption** system from RSA, which also includes the use of a digital certificate. SSL provides three elements of secure communications: **confidentiality**, **authentication**, and **integrity**.

SSL has evolved into **Transport Layer Security (TLS)**. TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL.

Secure/Multipurpose Internet Mail Extension (S/MIME)

Secure/Multipurpose Internet Mail Extension (S/MIME) is an Internet Engineering Task Force (IETF) standard for securing MIME data through the use of **digital signatures** and **encryption**.

Security Assertions Markup Language (SAML)

An **XML**-based framework which defines mechanisms for exchanging security information about a subject by making assertions about the subject that are used to make access control decisions. SAML enables the exchange of **authentication** and **authorization** information between identity providers and service providers who otherwise may not be able to interoperate.

SAML 2.0 is a major revision of the standard which updates SAML 1.1 and combines input from both Shibboleth and **Liberty ID-FF** specifications. A key aspect of SAML 2.0 is the ability for two sites to establish and maintain an identifier for a user, with that user's cooperation. Additional features include privacy mechanisms and support for global logout.

security token

In the Liberty protocol, refers to a set of security information that represents and substantiates a claim.

server certificate

A **certificate** that attests to the identity of an organization that uses a secure Web server to serve data. A server certificate must be associated with a **public/private key pair** issued by a mutually trusted **Certificate Authority (CA)**. Server certificates are required for secure communications between a browser and a Web server.

service provider

One of the three primary roles defined in the [identity federation](#) protocols supported by OSFS. The other roles are [identity provider](#) and [principal](#).

A service provider, which is the relying party in SAML, provides services or goods to a principal while relying on an identity provider to authenticate the principal's identity.

service time

The time between the initiation of a request and the completion of the response to the request.

session key

A [secret key](#) that is used for the duration of one message or communication session.

SGA

See [System Global Area \(SGA\)](#).

SHA

See [Secure Hash Algorithm \(SHA\)](#).

shared server

A server that is configured to allow many user processes to share very few server processes, so the number of users that can be supported is increased. With shared server configuration, many user processes connect to a dispatcher. The dispatcher directs multiple incoming network session requests to a common queue. An idle shared server process from a shared pool of server processes picks up a request from the queue. This means a small pool of server processes can server a large amount of clients. Contrast with dedicated server.

sibling

An entry that has the same parent as one or more other entries.

Signed Public Key And Challenge (SPKAC)

Signed Public Key And Challenge (SPKAC) is a proprietary protocol used by the Netscape Navigator browser to request certificates.

simple authentication

The process by which the client identifies itself to the server by means of a DN and a password which are not encrypted when sent over the network. In the simple authentication option, the server verifies that the DN and password sent by the client match the DN and password stored in the directory.

Simple Authentication and Security Layer (SASL)

Simple Authentication and Security Layer (SASL) is a method for adding [authentication](#) and [authorization](#) capabilities to application protocols. SASL provides a security layer between the protocol and the connection, so that users can be authenticated to a server. A security layer can also be negotiated to protect subsequent protocol interactions.

Simple Object Access Protocol (SOAP)

Simple Object Access Protocol (SOAP) is an [XML](#)-based protocol that defines a framework for exchanging messages between systems over the Internet. A common protocol for Web Services, SOAP is used with transport protocols such as HTTP and FTP. A SOAP message consists of three parts — an envelope that describes the

message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses.

single key-pair wallet

A **PKCS#12**-format wallet that contains a single user **certificate** and its associated **private key**. The **public key** is imbedded in the certificate.

single sign-off

The process by which you terminate an OracleAS Single Sign-On session and log out of all active partner applications simultaneously. You can do this by logging out of the application that you are working in.

single sign-on (SSO)

In a federated environment, single sign-on enables users to sign on once with a member of a federated group of identity providers and service providers, and later use resources available from members without needing to sign on again.

single sign-on SDK

Legacy APIs to enable OracleAS Single Sign-On partner applications for single sign-on. The SDK consists of PL/SQL and Java APIs as well as sample code that demonstrates how these APIs are implemented. This SDK is now deprecated and **mod_osso** is used instead.

single sign-on server

Program logic that enables users to log in securely to single sign-on applications such as expense reports, mail, and benefits.

SLAPD

Standalone LDAP daemon. An LDAP directory server service that is responsible for most functions of a directory except replication.

slave

See **consumer**.

smart knowledge reference

A **knowledge reference** that is returned when the knowledge reference entry is in the scope of the search. It points the user to the server that stores the requested information.

SOAP

See **Simple Object Access Protocol (SOAP)**.

specific administrative area

Administrative areas control:

- Subschema administration
- Access control administration
- Collective attribute administration

A *specific* administrative area controls one of these aspects of administration. A specific administrative area is part of an autonomous administrative area.

SPKAC

See [Signed Public Key And Challenge \(SPKAC\)](#).

sponsor node

In replication, the node that is used to provide initial data to a new node.

SSL

See [Secure Sockets Layer \(SSL\)](#).

SSO

See [single sign-on \(SSO\)](#).

stream cipher

Stream ciphers are a type of [symmetric algorithm](#). A stream cipher encrypts in small units, often a bit or a byte at a time, and implements some form of feedback mechanism so that the key is constantly changing. [RC4](#) is an example of a stream cipher.

See also: [block cipher](#).

subACLSubentry

A specific type of [subentry](#) that contains [access control list \(ACL\)](#) information.

subclass

An object class derived from another object class. The object class from which it is derived is called its [superclass](#).

subentry

A type of entry containing information applicable to a group of entries in a subtree. The information can be of these types:

- Access control policy points
- Schema rules
- Collective attributes

Subentries are located immediately below the root of an administrative area.

subordinate CA

In a hierarchical [public key infrastructure \(PKI\)](#), the subordinate [Certificate Authority \(CA\)](#) is a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.

subordinate reference

A [knowledge reference](#) pointing downward in the [directory information tree \(DIT\)](#) to a [naming context](#) that starts immediately below an entry

subschem DN

The list of [directory information tree \(DIT\)](#) areas having independent [schema](#) definitions.

subSchemaSubentry

A specific type of [subentry](#) containing [schema](#) information.

subtree

A section of a directory hierarchy, which is also called a **directory information tree (DIT)**. The subtree typically starts at a particular directory node and includes all subdirectories and objects below that node in the directory hierarchy.

subtype

An attribute with one or more options, in contrast to that same attribute without the options. For example, a `commonName (cn)` attribute with American English as an option is a subtype of the `commonName (cn)` attribute without that option. Conversely, the `commonName (cn)` attribute without an option is the **supertype** of the same attribute with an option.

success URL

When using Oracle Application Server Single Sign-On, the URL to the routine responsible for establishing the session and session cookies for an application.

super user

A special directory administrator who typically has full access to directory information.

superclass

The **object class** from which another object class is derived. For example, the object class `person` is the superclass of the object class `organizationalPerson`. The latter, namely, `organizationalPerson`, is a **subclass** of `person` and inherits the attributes contained in `person`.

superior reference

A **knowledge reference** pointing upward to a **directory system agent (DSA)** that holds a naming context higher in the **directory information tree (DIT)** than all the naming contexts held by the referencing DSA.

supertype

An attribute without options, in contrast to the same attribute with one or more options. For example, the `commonName (cn)` attribute without an option is the supertype of the same attribute with an option. Conversely, a `commonName (cn)` attribute with American English as an option is a **subtype** of the `commonName (cn)` attribute without that option.

supplier

In replication, the server that holds the master copy of the **naming context**. It supplies updates from the master copy to the **consumer** server.

symmetric algorithm

A symmetric algorithm is a cryptographic algorithm that uses the same key for encryption and decryption. There are essentially two types of symmetric (or secret key) algorithms — **stream ciphers** and **block ciphers**.

symmetric cryptography

Symmetric cryptography (or shared secret cryptography) systems use the same key to encipher and decipher data. The problem with symmetric cryptography is ensuring a secure method by which the sender and recipient can agree on the secret key. If a third party were to intercept the secret key in transit, they could then use it to decipher anything it was used to encipher. Symmetric cryptography is usually faster than

asymmetric cryptography, and is often used when large quantities of data need to be exchanged. [DES](#), [RC2](#), and [RC4](#) are examples of symmetric cryptography algorithms.

symmetric key

See [secret key](#).

System Global Area (SGA)

A group of shared memory structures that contain data and control information for one Oracle database instance. If multiple users are concurrently connected to the same instance, the data in the instance SGA is shared among the users. Consequently, the SGA is sometimes referred to as the "shared global area." The combination of the background processes and memory buffers is called an Oracle instance.

system operational attribute

An attribute holding information that pertains to the operation of the directory itself. Some operational information is specified by the directory to control the server, for example, the time stamp for an entry. Other operational information, such as access information, is defined by administrators and is used by the directory program in its processing.

think time

The time the user is not engaged in actual use of the processor.

third-party access management system

Non-Oracle single sign-on system that can be modified to use OracleAS Single Sign-On to gain access to Oracle Application Server applications.

throughput

The number of requests processed by Oracle Internet Directory for each unit of time. This is typically represented as "operations per second."

Time Stamp Protocol (TSP)

Time Stamp Protocol (TSP), as specified in RFC 3161, defines the participating entities, the message formats, and the transport protocol involved in time stamping a digital message. In a TSP system, a trusted third-party Time Stamp Authority (TSA) issues time stamps for messages.

TLS

See [Transport Layer Security \(TLS\)](#).

Transport Layer Security (TLS)

A protocol providing communications privacy over the Internet. The protocol enables client/server applications to communicate in a way that prevents eavesdropping, tampering, or message forgery.

Triple Data Encryption Standard (3DES)

Triple Data Encryption Standard (3DES) is based on the [Data Encryption Standard \(DES\)](#) algorithm developed by IBM in 1974, and was adopted as a national standard in 1977. 3DES uses three 64-bit long keys (overall key length is 192 bits, although actual key length is 56 bits). Data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key. This makes 3DES three times slower than standard DES but also three times more secure.

trusted certificate

A third party identity that is qualified with a level of trust. The trust is used when an identity is being validated as the entity it claims to be. Typically, trusted certificates come from a [Certificate Authority \(CA\)](#) you trust to issue user certificates.

trustpoint

See [trusted certificate](#).

TSP

See [Time Stamp Protocol \(TSP\)](#).

Unicode

A type of universal character set, a collection of 64K characters encoded in a 16-bit space. It encodes nearly every character in just about every existing character set standard, covering most written scripts used in the world. It is owned and defined by Unicode Inc. Unicode is canonical encoding which means its value can be passed around in different locales. But it does not guarantee a round-trip conversion between it and every Oracle character set without information loss.

UNIX Crypt

The UNIX encryption algorithm.

URI

Uniform Resource Identifier (URI). A way to identify any point of content on the Web, whether it be a page of text, a video or sound clip, a still or animated image, or a program. The most common form of URI is the Web page address, which is a particular form or subset of URI called a [URL](#).

URL

Uniform Resource Locator (URL). The address of a file accessible on the Internet. The file can be a text file, HTML page, image file, a program, or any other file supported by HTTP. The URL contains the name of the protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of the file location on the computer.

URLC token

The OracleAS Single Sign-On code that passes authenticated user information to the [partner application](#). The partner application uses this information to construct the session cookie.

user name mapping module

A OracleAS Single Sign-On Java module that maps a user [certificate](#) to the user's nickname. The nickname is then passed to an authentication module, which uses this nickname to retrieve the user's certificate from the directory.

user search base

In the Oracle Internet Directory default [directory information tree \(DIT\)](#), the node in the identity management realm under which all the users are placed.

UTC (Coordinated Universal Time)

The standard time common to every place in the world. Formerly and still widely called Greenwich Mean Time (GMT) and also World Time, UTC nominally reflects the

mean solar time along the Earth's prime meridian. UTC is indicated by a z at the end of the value, for example, 200011281010z.

UTF-8

A variable-width 8-bit encoding of **Unicode** that uses sequences of 1, 2, 3, or 4 bytes for each character. Characters from 0-127 (the 7-bit ASCII characters) are encoded with one byte, characters from 128-2047 require two bytes, characters from 2048-65535 require three bytes, and characters beyond 65535 require four bytes. The Oracle character set name for this is AL32UTF8 (for the Unicode 3.1 standard).

UTF-16

16-bit encoding of **Unicode**. The Latin-1 characters are the first 256 code points in this standard.

verification

Verification is the process of ensuring that a given **digital signature** is valid, given the **public key** that corresponds to the **private key** purported to create the signature and the data block to which the signature purportedly applies.

virtual host

A single physical Web server machine that is hosting one or more Web sites or domains, or a server that is acting as a proxy to other machines (accepts incoming requests and reroutes them to the appropriate server).

In the case of OracleAS Single Sign-On, virtual hosts are used for load balancing between two or more OracleAS Single Sign-On servers. They also provide an extra layer of security.

virtual host name

In an Oracle Application Server Cold Failover Cluster (Identity Management), the host name corresponding to a particular virtual IP address.

virtual IP address

In an Oracle Application Server Cold Failover Cluster (Identity Management), each physical node has its own physical IP address and physical host name. To present a single system image to the outside world, the cluster uses a dynamic IP address that can be moved to any physical node in the cluster. This is called the virtual IP address.

wait time

The time between the submission of the request and initiation of the response.

wallet

An abstraction used to store and manage security credentials for an individual entity. It implements the storage and retrieval of credentials for use with various cryptographic services. A wallet resource locator (WRL) provides all the necessary information to locate the wallet.

Wallet Manager

See [Oracle Wallet Manager](#).

Web service

A Web service is application or business logic that is accessible using standard Internet protocols, such as **HTTP**, **XML**, and **SOAP**. Web Services combine the best aspects of component-based development and the World Wide Web. Like components, Web

Services represent black-box functionality that can be used and reused without regard to how the service is implemented.

Web Services Description Language (WSDL)

Web Services Description Language (WSDL) is the standard format for describing a Web service using [XML](#). A WSDL definition describes how to access a Web service and what operations it will perform.

WSDL

See [Web Services Description Language \(WSDL\)](#).

WS-Federation

Web Services Federation Language (WS-Federation) is a specification developed by Microsoft, IBM, BEA, VeriSign, and RSA Security. It defines mechanisms to allow [federation](#) between entities using different or like mechanisms by allowing and brokering trust of identities, attributes, and authentication between participating [Web services](#).

See also: [Liberty Alliance](#).

X.500

X.500 is a standard from the International Telecommunication Union (ITU) that defines how global directories should be structured. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city.

X.509

X.509 is the most widely used standard for defining digital certificates. A standard from the International Telecommunication Union (ITU), for hierarchical directories with authentication services, used in many [public key infrastructure \(PKI\)](#) implementations.

XML

Extensible Markup Language (XML) is a specification developed by the World Wide Web Consortium (W3C). XML is a pared-down version of Standard Generalized Mark-Up Language (SGML), designed especially for Web documents. XML is a metalanguage (a way to define tag sets) that allows developers to define their own customized markup language for many classes of documents.

XML canonicalization (C14N)

This is a process by which two logically equivalent XML documents can be resolved to the same physical representation. This has significance for digital signatures because a signature can only verify against the same physical representation of the data against which it was originally computed. For more information, see the W3C's XML Canonicalization specification.

Index

A

account lockout, 3-3
addsub.csh script, 10-5
Administer External Applications page, 5-1 to 5-4
administration pages
 accessing, 2-8
 debugging, A-18
 external applications, 5-1
application service providers, 10-1
authentication adapters. See authentication plugins
authentication dynamics
 certificate-enabled sign-on, 8-1, 8-2
 identity management realms, 10-3, 10-4
 third-party access management, 13-1, 14-1, 14-3
authentication levels, 6-2, 6-3
authentication plugins, 6-3

B

backup and recovery, 9-10
basic authentication method, 5-2, 5-6
browser settings
 standard, 2-7

C

certificate revocation lists, 8-7
certificate-enabled sign-on
 authentication dynamics, 8-1, 8-2
 configuring
 Oracle HTTP Server, 8-2, 8-3
 Oracle Internet Directory, 8-6, 8-7
 single sign-on server, 8-3 to 8-6
 user name mapping module, 8-4, 8-6
 CRL maintenance, 8-7
 error messages, A-11
 sample files, 2-12
change password page
 behavior, 3-2
 error messages, 12-9
 installing, 12-12
 overview, 1-6
 parameters, 12-5
configuration files
 httpd.conf, 4-7, 9-5, A-9

osso.conf, 4-8, 9-7
policy.properties, 6-2 to 6-4, 8-4, A-16
ssl.conf, 8-2, 8-3
targets.xml, 11-4
x509CertAuth.properties, 8-4, 8-6

D

debugging
 administration pages, A-18
 PL/SQL pages, A-18
deployment scenarios
 geographically distributed instances, 9-8
 multilevel authentication, 6-4
 multiple middle tiers, 9-3
 partner applications, 4-5
deployment-specific pages
 examples, 12-13
 globalization support, 12-10
 guidelines, 12-11
 sample files, 2-12
 support for OracleAS Wireless, 12-12
Details of Login Failures page, 11-3
directory access
 configuring, 3-5
 scripts, 3-5
directory entries, for OracleAS Single Sign-On, 3-3, 3-4
disaster recovery, 9-10
Distributed Cluster Management, 4-8, 9-6

E

Edit SSO Server page, 2-9
enblhstg.csh script, 10-5
error messages
 basic, A-6
 certificate-enabled sign-on, A-11
 export and import, 15-5 to 15-7
export and import
 error messages, 15-5 to 15-7
 scenarios, 15-3
 scripts, 15-4
External applications
 login pages, 12-12
external applications

- access using mod_osso/mod_proxy, 5-5 to 5-7
- adding, 5-1 to 5-4
- administration pages, 5-1
- authentication dynamics, 1-5, 1-6
- authentication methods
 - basic, 5-2, 5-6
 - GET, 5-2
 - POST, 5-2
- editing, 5-4
- login, 5-4, 5-5
- overview, 1-2

External Applications portlet, 5-5

F

- features
 - new, xv
- force change password feature, 3-3

G

- GET authentication method, 5-2, A-20
- global user inactivity timeout, A-20
 - configuring, 2-10, 2-11
 - overview, 1-7
 - scripts, 2-10
- globalization support
 - deployment-specific pages, 12-10
 - standard pages, 2-9
- grace login, 3-3

H

- high server availability
 - configuring, 9-10
 - deployment options
 - geographically distributed instances, 9-8 to 9-10
 - multiple middle tiers, 9-2 to 9-8
 - replicated directory, 9-8
- http
 - //metalink.oracle.com, A-20
- httpd.conf file, 4-7, 4-10, 9-5, A-9

I

- iASAdmins administration group, 2-2
- identity management infrastructure database
 - configuring for SSL, 7-3
 - replicating, 9-11 to 9-13
 - support for multiple realms, 10-1
- identity management realms
 - administrative privileges, 10-6
 - authentication dynamics, 10-3, 10-4
 - benefits, 10-1
 - configuring, 10-4 to 10-6
 - overhead, 10-1
 - overview, 10-1
 - support for partner applications, 10-3
- IP checking, 2-9

L

- LDAP command-line tools, 3-1
- LDAP connection timeout
 - configuring, A-8
- load balancers
 - OracleAS Web Cache, 9-6
 - with multiple partner applications, 4-5, 4-7
 - with multiple single sign-on middle tiers, 9-2, 9-4, 9-6
- login page
 - error messages, 12-7, 12-8, 12-9
 - installing, 12-12
 - parameters, 12-3
 - password reset feature, 12-4
- login pages
 - for external applications, 12-12
- login scenarios
 - third-party access, 14-2

M

- mod_osso
 - compared with single sign-on SDK, 1-2
 - overview, 1-2
 - registering, 4-1
 - reregistering, 4-8, 9-6, 9-7, 9-15
- mod_osso.conf file, 2-11, 4-9
- monitoring
 - access the monitoring console, 11-1
 - changing the port number of the HTTP server, 11-4
 - from OracleAS Web Cache, 11-5
 - home page, 11-2
 - interpreting the data, 11-2, 11-3
 - login failures page, 11-3
 - ports, 11-4
 - setting the database password for, 11-1
 - SSL-enabled Single Sign-On Server, 11-5
- monitoring home page, 11-2
- monitoring pages
 - accessing, 11-1
 - ports, 11-4
- multilevel authentication
 - authentication levels, 6-2, 6-3
 - configuring, 6-4
 - flow, 6-1
 - plugins, 6-3
- multimaster replication, 9-11

O

- oidprovtool, 9-16
- Oracle Delegated Administration Services, 1-6, 3-1
- Oracle Directory Manager, 2-3, 3-1
- Oracle HTTP Server
 - configuring
 - certificate-enabled sign-on, 8-2, 8-3
 - partner application middle tier, 4-6
 - single sign-on middle tier, 9-5, 9-6
 - SSL configuration, 7-3

- starting and stopping, 2-5
- Oracle Internet Directory
 - configuring for certificate-enabled sign-on, 8-6, 8-7
 - configuring for SSL, 7-5
 - role in third-party access management, 14-3
 - synchronization with Microsoft Active Directory, 14-3
- OracleAS Certificate Authority, 8-3
- OracleAS Cold Failover Cluster, 9-10
- OracleAS Discoverer, 15-1, 15-3, 15-4
- OracleAS Portal
 - External Applications portlet, 5-5
 - registering, 4-1
- OracleAS Single Sign-On
 - administrative pages, 1-3
 - administrators, 2-1 to 2-3
 - benefits, 1-1
 - browser preferences, 2-7, 2-8
 - configuring directory access, 3-5
 - directory information tree, 3-3, 3-4
 - external applications, 5-1 to 5-4
 - globalization support, 2-9, 12-10
 - home page, 1-3
 - nondefault configuration, 9-1
 - password policies, 3-2, 3-3
 - passwords, 1-6
 - sample files, 2-12
 - scripts
 - addsub.csh, 10-5
 - enblhstg.csh, 10-5
 - ssocfg, 9-6, 9-14
 - ssogito.sql, 2-10
 - ssomig, 15-1
 - ssooconf.sql, 3-5, A-3, A-6
 - ssoreoid.sql, 3-6, A-6, A-20
 - timeouts, 1-7
 - user accounts, 3-1
 - user attributes, 1-2
- OracleAS Web Cache, 4-7, 9-6
 - use in monitoring, 11-5
- OracleAS Wireless, 1-7
- osso.conf file, 4-8, 9-7

P

- partner applications
 - configuring for high availability, 4-5
 - deploying, 4-5
 - examples of, 1-2
 - overview, 1-2
 - registering, 4-1
 - reregistering, 4-8, 7-6, 9-6, 9-7
- password policies, 3-2, 3-3
- passwords
 - changing, 1-6, 3-2
 - configuring, 3-3
 - expiry, 3-2
 - external applications, 1-2
 - force change password feature, 3-3

- management, 3-2
- resetting, 1-6, 3-2, 12-4
- rules, 3-2
- schema, 3-6, B-1
- policy.properties file
 - in certificate-enabled sign-on, 8-4
 - in debugging, A-16
 - in multilevel authentication, 6-2 to 6-4
 - in third-party access management, 14-12
- ports
 - changes in HTTP Server port number, 11-4
- POST authentication method, 5-2, A-20
- proxy authentication, 5-5 to 5-7
- proxy server
 - configuring, 9-14, 9-15
 - function, 9-14

R

- refresh script, 3-6
- Remember My Login Information For This
 - Application check box, 5-4
- reverse proxy, 9-13 to 9-15

S

- sample files
 - certificate-enabled sign-on, 2-12
 - deployment-specific pages, 2-12
- scripts
 - ssogito.sql, 2-10
 - ssomig, 15-1, 15-2
 - ssooconf.sql, 3-5
 - ssoreg, 4-1, 4-2, 4-4, 9-15
 - ssoreoid.sql, 3-6
- server cache, 3-6
- sign-off page
 - installing, 12-12
- single sign-off page
 - installing, 12-12
 - parameters, 12-5, 12-6
- single sign-on administrators
 - assigning privileges to, 2-2
 - creating a new group for, 2-3
 - duties, 2-1
- single sign-on server
 - accessing, 1-3
 - cache, 3-6
 - configuring directory access, 3-5
 - deployment options
 - geographically distributed instances, 9-8 to 9-10
 - multiple middle tiers, 9-2, 9-8
 - replicated directory, 9-8
 - overview, 1-1
 - role in third-party access management, 14-1
 - starting and stopping, 2-5
 - with reverse proxy, 9-13
- single sign-on session timeout, 2-9
- SSL (Secure Sockets Layer), 7-2 to 7-6

- ssl.conf file, 4-9, 4-10, 8-2, 8-3
- SSO Server Administration page, 2-9
- ssocfg script, 9-6, 9-14
- ssogito.sql script, 2-10
- ssomig script
 - executing, 15-4
 - parameters, 15-2, 15-3
 - syntax, 15-1
- ssomig.log file, 15-5
- ssooconf.sql script, 3-5, A-3, A-6
- ssoreg script
 - example, 4-4
 - purpose, 4-1
 - syntax, 4-2
 - usage, 9-15
- ssoreoid.sql script, 3-6, A-6, A-20
- ssoreplsetup.jar tool, 9-12
- synchronization
 - between directory and single sign-on server, 9-15, 9-16
 - between third-party directory and Oracle Internet Directory, 14-3

T

- targets.xml file, 11-4
- third-party access management
 - authentication dynamics, 13-1, 14-1, 14-3
 - code example, 14-12, 14-13
 - logout, 14-10, 14-11
 - migration, 14-13 to 14-15
- timeouts
 - global user inactivity timeout, 1-7, 2-10, 2-11
 - LDAP connections, A-8
 - single sign-on session timeout, 2-9

U

- URLs, configuring for SSL, 7-5
- URLs, protecting, 7-3 to 7-5, 9-6
- user accounts
 - lockout, 3-3
 - management, 3-1
- user management tools, 3-1
- user name mapping module, 8-4
 - custom implementation, 8-5, 8-6
 - default implementation, 8-4

V

- virtual hosts, 4-9, 4-10, 9-14

W

- Web Cache
 - use in monitoring, 11-5
- what's new in this release, xv
 - working with OracleAS SSO, xvi

X

- X509CertAuth.properties file, 8-4, 8-6