

Oracle® Application Server

Release Notes

10g (10.1.4.0.1) for AIX 5L Based Systems (64-Bit)

B32104-02

December 2006

Copyright © 2006, Oracle. All rights reserved.

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 | ix |
| Audience | ix |
| Documentation Accessibility | ix |
| Related Documents | x |
| Conventions | x |
| | |
| What's New in the <i>Oracle Application Server Release Notes</i>? | xi |
| Chapter 2, "Installation and Upgrade Issues" | xi |
| Chapter 5, "Oracle Access Manager" | xi |
| Chapter 6, "Oracle Application Server Single Sign-On" | xii |
| Chapter 7, "Oracle Identity Federation" | xii |
| Chapter 9, "Oracle Internet Directory" | xii |
| | |
| 1 Introduction | |
| 1.1 Latest Release Information | 1-1 |
| 1.2 Purpose of this Document | 1-1 |
| 1.3 Operating System Requirements | 1-1 |
| 1.4 Multiple Versions of Identity Management in this Release..... | 1-2 |
| 1.5 Certification Information | 1-2 |
| 1.6 Licensing Information | 1-2 |
| | |
| 2 Installation and Upgrade Issues | |
| 2.1 Installation Issues..... | 2-1 |
| 2.1.1 Unique Global Database Name Required During Installation | 2-2 |
| 2.1.2 Do Not Use Turkish Locale During Installation | 2-2 |
| 2.1.3 Oracle Application Server Repository Creation Assistant Fails During Loading When the Database Uses Certain Chinese Character Sets | 2-2 |
| 2.1.4 OracleAS Cold Failover Cluster: Additional Configuration Steps for Oracle Delegated Administration Services..... | 2-2 |
| 2.1.5 Oracle Internet Directory SSL Connection Fail Intermittently..... | 2-3 |
| 2.1.6 Incorrect Location for Debug Message | 2-3 |
| 2.1.7 Illegible or Garbage Characters Output in a Russian Locale | 2-3 |
| 2.1.8 Application Server Control Console Link Not Operational in non-English Installations | 2-3 |
| 2.1.9 Set the NLS Parameter Before Installing | 2-3 |

| | | |
|--------|--|------|
| 2.1.10 | Excessive Privileges for OracleAS Metadata Repository Installations | 2-4 |
| 2.1.11 | Incorrect Guidelines for Online Help | 2-5 |
| 2.1.12 | OID Configuration Assistant Fails While Installing Oracle Application Server in Japanese Locale | 2-5 |
| 2.1.13 | OIDCA Fails Due to Misconfigure in /ECT/HOSTS..... | 2-5 |
| 2.1.14 | DB Console of Infrastructure IM+MR Cannot be Started..... | 2-5 |
| 2.2 | Upgrade Issues | 2-6 |
| 2.2.1 | Upgrade of Identity Management Installation to 10.1.4.0.1 | 2-6 |
| 2.2.2 | Additional Step Required When Upgrading OracleAS Metadata Repository Release 9.0.4.3 to 10.1.4.0.1 | 2-7 |
| 2.2.3 | Configuring Port Values for the Load Balancer and Oracle Internet Directory When Upgrading Oracle Application Server Cluster (Identity Management) | 2-8 |
| 2.2.4 | Harmless Error Messages During OracleAS Metadata Repository Upgrade..... | 2-9 |
| 2.2.5 | Metadata Repository Container Version..... | 2-10 |
| 2.2.6 | Issues When Using the Idifwrite Command to Back Up the Oracle Internet Directory | 2-10 |
| 2.2.7 | Upgrade of OracleAS Cold Failover Clusters Fails While Running Configuration Assistant | 2-10 |
| 2.3 | Documentation Errata | 2-11 |
| 2.3.1 | Incorrect Line Breaks in MRUA Sample Output | 2-11 |
| 2.3.2 | Incorrect Global Database Naming Standard..... | 2-11 |

3 General Management and Security Issues

| | | |
|-------|---|-----|
| 3.1 | General Management Issues | 3-1 |
| 3.1.1 | Modifying targets.xml After Enabling SSL for Oracle Identity Management 10g (10.1.4.0.1) | 3-1 |
| 3.1.2 | Changing the IP Address of a Metadata Repository Created with Oracle Application Server Repository Creation Assistant | 3-2 |
| 3.1.3 | Oracle Enterprise Manager Grid Control Does not Display all Integration Profiles. | 3-3 |
| 3.1.4 | Additional Information for Changing Hostname for Identity Management Installations | 3-3 |
| 3.2 | Documentation Errata | 3-4 |
| 3.2.1 | References to OracleAS Web Cache and OracleAS Portal in the Application Server Control Console Online Help..... | 3-4 |

4 High Availability

| | | |
|-------|--|-----|
| 4.1 | General Issues and Workarounds | 4-1 |
| 4.1.1 | Problem Performing a Clone Instance or Clone Topology Operation..... | 4-1 |
| 4.1.2 | OracleAS Guard Release 10.1.2.1.1 Cannot Be Used with Oracle RAC Databases.... | 4-1 |
| 4.1.3 | OracleAS Guard Returned an Inappropriate Message When It Could Not Find the User Specified Database Identifier | 4-2 |
| 4.2 | Configuration Issues and Workarounds | 4-2 |
| 4.2.1 | The asgctl shutdown topology Command Does Not Shut Down an MRCA Database That is Detected To Be of a repCa Type Database | 4-2 |
| 4.3 | Documentation Errata and Omissions..... | 4-2 |
| 4.3.1 | Availability of a Previously Undocumented asgctl Command: create standby database | 4-3 |
| 4.3.2 | Connecting to an OracleAS Guard Server May Return an Authentication Error..... | 4-3 |

| | | |
|-------|--|-----|
| 4.3.3 | All emagents Must Be Shut Down Before Performing OracleAS Guard Operations | 4-3 |
| 4.3.4 | Procedure to Patch a 10.1.2.0.0 Disaster Recovery Setup with a 10.1.2.1.0 Patchset.. | 4-4 |
| 4.3.5 | Running Instantiate Topology Across Nodes After Executing a Failover Operation Results in an ORA-01665 Error | 4-4 |
| 4.3.6 | OracleAS Guard Is Unable to Shutdown the Database Because More Than One Instance of Oracle RAC is Running | 4-4 |

5 Oracle Access Manager

| | | |
|--------|--|------|
| 5.1 | General Issues..... | 5-1 |
| 5.1.1 | Known Issue With JDK 1.1.7 | 5-1 |
| 5.1.2 | The Name "Query Builder" Is Not Always Translated | 5-1 |
| 5.1.3 | Users Can Access Resources After Password Reset Without Logging In | 5-2 |
| 5.2 | Installation and Upgrade Issues and Workarounds..... | 5-2 |
| 5.2.1 | Change the Transport Security Mode During Installation | 5-2 |
| 5.2.2 | Special Considerations for adding Language Packs to an Installation area with Space Characters | 5-3 |
| 5.2.3 | iPlanet Server Fails After Tuning | 5-4 |
| 5.2.4 | Oracle Internet Directory Servers Require Tuning After Installation..... | 5-4 |
| 5.2.5 | Support for DirX Has Been Deprecated | 5-4 |
| 5.2.6 | "Enter Password" String Does Not Display Correctly During Installation..... | 5-4 |
| 5.2.7 | Uninstalling a Language Pack With a "2" Designation Causes an Error | 5-4 |
| 5.3 | Removal Issues and Workarounds..... | 5-5 |
| 5.3.1 | Removing Language Packs | 5-5 |
| 5.3.2 | Removing the Default Administrator Language | 5-5 |
| 5.3.3 | Removing Components and Reinstalling | 5-5 |
| 5.4 | Access System Issues and Workarounds..... | 5-6 |
| 5.4.1 | WebGate Diagnostics URL Incorrectly Report the Access Server Is Down..... | 5-6 |
| 5.4.2 | WebGate Is Unable to Connect to Its Associated Access Server | 5-7 |
| 5.4.3 | Memory Usage Rises After Configuring a Directory Server Profile | 5-7 |
| 5.4.4 | The Passthrough Challenge Parameter Does Not Work on a Domino Web Server .. | 5-7 |
| 5.4.5 | Steps for Integrating the Access System with OracleAS Single Sign-On 10.1.2.0.2 ... | 5-7 |
| 5.4.6 | Return Type Parameters Are Case-Sensitive in This Release | 5-10 |
| 5.4.7 | Single Sign-On with Oracle Identity Management Fails | 5-10 |
| 5.5 | Identity System Workarounds and Issues | 5-10 |
| 5.5.1 | Identity System Deletes a User Entry When an RDN is Modified | 5-11 |
| 5.5.2 | Identity System Deletes a User Entry When an RDN is Modified | 5-11 |
| 5.5.3 | Auditing for the Identity System Ceases to Work | 5-12 |
| 5.5.4 | Identity Server Crashes if It Cannot Find a Style Sheet | 5-12 |
| 5.5.5 | WebPass Is Unable to Connect to Its Associated Identity Server | 5-12 |
| 5.5.6 | Memory Usage Rises for an Identity Server After Configuring a Directory Server Profile | 5-12 |
| 5.5.7 | Errors Are Found in the HTTP Logs After Setting Up the Identity System | 5-13 |
| 5.5.8 | Reports With Non-ASCII Characters Are Not Imported Correctly in Excel | 5-13 |
| 5.5.9 | Translation of Tab Names May be Incomplete | 5-13 |
| 5.5.10 | Non-ASCII Values for Certain Display Types Are Corrupted in the Identity System Console | 5-14 |
| 5.5.11 | Data Is Lost When Saving an Object Profile in Org. Manager | 5-14 |

| | | |
|-------|---|------|
| 5.6 | Directory Issues..... | 5-14 |
| 5.6.1 | Error "There Is No Profile Configured for this Kind of Object" | 5-14 |
| 5.6.2 | Issues With the Display of Messages in Some Languages..... | 5-15 |
| 5.6.3 | Support for eDirectory 8.7.3..... | 5-15 |
| 5.7 | Documentation Issues | 5-15 |
| 5.7.1 | Reference to Oracle Internet Directory Is Needed in Installation Preparation Checklist | 5-16 |
| 5.7.2 | Help Mentions WebGateStatic.lst But No Such File Exists | 5-16 |
| 5.7.3 | The obEnableCredentialCache Credential Mapping Parameter Is Misspelled | 5-16 |
| 5.7.4 | Warning Regarding Retrieving Authorization Data From an External Source | 5-16 |
| 5.7.5 | Active Directory MaxPageSize Parameter Stated as PageSize Parameter | 5-17 |
| 5.7.6 | Missing Parameter in globalparams.xml Documentation | 5-17 |

6 Oracle Application Server Single Sign-On

| | | |
|-------|--|-----|
| 6.1 | Installation, Installation and Upgrade Issues | 6-1 |
| 6.1.1 | Directory Considerations During Installation..... | 6-1 |
| 6.1.2 | Directory Considerations After Installation | 6-2 |
| 6.1.3 | Identity Management Grid Control Considerations During Uninstallation | 6-2 |
| 6.2 | General Issues..... | 6-2 |
| 6.2.1 | A "Host Unavailable" Entry Appears on Non-English Monitoring Pages | 6-2 |
| 6.2.2 | Dynamic Global Logout Directives Must Pass the String "Oracle SSO"..... | 6-3 |
| 6.2.3 | Multilevel Authentication Configuration May or May Not Require a Port Number | 6-3 |

7 Oracle Identity Federation

| | | |
|-------|--|-----|
| 7.1 | General Issues and Workarounds | 7-1 |
| 7.1.1 | Credential Re-entry When Accessing a SiteMinder Protected Resource | 7-1 |
| 7.1.2 | Reauthentication after Session Timeout with OracleAS Single Sign-On and SAML 1.x or WS-Federation | 7-1 |
| 7.1.3 | Attribute Sharing with the Microsoft Internet Information Server | 7-2 |
| 7.1.4 | Redirection Loops with Oracle Access Manager | 7-2 |
| 7.1.5 | Truncated Text in Japanese Version of Oracle Universal Installer..... | 7-2 |
| 7.1.6 | Unused Assertion Profile With Invalid Attribute Mapping Can Cause SSO Failure | 7-3 |
| 7.1.7 | Signed SAML 1.0 Assertions Can Cause SSO Failures | 7-3 |
| 7.1.8 | Encrypting Network Connections..... | 7-4 |
| 7.1.9 | Spurious Certificate Verification Failure in Debug Log..... | 7-4 |
| 7.2 | Configuration Issues and Workarounds | 7-4 |
| 7.2.1 | Administration Console Is Not Accessible After Changing Transient Data Store | 7-4 |
| 7.2.2 | Signing SAML Response with Assertion | 7-5 |
| 7.2.3 | Assertions Using SAML 1.x POST Method Fail in Japanese Locale | 7-5 |
| 7.2.4 | Using RDBMS as a User Data Store with a Login column ID of type CHAR..... | 7-5 |
| 7.2.5 | Some Peer Providers Are Not Displayed in Administration Console..... | 7-6 |
| 7.2.6 | SAML 2.0 Metadata AttributeRequesterDescriptor Not Supported | 7-6 |
| 7.2.7 | Problems Disabling Protocol Profiles in Administration Console | 7-6 |
| 7.2.8 | Metadata Service URLs With Query Parameters Not Supported | 7-6 |
| 7.3 | Documentation Errata | 7-7 |
| 7.3.1 | Incorrect Header in Oracle Identity Federation Online Help | 7-7 |
| 7.3.2 | Usage of Command-line Configuration Assistants | 7-7 |

8 Oracle Security Developer Tools

| | | |
|-------|---|-----|
| 8.1 | General Issues and Workarounds | 8-1 |
| 8.1.1 | Oracle XML Security Does Not Handle the InclusiveNamespaces Tag | 8-1 |

9 Oracle Internet Directory

| | | |
|-------|--|-----|
| 9.1 | General Issues and Workarounds | 9-1 |
| 9.1.1 | Perform Full Database Backup After Administrative Changes to Oracle Internet Directory | 9-1 |
| 9.1.2 | Comment Out ACL Attributes Not Defined in the Schema | 9-2 |
| 9.1.3 | Specify DN of the DIT When Dumping Directory Entries for an Advanced Replication Agreement | 9-2 |
| 9.2 | Configuration Issues and Workarounds | 9-3 |
| 9.2.1 | Set Language Before Using bulkload | 9-3 |
| 9.3 | Documentation Errata | 9-3 |
| 9.3.1 | Bad Links in Online Help Pages | 9-3 |
| 9.3.2 | Missing Line Break in sqlplus Command | 9-3 |
| 9.3.3 | Errors in oracle.ldap.util.Subscriber.createUser() Documentation | 9-4 |
| 9.3.4 | Missing Example: How to Decode a Mime-Encoded Header Set by mod_sso | 9-4 |
| 9.3.5 | Error in Identity Management Grid Control Plug-in Context-Sensitive Help | 9-4 |
| 9.3.6 | Missing Note: The labeledURI Attribute host:port is for Syntax Purposes Only | 9-5 |
| 9.3.7 | Missing Example: Listing All the Attributes in the Directory by Using ldapsearch | 9-5 |
| 9.3.8 | Incorrect Environment Variables in Plug-in Debugging Examples | 9-5 |
| 9.3.9 | Figure Errors in Replication Concepts Chapter | 9-5 |

10 Oracle Application Server Certificate Authority

| | | |
|--------|---|------|
| 10.1 | Documentation Errata | 10-1 |
| 10.1.1 | Java Classes for Custom Policy Plug-in Must Use JDK 1.4.2 | 10-1 |
| 10.1.2 | Incorrect Class Name in Custom Policy Example | 10-1 |

11 Oracle Delegated Administration Services

| | | |
|--------|--|------|
| 11.1 | General Issues and Workarounds | 11-1 |
| 11.1.1 | Installation Process Does Not Enable SSL for Oracle Delegated Administration Services | 11-1 |
| 11.1.2 | Using Single Wildcard Characters to Search for Entries Fails to Return Results.... | 11-1 |
| 11.1.3 | Oracle Internet Directory Self-Service Console Link Does Not Work in Oracle Identity Manager Grid Control Plug-in | 11-1 |
| 11.2 | Administration Issues and Workarounds | 11-2 |
| 11.2.1 | Disabling Password Change and Reset Functionality | 11-2 |
| 11.2.2 | Resetting Oracle Application Server Single Sign-On Passwords Redirects Users to Oracle Delegated Administration Services Home Page | 11-2 |

12 Oracle Directory Integration Platform

| | | |
|--------|--|------|
| 12.1 | Configuration Issues and Workarounds | 12-1 |
| 12.1.1 | Configuration Requirements for Synchronizations with Domain-Level Mappings | 12-1 |
| 12.1.2 | Directory Integration Assistant Throws "LDAP: error code 2 - Decoding Error" When Uploading an Additional Configuration Information File | 12-2 |

| | | |
|--------|--|------|
| 12.1.3 | Reconfiguring the Oracle Password Filter for Microsoft Active Directory Generates Errors | 12-2 |
| 12.1.4 | In a High Availability Environment Using Multimaster Replication, Provisioning Events May not Be Propagated or May Be Duplicated | 12-3 |
| 12.1.5 | Manual Step Required After Configuring Oracle Directory Integration Platform from Oracle Enterprise Manager | 12-3 |
| 12.1.6 | Securing the Windows Registry Before Installing the Oracle Password Filter for Microsoft Active Directory | 12-4 |
| 12.2 | Administration Issues and Workarounds | 12-4 |
| 12.2.1 | Default Mapping Rule Can Be Simplified in Single-Domain Microsoft Active Directory Deployments | 12-4 |
| 12.2.2 | Oracle Directory Integration Platform Not Sending Provisioning Events Due to Purged Change Log Entries | 12-5 |
| 12.2.3 | Oracle Internet Directory Field Unavailable in Oracle Identity Manager Grid Control Plug-in | 12-5 |
| 12.2.4 | Synchronization from Novell eDirectory or OpenLDAP Fails When the Oracle Internet Directory Container is Within the Default Realm..... | 12-6 |

Preface

This preface includes the following topics:

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

Audience

This document is intended for users of Oracle Application Server 10g.

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 Application Server Documentation on Oracle Application Server Disk 1
- Oracle Application Server Documentation Library 10g (10.1.4.0.1)

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. |
| <code>monospace</code> | 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 the *Oracle Application Server Release Notes*?

This chapter provides a listing of new topics introduced with this version of the *Oracle Application Server Release Notes*. The new topics are in the following chapters:

- Chapter 2, "Installation and Upgrade Issues"
- Chapter 5, "Oracle Access Manager"
- Chapter 6, "Oracle Application Server Single Sign-On"
- Chapter 7, "Oracle Identity Federation"
- Chapter 9, "Oracle Internet Directory"

Chapter 2, "Installation and Upgrade Issues"

- Section 2.1.13, "OIDCA Fails Due to Misconfigure in /ECT/HOSTS"
- Section 2.1.14, "DB Console of Infrastructure IM+MR Cannot be Started"
- Section 2.1.12, "OID Configuration Assistant Fails While Installing Oracle Application Server in Japanese Locale"
- Section 2.2.6, "Issues When Using the Idifwrite Command to Back Up the Oracle Internet Directory"
- Section 2.2.7, "Upgrade of OracleAS Cold Failover Clusters Fails While Running Configuration Assistant"

Chapter 5, "Oracle Access Manager"

- Section 5.1.3, "Users Can Access Resources After Password Reset Without Logging In"
- Section 5.4.6, "Return Type Parameters Are Case-Sensitive in This Release"
- Section 5.4.7, "Single Sign-On with Oracle Identity Management Fails"
- Section 5.5.1, "Identity System Deletes a User Entry When an RDN is Modified"
- Section 5.7.5, "Active Directory MaxPageSize Parameter Stated as PageSize Parameter"
- Section 5.7.6, "Missing Parameter in globalparams.xml Documentation"

Chapter 6, "Oracle Application Server Single Sign-On"

- [Section 6.2.3, "Multilevel Authentication Configuration May or May Not Require a Port Number"](#)

Chapter 7, "Oracle Identity Federation"

- [Section 7.1.9, "Spurious Certificate Verification Failure in Debug Log"](#)
- [Section 7.2.5, "Some Peer Providers Are Not Displayed in Administration Console"](#)
- [Section 7.2.6, "SAML 2.0 Metadata AttributeRequesterDescriptor Not Supported"](#)
- [Section 7.2.7, "Problems Disabling Protocol Profiles in Administration Console"](#)
- [Section 7.2.8, "Metadata Service URLs With Query Parameters Not Supported"](#)

Chapter 9, "Oracle Internet Directory"

- [Section 9.3.3, "Errors in oracle.ldap.util.Subscriber.createUser\(\) Documentation"](#)
- [Section 9.3.4, "Missing Example: How to Decode a Mime-Encoded Header Set by mod_sso"](#)
- [Section 9.3.5, "Error in Identity Management Grid Control Plug-in Context-Sensitive Help"](#)
- [Section 9.3.6, "Missing Note: The labeledURI Attribute host:port is for Syntax Purposes Only"](#)
- [Section 9.3.7, "Missing Example: Listing All the Attributes in the Directory by Using ldapsearch"](#)
- [Section 9.3.8, "Incorrect Environment Variables in Plug-in Debugging Examples"](#)
- [Section 9.3.9, "Figure Errors in Replication Concepts Chapter"](#)

Introduction

This chapter introduces Oracle Application Server Release Notes, 10g (10.1.4.0.1). It includes the following topics:

- [Section 1.1, "Latest Release Information"](#)
- [Section 1.2, "Purpose of this Document"](#)
- [Section 1.3, "Operating System Requirements"](#)
- [Section 1.4, "Multiple Versions of Identity Management in this Release"](#)
- [Section 1.5, "Certification Information"](#)
- [Section 1.6, "Licensing Information"](#)

1.1 Latest Release Information

This document is accurate at the time of publication. Oracle will update the release notes periodically after the software release. You can access the latest information and additions to these release notes on the Oracle Technology Network at:

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

1.2 Purpose of this Document

This document contains the release information for Oracle Application Server 10g (10.1.4.0.1). It describes differences between Oracle Application Server and its documented functionality.

Oracle recommends you review its contents before installing, or working with the product.

When you install Oracle Identity Management 10g (10.1.4.0.1), specific installation types include Oracle HTTP Server, Oracle Containers for J2EE (OC4J), and Oracle Enterprise Manager Application Server Control Console. For release notes that affect these components, refer to the *Oracle Application Server Release Notes* for Oracle Application Server 10g Release 2 (10.1.2.0.2).

1.3 Operating System Requirements

Oracle Application Server installation and configuration will not complete successfully unless users meet the hardware and software pre-requisite requirements before installation. See *Oracle Application Server Installation Guide* for a complete list of operating system requirements.

1.4 Multiple Versions of Identity Management in this Release

The 10g (10.1.2.0.2) CD Pack currently ships with two versions of the Identity Management components, the original 10g (10.1.2.0.2) Identity Management components and the new 10g (10.1.4.0.1) Identity Management components. Except in very special circumstances, such as use of third party products that are only certified against the original 10g (10.1.2.0.2) Identity Management, it is recommended that the new 10g (10.1.4.0.1) Identity Management components be used from the CD Pack. Please check the certification matrix on Oracle*MetaLink* site, (<http://metalink.oracle.com>) for compatibility with your operating systems, platforms and third party products

1.5 Certification Information

The latest certification information for Oracle Application Server *10g* (10.1.4.0.1) is available at:

<http://metalink.oracle.com>

1.6 Licensing Information

Licensing information for Oracle Application Server is available at:

<http://oraclestore.oracle.com>

Detailed information regarding license compliance for Oracle Application Server is available at:

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

Installation and Upgrade Issues

This chapter describes installation and upgrade issues and their workarounds associated with Oracle Application Server. It includes the following topics:

- [Section 2.1, "Installation Issues"](#)
- [Section 2.2, "Upgrade Issues"](#)
- [Section 2.3, "Documentation Errata"](#)

2.1 Installation Issues

This section describes issues with installation of Oracle Application Server. It includes the following topics:

- [Section 2.1.1, "Unique Global Database Name Required During Installation"](#)
- [Section 2.1.2, "Do Not Use Turkish Locale During Installation"](#)
- [Section 2.1.3, "Oracle Application Server Repository Creation Assistant Fails During Loading When the Database Uses Certain Chinese Character Sets"](#)
- [Section 2.1.4, "OracleAS Cold Failover Cluster: Additional Configuration Steps for Oracle Delegated Administration Services"](#)
- [Section 2.1.5, "Oracle Internet Directory SSL Connection Fail Intermittently"](#)
- [Section 2.1.6, "Incorrect Location for Debug Message"](#)
- [Section 2.1.7, "Illegible or Garbage Characters Output in a Russian Locale"](#)
- [Section 2.1.8, "Application Server Control Console Link Not Operational in non-English Installations"](#)
- [Section 2.1.9, "Set the NLS Parameter Before Installing"](#)
- [Section 2.1.10, "Excessive Privileges for OracleAS Metadata Repository Installations"](#)
- [Section 2.1.11, "Incorrect Guidelines for Online Help"](#)
- [Section 2.1.12, "OID Configuration Assistant Fails While Installing Oracle Application Server in Japanese Locale"](#)
- [Section 2.1.13, "OIDCA Fails Due to Misconfigure in /ECT/HOSTS"](#)
- [Section 2.1.14, "DB Console of Infrastructure IM+MR Cannot be Started"](#)

2.1.1 Unique Global Database Name Required During Installation

During installation of either of the install types, Oracle Identity Management and OracleAS Metadata Repository, or OracleAS Metadata Repository, you must enter a unique Global Database Name on the **Specify Database Information** screen.

If there are 2 databases present on the same host, then each database should have a unique SID and Global Database Name.

Currently, the Oracle Universal Installer only checks if a unique SID is entered by user; it does not check if a Global Database Name is entered by the user. Both the SID and Global Database Name values are entered on the **Specify Database Information** screen. The installation proceeds with a potential Oracle Internet Directory Configuration Assistant failure. You may see an error message such as the following:

```
"The Network Adapter could not establish the connection"
```

2.1.2 Do Not Use Turkish Locale During Installation

Oracle recommends that you avoid running the Oracle Universal Installer to install Oracle Application Server using the Turkish locale because some of the installation screens will not be displayed properly and will not be usable.

2.1.3 Oracle Application Server Repository Creation Assistant Fails During Loading When the Database Uses Certain Chinese Character Sets

During loading of OracleAS Metadata Repository into an existing database, OracleAS RepCA fails if the database uses the ZHT16MSWIN950, ZHT16HKSCS, or ZHT16HKSCS31 character set.

To check the character set of your database, query the NLS_DATABASE_PARAMETERS view:

```
sqlplus "sys/password as sysdba"
SQL> select VALUE from NLS_DATABASE_PARAMETERS where PARAMETER='NLS_CHARACTERSET';
```

where *password* specifies the password for the SYS user.

2.1.4 OracleAS Cold Failover Cluster: Additional Configuration Steps for Oracle Delegated Administration Services

Additional configuration steps are required to configure Oracle Delegated Administration Services to work with an OracleAS Cold Failover Cluster.

Open the ORACLE_HOME/sysman/emd/targets.xml file and locate the oracle_das_server target and the HTTPMachine, DasURL, and DASMonitorURL properties:

```
<Target TYPE="oracle_das_server" NAME="instance.domain.com_DAS" DISPLAY_
NAME="instance.domain.com_DAS">
  <Property NAME="HTTPMachine" VALUE="LocalHost" />
  ...
  <Property NAME="DasURL" VALUE="http://LocalHost:7777/oiddas" />
  <Property NAME="DasMonitorURL"
VALUE="http://LocalHost:7777/oiddas/dasmetrics" />
  ...
</Target>
```

Change the HTTPMachine, DasURL, and DASMonitorURL property values to the virtual Apache host:

```
<Target TYPE="oracle_das_server" NAME="instance.domain.com_DAS" DISPLAY_
NAME="instance.domain.com_DAS">
  <Property NAME="HTTPMachine" VALUE="VirtualApacheHost"/>
  ...
  <Property NAME="DasURL" VALUE="http://VirtualApacheHost:7777/oiddas"/>
  <Property NAME="DasMonitorURL"
VALUE="http://VirtualApacheHost:7777/oiddas/dasmetrics"/>
  ...
</Target>
```

2.1.5 Oracle Internet Directory SSL Connection Fail Intermittently

The Oracle Internet Directory SSL connection may fail intermittently during an Oracle Application Server installation. Specifically, this failure may occur during an Identity Management and High Availability collocated installation.

To workaroud this issue, retry the failed configuration assistant from the installation.

2.1.6 Incorrect Location for Debug Message

If you encounter Oracle Internet Directory SSL connection failure, the log file (*ORACLE_HOME/sso/log/ssoca.log*) contains the message of connection failure to LDAP URL, but the correct debug message is `ldaps url`.

2.1.7 Illegible or Garbage Characters Output in a Russian Locale

When you install Oracle Application Server in Russian locale and some of the configuration assistants fail, you may receive exception message output to Oracle Universal Installer which contain illegible or garbage characters.

If you encounter this type of error message, you can safely ignore the message and continue with the installation and rerun the configuration assistants.

2.1.8 Application Server Control Console Link Not Operational in non-English Installations

In some non-English locale Oracle Application Server installations the Oracle Enterprise Manager 10g Application Server Control Console (Application Server Control Console) hyperlink is not operational on the Welcome page. If the hyperlink is not working in your installation, do the following:

1. Open the *ORACLE_HOME*/Apache/Apache/htdocs/index.html file.
2. Locate the line `` in the index.html file.
3. Replace `%s_hostName%` with your local hostname.
4. Replace `%s_oemConsolePort%` with the value of the Application Server Control Console port from the *ORACLE_HOME*/install/portlist.ini file,

2.1.9 Set the NLS Parameter Before Installing

If you set the following NLS parameters before installation of Oracle Identity Federation through Oracle Application Server:

```
LANG=zh_CN.GB18030
LC_ALL=zh_CN.GB18030
```

and then check the *ORACLE_*

HOME/dv/OraHome/inventory/Contents/comp.xml file at line 172 you will see the following:

```
<DEP NAME="oracle.iappserver.charts"VER="10.1.2.0.0" DEP_GRP_NAME="group2" HOME_
IDX="5"/>
```

Column 43 refers to the beginning of attribute VER, just after the XML attribute value of parameter NAME. A whitespace between the double quote and the parameter name is missing.

If you then install an additional Oracle Identity Federation instance on the same computer, you will receive an error message during the installation.

To workaroud this problem, set the NLS parameter as follows:

```
LANG=zh_CN.GBK
LC_ALL=zh_CN.GBK
```

In Oracle Application Server 10g (10.1.4.0.1), the Java Developer Kit does not support GB18030 encoding.

2.1.10 Excessive Privileges for OracleAS Metadata Repository Installations

This topic is applicable to installations of OracleAS Metadata Repository created with the Oracle Application Server Repository Creation Assistant or installed as part of an OracleAS Infrastructure installation.

The EXECUTE privilege is given to PUBLIC for the following packages:

- UTL_FILE
- DBMS_RANDOM
- UTL_HTTP
- UTL_SMTTP
- UTL_TCP

These privileges may be excessive, and not necessary for your enterprise.

Oracle recommends that you complete the following steps to determine if the EXECUTE privilege has been applied correctly in your enterprise:

1. Analyze your application and determine which account / applications require the above packages. If any accounts do require these privileges they will typically be accounts which own applications such as HR or CRM type applications.
2. Grant execute on the corresponding package to the account / application identified in Step 1. If you were not able to complete the analysis in Step 1, you can optionally grant execute on these packages to the existing application type accounts.
3. Revoke the EXECUTE privilege for the above packages from the group PUBLIC and verify your application continues to work properly. Completing this step will ensure that new accounts created in the future will not have execute on these packages by default.

2.1.11 Incorrect Guidelines for Online Help

The online help for the **Specify Database Configuration Options** screen lists the following two guidelines for specifying the global database name:

- The following characters are valid in the database domain: alphanumeric characters, the underscore (_) character, the minus (-) character, and the pound sign (#) character.
- The database name can contain only alphanumeric characters (A-Z and 0-9).

These guidelines are incorrect and should be replaced with the following guideline:

- The following characters are valid in the database domain and domain name: alphanumeric characters, the underscore (_) character, and the pound sign (#) character.

2.1.12 OID Configuration Assistant Fails While Installing Oracle Application Server in Japanese Locale

The OID Configuration Assistant may fail while performing an OracleAS Infrastructure installation. This happens when the character set is SJIS in Japanese locale.

To workaroud this issue, perform the following steps before running `root.sh`:

1. Backup `opmnctl` script in `$ORACLE_HOME/opmn/bin`.
2. Modify the `NLS_LANG` parameter in `opmnctl` script to `JAPANESE_JAPAN.JA16SJIS`.
3. Stop and Start OracleAS Infrastructure components by giving the following commands:


```
opmnctl stopall
opmnctl start
```
4. Run `root.sh` to continue the installation.

2.1.13 OIDCA Fails Due to Misconfigure in /ECT/HOSTS

If the virtual hostname specified during a DR/CFC OID installation is an alias hostname instead of valid virtual hostname or IP address, and does not have the domain name configured the system, OUI (OIDCA) may fail. If so, a `gethostbyname failed` message appears in the `$ORACLE_HOME/ldap/log/oidldapd01.log`

To resolve this issue, add the domain name to the alias name in the `/etc/hosts` file, click the **Retry** button on OUI, and OUI continues to install.

2.1.14 DB Console of Infrastructure IM+MR Cannot be Started

If you install AS 10.1.4IM Infrastructure IM+MR, and try to open the Enterprise Manager using the `$OH/emctl start dbconsole` command, you may receive the following error message:

```
OC4J Configuration Issue.
<ORACLE_HOME>/oc4j/j2ee/OC4J_DBConsole_jphp4d54.jp.oracle.com_infd4 not
found.
```

To work around this issue, run `emca post install` as:

```
.
```

emca -r

2.2 Upgrade Issues

This section describes issues with upgrade of Oracle Application Server. It includes the following topics:

- [Section 2.2.1, "Upgrade of Identity Management Installation to 10.1.4.0.1"](#)
- [Section 2.2.2, "Additional Step Required When Upgrading OracleAS Metadata Repository Release 9.0.4.3 to 10.1.4.0.1"](#)
- [Section 2.2.3, "Configuring Port Values for the Load Balancer and Oracle Internet Directory When Upgrading Oracle Application Server Cluster \(Identity Management\)"](#)
- [Section 2.2.4, "Harmless Error Messages During OracleAS Metadata Repository Upgrade"](#)
- [Section 2.2.5, "Metadata Repository Container Version"](#)
- [Section 2.2.6, "Issues When Using the Idifwrite Command to Back Up the Oracle Internet Directory"](#)
- [Section 2.2.7, "Upgrade of OracleAS Cold Failover Clusters Fails While Running Configuration Assistant"](#)

2.2.1 Upgrade of Identity Management Installation to 10.1.4.0.1

If you have the following upgrade:

- Upgrade your Identity Management installation to 10.1.4.0.1
- Install Oracle Enterprise Manager 10g Grid Control Plug-in and Oracle Identity Management Grid Control Plug-in Agent
- Each Identity Management component will display two targets in Oracle Enterprise Manager Grid Control. One target is for the pre-upgrade Identity Management installation, and the other is for the upgraded Identity Management installation.

This is expected behavior because the pre-upgrade Oracle home is still registered with `oraInventory`. The Oracle Enterprise Manager Grid Control Plug-in Agent discovers all of the Oracle homes on a host and collects information from the respective `targets.xml` files.

To avoid this problem:

1. Upgrade your Identity Management installation to 10.1.4.0.1.
2. Install Oracle Enterprise Manager 10g Grid Control Agent and Oracle Identity Management Grid Control Plug-in Agent.
3. Remove the pre-upgrade Oracle Application Server Single Sign-On and Oracle Internet Directory targets as follows:
 - a. Open the Oracle Enterprise Manager Grid Control.
 - b. Select and click **Targets**.
 - c. Select and click **All Targets**
 - d. For each pre-upgrade Oracle Application Server Single Sign-On and Oracle Internet Directory target:

- Select the target instance
- Click **Remove**

For the Oracle Enterprise Manager 10g Grid Control Agent to collect proper monitoring data, you will need to reset the password of the database user `dbsnmp` of the upgraded Identity Management installation.

To reset the database user password, run the following command (`sqlplus "/as sysdba"`) from the Identity Management database `ORACLE_HOME`:

```
> alter user dbsnmp identified by "/dbsnmp_passwd/";
> commit;
```

2.2.2 Additional Step Required When Upgrading OracleAS Metadata Repository Release 9.0.4.3 to 10.1.4.0.1

If you have applied Oracle Application Server 10g (9.0.4) Patchset 3 (9.0.4.3) to your release 9.0.4 instance, and now want to upgrade the OracleAS Metadata Repository to release 10.1.4.0.1 by running 10.1.4.0.1 MRUA, you must first apply patch 5365207 to your 10.1.4.0.1 MRUA. For this, you must copy the contents of the 10.1.4.0.1 MRUA and Utilities CD-ROM to a location where you have write permission. Then apply patch 5365207 on your 10.1.4.0.1 MRUA staged directory. You can find this patch on Oracle *Metalink* at

<http://metalink.oracle.com>

Use the patched version of 10.1.4.0.1 MRUA to upgrade a release 9.0.4.3 instance to release 10.1.4.0.1. For details about running MRUA, refer to the *Oracle Application Server Upgrade and Compatibility Guide*.

If you do not apply patch 5365207, then the portal component upgrade will fail with the following error when running 10.1.4.0.1 MRUA:

```
Calling upgrade plugin for PORTAL
Error: Component upgrade failed PORTAL
Error: PORTAL component version is: 9.0.4.3.0 INVALID
```

This error message is displayed on screen and is also recorded in the MRUA log file, `ORACLE_HOME\upgrade\logs\mrua.log`. For the detailed error message, review the portal upgrade precheck log file, `ORACLE_HOME\upgrade\temp\portal\precheck.log`. Refer to the *Oracle Application Server Upgrade and Compatibility Guide* for further information on reviewing the upgrade log files.

The detailed error message from the `precheck.log` file reads as follows:

```
### Install Schema Validation Utility
>>> Running upg/common/prechk/svuver.sql .
Portal SQL script started at Thu Jun  1 08:55:22 2006
Connected.
# Beginning outer script: common/prechk/svuver
# Portal Schema Version = 9.0.4.3.0
# Version of schema validation utility being installed =
Connected.
###
### ERROR: Exception Executing upg/common/prechk/svuver.sql
###
### Check Failed at Thu Jun  1 08:55:24 2006 Continuing as PreCheck mode is
specified
```

```

### Invoke Schema Validation Utility in Report Mode
>>> Running upg/common/prechk/./svurun.sql .
Portal SQL script started at Thu Jun  1 08:55:24 2006
Connected.
# Beginning outer script: common/prechk/svurun
#-- Beginning inner script: common/common/svurun

l_mode := wwutl_schema_validation.MODE_REPORT;

          *

ERROR at line 5:
ORA-06550: line 5, column 19:
PLS-00201: identifier 'WWUTL_SCHEMA_VALIDATION.MODE_REPORT' must be declared
ORA-06550: line 5, column 9:
PL/SQL: Statement ignored
ORA-06550: line 8, column 19:
PLS-00201: identifier 'WWUTL_SCHEMA_VALIDATION.MODE_CLEANUP' must be declared

ORA-06550: line 8, column 9:
PL/SQL: Statement ignored
ORA-06550: line 15, column 5:
PLS-00201: identifier 'WWUTL_SCHEMA_VALIDATION.VALIDATE_ALL' must be declared

ORA-06550: line 15, column 5:
PL/SQL: Statement ignored
Connected.
###
### ERROR: Exception Executing upg/common/prechk/./svurun.sql REPORT
###
### Check Failed at Thu Jun  1 08:55:25 2006 Continuing as PreCheck mode is
specified

```

Note: In the case where you have already encountered this error, apply patch 5365207 and rerun the upgrade. There is no need to restore the OracleAS Metadata Repository from backup before rerunning the upgrade. This is because the upgrade failed during the precheck phase and the portal schema in the OracleAS Metadata Repository has not been altered in the precheck phase.

If the portal upgrade fails in the precheck phase even after applying patch 5365207, then review the precheck log file for details about the new error. Based on the description of the error, resolve the problem and perform the upgrade again, or contact Oracle Support Services for help.

2.2.3 Configuring Port Values for the Load Balancer and Oracle Internet Directory When Upgrading Oracle Application Server Cluster (Identity Management)

The procedure for upgrading to 10g (10.1.4.0.1) Oracle Application Server Cluster (Identity Management) (OracleAS Cluster (Identity Management)) is documented in Appendix B of the *Oracle Application Server Upgrade and Compatibility Guide*. However, if you are upgrading this type of environment, there is an additional task you must perform if all of the following is true:

- You are upgrading an OracleAS Cluster (Identity Management) environment to 10g (10.1.4.0.1).
- Your load balancer and Oracle Internet Directory are using different ports.
- Your Oracle Internet Directory ports are set to a value less than 1024 and your load balancer ports are set to a value higher than 1024.

In this specific scenario, perform the following steps when you are prompted by Oracle Universal Installer to run the `root.sh` script:

1. Use a text editor to open the `root.sh` file in the Oracle home of the Identity Management instance you are upgrading.
2. Edit the following two entries in the `root.sh` file so they point to the SSL and non-SSL port of the Oracle Internet Directory.

For example:

```
SSLPORT=636
NONSSLPORT=389
```

Make sure these entries do not point to the load balancer ports.

3. Save and close the `root.sh` file.
4. Run the `root.sh` file as the root user, as directed by the Oracle Universal Installer instructions.

If you do not perform these steps during the upgrade procedure, the Oracle Internet Directory configuration assistant will fail during the configuration phase of the upgrade procedure.

To fix this problem after the Oracle Internet Directory configuration assistant fails:

1. Leave Oracle Universal Installer running (with the configuration screen displayed) and open a new terminal window.
2. From the new terminal window, execute the following commands as the root user in the destination Oracle home:

```
chown root <DESTINATION_ORACLE_HOME>/bin/oidldapd
chmod 4710 <DESTINATION_ORACLE_HOME>/bin/oidldapd
```

3. Return to the Oracle Universal Installer window and retry the Oracle Internet Directory configuration assistant.

2.2.4 Harmless Error Messages During OracleAS Metadata Repository Upgrade

When you upgrade your OracleAS Metadata Repository `ORACLE_HOME` to 10g (10.1.4.0.1) you may see the following message in the `installActions.log` file, or the XTERM terminal or DOS command shell window if you are performing a non-interactive installation:

```
getXMLUserManager:Exception /ORACLE_HOME/in1014MR/sysman/j2ee/config/jazn-data.xml
(No such file or directory)
getRealmUser: XMLUserManager is null
getXMLUserManager:Exception
/ORACLE_HOME/in1014MR/sysman/j2ee/config/jazn-data.xml (No such file or directory)
```

There is no adverse effects to the installed OracleAS Metadata Repository. The observed messages are only debug messages.

You can ignore the observed messages, there is no adverse effect to the upgrade process.

2.2.5 Metadata Repository Container Version

The Metadata Repository Container (MRC) version in `app_registry` is 10g (10.1.2.0.2).

There were no schema changes to any OracleAS Metadata Repository components in the 10g (10.1.4.0.1) release. Upgrades from the 10g (10.1.4.0.1) release to the OracleAS Portal (10.1.4.0.0) release is therefore supported.

2.2.6 Issues When Using the `ldifwrite` Command to Back Up the Oracle Internet Directory

When using the data migration method of upgrading the OracleAS Identity Management, the instructions in Section C.2 of the Oracle Application Server Upgrade and Compatibility Guide instruct you to use the `ldifwrite` command to backup the Oracle Internet Directory.

When you use the `ldifwrite` command, you might be prompted to enter the OID password. In response to this prompt, enter the password for the ODS schema in the Oracle Internet Directory database.

If you do not know the ODS schema password, refer to section 6.3, "Viewing OracleAS Metadata Repository Schema Passwords," in the *Oracle Application Server Administrator's Guide*.

In addition, if you receive an error stating that you cannot connect to the database while attempting to use the `ldifwrite` command, then try creating a wallet for the Oracle Internet Directory ODS schema password. Use the following command to create a wallet for the password:

```
oidpasswd connect=<conn_string>
           create_wallet=true
           current_password=<ods_schema_password>
```

For more information, see the information on the `oidpasswd` command in Chapter 3, "Oracle Internet Directory Database Administration Tools," in the *Oracle Identity Management User Reference*.

2.2.7 Upgrade of OracleAS Cold Failover Clusters Fails While Running Configuration Assistant

You can upgrade your OracleAS Cold Failover Clusters environment to Oracle Application Server Release 3 (10.1.4.0.1) using the instructions in Appendix B of the Oracle Application Server Upgrade and Compatibility Guide.

However, for the upgrade to be successful, it is important that the active node in the cluster is associated with the correct virtual hostname and virtual IP address. This allows clients to access the OracleAS Cold Failover Cluster using the virtual hostname.

If you have reconfigured your environment since installing OracleAS Failover Clusters--then the upgrade to Release 3 (10.1.4.0.1) will fail while running the DBMS_IAS_VERSION package Configuration Assistant in Oracle Universal Installer. The installer log files will include the following message:

```
"DBMS_IAS_VERSION package Configuration Assistant" failed java.sql.SQLException:
Listener refused the connection with the following error:
```

ORA-12514, TNS:listener does not currently know of service requested in connect descriptor

To remedy this problem, refer the instructions for mapping the Virtual Hostname and Virtual IP address, which are included in the section, "Preinstallation Steps for OracleAS Cold Failover Clusters," in the *Oracle Application Server Installation Guide* for your platform. Then, run the configuration assistant again. For more information, see the "Configuration Assistants" appendix of the Installation Guide for your platform.

2.3 Documentation Errata

This section describes issues with Oracle Application Server documentation. It includes the following topics:

- [Section 2.3.1, "Incorrect Line Breaks in MRUA Sample Output"](#)
- [Section 2.3.2, "Incorrect Global Database Naming Standard"](#)

2.3.1 Incorrect Line Breaks in MRUA Sample Output

Example 8-1, "Sample Output from an MRUA Session" in the *Oracle Application Server Upgrade and Compatibility Guide*, shows the output from a typical session with the Metadata Repository Upgrade Assistant. However, in the HTML version of the guide, the line breaks are shown incorrectly. The following lines in the sample output should appear as follows:

```
Upgrading the OracleAS Metadata Repository to release 10.1.4.0.1.
```

```
Calling upgrade plugin for MRUA  
Component upgraded successfully MRUA
```

2.3.2 Incorrect Global Database Naming Standard

In Table 4-14, "Database Screens", in the **Specify Database Identification** screen description in the *Oracle Application Server Installation Guide*, the section incorrectly states that the database name portion of the global database name must contain alphanumeric characters only. This is incorrect. The database name can contain alphanumeric, underscore (_), and pound (#) characters.

General Management and Security Issues

This chapter describes management and security issues associated with Oracle Application Server. It includes the following topics:

- [Section 3.1, "General Management Issues"](#)
- [Section 3.2, "Documentation Errata"](#)

3.1 General Management Issues

This section describes general management issues with installation of Oracle Application Server. It includes the following topic:

- [Section 3.1.1, "Modifying targets.xml After Enabling SSL for Oracle Identity Management 10g \(10.1.4.0.1\)"](#)
- [Section 3.1.2, "Changing the IP Address of a Metadata Repository Created with Oracle Application Server Repository Creation Assistant"](#)
- [Section 3.1.3, "Oracle Enterprise Manager Grid Control Does not Display all Integration Profiles"](#)
- [Section 3.1.4, "Additional Information for Changing Hostname for Identity Management Installations"](#)

3.1.1 Modifying targets.xml After Enabling SSL for Oracle Identity Management 10g (10.1.4.0.1)

After you enable SSL for Oracle Identity Management, you must modify the `targets.xml` configuration file to be sure that Application Server Control can connect to the required OracleAS Single Sign-On and Oracle Delegated Administration Services URLs:

1. Locate and open the `targets.xml` file with a text editor.

The file is located in the destination Oracle home:

2. In the `targets.xml` file, locate the Oracle Delegated Administration Services element:

```
<Target TYPE="oracle_das_server" ... >
  ...
</Target>
```

3. Within the `oracle_das_server` element, update the properties shown in [Table 3–1](#) with the recommended values shown for each property.

Table 3–1 OracleAS Single Sign-On and Oracle Delegated Administration Services Properties to Modify in the targets.xml Configuration File

| Property | Description and Required Value |
|---------------|--|
| HTTPProtocol | The protocol used by the Oracle HTTP Server. The value can be either HTTP or HTTPS (for secure SSL connections). |
| MonitorPort | The physical port used to monitor the Oracle Delegated Administration Services on the host. This is often the default Oracle HTTP Server port. |
| DasPort | The physical port used to monitor Oracle Delegated Administration Services on the host. This is often the default Oracle HTTP Server port. |
| DasURL | The complete Oracle Delegated Administration Services URL, including the protocol, physical host name, and port. Do not use the load balancer virtual host and port. |
| DasMonitorURL | The complete URL used by Application Server Control to monitor the Oracle Delegated Administration Services, including the protocol, physical host name, and port. Do not use the load balancer virtual host and port. |

4. Locate the OracleAS Single Sign-On element within the `targets.xml` file:

```
<Target TYPE="oracle_sso_server" ... >
  ....
</Target>
```

5. Edit the values for the `HTTPPort` and `HTTPProtocol` properties within the `oracle_sso_server` element.

Be sure to enter the port and protocol for the physical OracleAS Single Sign-On host; do not use the port and protocol used to connect to the load balancer.

6. Save your changes and close the `targets.xml` file.

3.1.2 Changing the IP Address of a Metadata Repository Created with Oracle Application Server Repository Creation Assistant

You can change the IP address of a host that contains a OracleAS Metadata Repository, whether it is one created by an installation of OracleAS Infrastructure or by running Oracle Application Server Repository Creation Assistant. The chapter, "Changing Network Configurations" in the *Oracle Application Server Administrator's Guide* describes how to change the IP address.

If the `tnsnames.ora` file contains the IP address, you must take the following steps to change the IP address of a OracleAS Metadata Repository created by the Repository Creation Assistant:

1. Stop all processes in the middle tier and Infrastructure.
2. Set the `ORACLE_HOME` environment variable.
3. On the Metadata Repository host, if the entry in the `$ORACLE_HOME/network/admin/tnsnames.ora` file contains the IP address for the OracleAS Metadata Repository, change the IP address.
4. Start the Oracle Internet Directory server instance, for example:

```
$ORACLE_HOME/bin/oidmon start
$ORACLE_HOME/bin/oidctl connect=connect_string server=oidldapd\
instance=server_instance_number\
```

```
configset=configset_number] [host=virtual/host_name] \
start
```

5. On the middle tier host, if the entry in the `$ORACLE_HOME/network/admin/tnsnames.ora` file contains the IP address for the Metadata Repository, change the IP address in the file.
6. Start the middle tier.

3.1.3 Oracle Enterprise Manager Grid Control Does not Display all Integration Profiles

If you install the following:

- Install a 10.1.4.0.1 OracleAS Infrastructure with Identity Management
- Install Oracle Identity Management Agent Plug-in on the same host
- In Oracle Enterprise Manager Grid Control, navigate to **Targets > Identity Management > DIP**
- In the Integration Profiles table, only one profile is displayed and it shows a status of "disabled".

To workaroud this issue:

1. Using the Directory Integration Assistant (`dipassistant`), enable any profile.
2. Refresh the Oracle Directory Integration Platform (DIP) page in Oracle Enterprise Manager 10g Grid Control.
3. All fourteen Integration Profiles will be displayed.

3.1.4 Additional Information for Changing Hostname for Identity Management Installations

The *Oracle Application Server Administrator's Guide* describes how to change the hostname of machine containing an Identity Management installation. However, the procedure may fail if SSL is enabled (in this case, the non-ssl port is not available). Therefore, if SSL is enabled, you must take the following steps before you change the hostname of the machine:

1. Check the values of the `OIDport` and `SSLOnly` parameters in the following file:

```
Oracle_Home/config/ias.properties
```

If `SSLOnly` is set to true and `OIDport` has an empty value, proceed with Steps 2 through 5.

2. Verify that the non-SSL port for Oracle Internet Directory is enabled and up. If it is not, enable the non-SSL port for Oracle Internet Directory. Using Oracle Directory Manager, take the following steps:
 - a. In the navigator pane, expand **Oracle Internet Directory Servers**, then the *directory server instance*, then **Server Management**.
 - b. Expand either **Directory Server** or **Replication Server**, as appropriate. The numbered configuration sets are listed beneath your selection.
 - c. Select the configuration set that you want to change.
 - d. On the General tab, enter a port number for **Non-SSL port**, if there is not a port number listed.

- e. On the SSL Settings tab page, change the **SSL enabled** field to **Both SSL and Non-SSL**.
 - f. Click **Apply**.
 - g. Restart the server instance.
 3. In the Oracle homes for the other Identity Management components, run the Change Identity Management Services wizard and associate the other Identity Management components to Oracle Internet Directory using the non-ssl port:
 - a. Using the Application Server Control Console, navigate to the Application Server Home page for instance and click the **Infrastructure** link.
 - b. On the Infrastructure page, in the Identity Management section, click **Change**.
 - c. On the Change Identity Management page, specify the **Host name** and, for **Port**, the non-SSL port number.
 - d. Follow the steps in the wizard for supplying the login information.
 4. Verify that the `ias.properties` file contains the following:

```
OIDport=<non-empty_value>
SSLonly=false
```
 5. Proceed with the rest of the procedure as documented in the *Oracle Application Server Administrator's Guide*. After you complete the procedure, you can reenable SSL using the Application Server Control Console's Identity Management Services wizard.

3.2 Documentation Errata

This section describes documentation errata in management documentation. It includes the following topic:

- [Section 3.2.1, "References to OracleAS Web Cache and OracleAS Portal in the Application Server Control Console Online Help"](#)

3.2.1 References to OracleAS Web Cache and OracleAS Portal in the Application Server Control Console Online Help

Application Server Control Console includes references to Oracle Application Server Web Cache and Oracle Application Server Portal. In fact, these two components are not distributed as part of the Oracle Identity Management product.

These references in the Application Server Control Console online help can be ignored.

High Availability

This chapter describes issues related to highly available topologies using the OracleAS Disaster Recovery solution. This chapter contains the following issues:

- [Section 4.1, "General Issues and Workarounds"](#)
- [Section 4.2, "Configuration Issues and Workarounds"](#)
- [Section 4.3, "Documentation Errata and Omissions"](#)

4.1 General Issues and Workarounds

This section describes general issues and workarounds. It includes the following topic:

- [Section 4.1.1, "Problem Performing a Clone Instance or Clone Topology Operation"](#)
- [Section 4.1.2, "OracleAS Guard Release 10.1.2.1.1 Cannot Be Used with Oracle RAC Databases"](#)
- [Section 4.1.3, "OracleAS Guard Returned an Inappropriate Message When It Could Not Find the User Specified Database Identifier"](#)

4.1.1 Problem Performing a Clone Instance or Clone Topology Operation

At the current time, the semantics of an `asgctl` clone topology operation will not clone databases that are outside of the OracleAS home, thus only the default database installed into the OracleAS home by some infrastructure installation types will be cloned. The `asgctl create standby database` command should be used by users not familiar with Oracle Data Guard.

4.1.2 OracleAS Guard Release 10.1.2.1.1 Cannot Be Used with Oracle RAC Databases

OracleAS Guard version shipped with this release is 10.1.2.1.1. This version of OracleAS Guard cannot be used with Oracle RAC Databases. For all other purposes, this OracleAS Guard version is completely supported by Oracle.

To use OracleAS Guard with an Oracle RAC database, it is recommended to use Release 10.1.2.2 stand alone version of OracleAS Guard with this release. OracleAS Guard 10.1.2.2 version (with instructions) is available for download from Oracle OTN as an OracleAS Guard stand alone install, or please contact Oracle Support for further instructions.

4.1.3 OracleAS Guard Returned an Inappropriate Message When It Could Not Find the User Specified Database Identifier

When OracleAS Guard could not find the user specified identifier, an inappropriate error message was returned. If the user had entered the database name rather than the Oracle instance SID, there was no indication that this was the problem.

Now if OracleAS Guard is unable to locate the oratab entry for the user specified database identifier, the following ASG_SYSTEM-100 message now precedes the existing ASG_DUF-3554 message and both messages will be displayed to the console:

```
ASG_SYSTEM-100: An Oracle database is identified by its database unique name (db_
name)
ASG_DUF-3554: The Oracle home that contains SID <user specified identifier> cannot
be found
```

4.2 Configuration Issues and Workarounds

This section describes configuration issues and their workarounds. It includes the following topics:

- [Section 4.2.1, "The asgctl shutdown topology Command Does Not Shut Down an MRCA Database That is Detected To Be of a repCa Type Database"](#)

4.2.1 The asgctl shutdown topology Command Does Not Shut Down an MRCA Database That is Detected To Be of a repCa Type Database

The asgctl shutdown topology command only handles non-database instances. Thus, in a repCA environment when OracleAS Guard detects an instance and determines it to be a repCa type database, its instance is ignored in a shutdown topology operation. Any repCA type database is considered to be managed outside of OracleAS Guard.

4.3 Documentation Errata and Omissions

This section describes documentation errata and omissions. It includes the following topics:

- [Section 4.3.1, "Availability of a Previously Undocumented asgctl Command: create standby database"](#)
- [Section 4.3.2, "Connecting to an OracleAS Guard Server May Return an Authentication Error"](#)
- [Section 4.3.3, "All emagents Must Be Shut Down Before Performing OracleAS Guard Operations"](#)
- [Section 4.3.4, "Procedure to Patch a 10.1.2.0.0 Disaster Recovery Setup with a 10.1.2.1.0 Patchset"](#)
- [Section 4.3.5, "Running Instantiate Topology Across Nodes After Executing a Failover Operation Results in an ORA-01665 Error"](#)
- [Section 4.3.6, "OracleAS Guard Is Unable to Shutdown the Database Because More Than One Instance of Oracle RAC is Running"](#)

4.3.1 Availability of a Previously Undocumented asgctl Command: create standby database

The asgctl create standby database command is not documented. The following information describes this command in more detail.

The syntax for the asgctl create standby database command is as follows:

```
create standby database <database_name> on <remote_host>
```

<database_name> is the primary database unique name used to create the standby database on the remote host system.

<remote_host> is the name of the host system on which the standby database is to be created.

Oracle software and OracleAS Guard software are required to be installed on the node designated as <remote_host>.

The `init.ora` parameter file generated for the standby database is configured assuming a non Oracle RAC enabled standby database. If the standby database is to be Oracle RAC enabled, the following initialization parameters must be defined appropriately:

- cluster_database
- cluster_database_instances
- remote_listener

Users should use this command sparingly and only as needed.

4.3.2 Connecting to an OracleAS Guard Server May Return an Authentication Error

When a user connects to an OracleAS Guard server and gets an authentication error even though the correct user name and password were entered, the user should try to put the following flag in the `dsa.conf` file in the `<ORACLE_HOME>/dsa` directory and try the operation again: `dsa_realm_override=1`.

Note that this DSA configuration file parameter is not documented in the "OracleAS Guard Configuration File Parameters" section of the OracleAS Guard Release Information `readme.txt` file.

4.3.3 All emagents Must Be Shut Down Before Performing OracleAS Guard Operations

Before performing any OracleAS Guard operations, you must shut down the emagents. This operation is required for OracleAS Guard commands that recycle OracleAS services. You can issue the asgctl run command in a script to perform this operation from within OracleAS Guard. See the OracleAS Disaster Recovery chapters in the *Oracle Application Server High Availability Guide* for more information.

Otherwise, for example you may get an "ORA-01093: ALTER DATABASE CLOSE only permitted with no sessions connected" error message.

Shutting down emagents is only described for performing a switchover operation. However, it applies to all OracleAS Guard operations. The documentation will be updated in a future release.

4.3.4 Procedure to Patch a 10.1.2.0.0 Disaster Recovery Setup with a 10.1.2.1.0 Patchset

Assuming you already have an existing Disaster Recovery Setup for a 10.1.2.0.0 production database, follow these conceptual steps to apply a 10.1.2.1.0 Disaster Recovery Patchset:

1. Break the Disaster Recovery setup. Perform an `asgctl failover` command.
2. Apply the patch 10.1.2.1.0.
3. Recreate the Disaster Recovery setup. Perform an `asgctl create standby database` command followed by an `asgctl instantiate topology` command. Alternatively, see the Oracle Data Guard documentation for more information about how to reestablish the standby database.

4.3.5 Running Instantiate Topology Across Nodes After Executing a Failover Operation Results in an ORA-01665 Error

If you attempt to perform an `asgctl instantiate topology` operation immediately following an `asgctl failover` operation, an "ORA-01665: control file is not a standby control file" error message is returned.

To work around this problem, you must first perform an `asgctl create standby database` command to create the standby database on the remote host. See [Section 4.3.1, "Availability of a Previously Undocumented asgctl Command: create standby database"](#) for more information about this previously undocumented `asgctl` command. Also see [Section 4.3.4, "Procedure to Patch a 10.1.2.0.0 Disaster Recovery Setup with a 10.1.2.1.0 Patchset"](#) for more information.

4.3.6 OracleAS Guard Is Unable to Shutdown the Database Because More Than One Instance of Oracle RAC is Running

When you are running OracleAS Guard in an Oracle RAC environment, you should have only one Oracle RAC instance running while performing OracleAS Guard operations. Otherwise, an error will occur where the primary database will complain that it is mounted by more than one instance, which will prevent a shutdown.

For example, when performing an OracleAS Guard create standby database operation in an Oracle RAC environment with more than one Oracle RAC instance running, the following error will be seen:

```
ASGCTL> create standby database orcl1 on stanb06v3
.
.
.
      This operation requires the database to be shutdown. Do you want to
continue? Yes or No
Y
      Database must be mounted exclusive
stanb06v1: -->ASG_DUF-4950: An error occurred on host "stanb06v1" with IP
"141.86.22.32" and port "7890"
stanb06v1: -->ASG_DUF-3514: Failed to stop database orcl1.us.oracle.com.
stanb06v1: -->ASG_DGA-13002: Error during Create Physical Standby:
Prepare-primary processing.
stanb06v1: -->ASG_DUF-3027: Error while executing Creating physical standby
database - prepare phase at step - primary processing step.
```

Oracle Access Manager

This chapter provides information about known issues and workarounds for Oracle Access Manager. The following topics are included:

- [Section 5.1, "General Issues"](#)
- [Section 5.2, "Installation and Upgrade Issues and Workarounds"](#)
- [Section 5.3, "Removal Issues and Workarounds"](#)
- [Section 5.4, "Access System Issues and Workarounds"](#)
- [Section 5.5, "Identity System Workarounds and Issues"](#)
- [Section 5.6, "Directory Issues"](#)
- [Section 5.7, "Documentation Issues"](#)

5.1 General Issues

This section describes the general issues and workarounds. It includes the following topics:

- [Section 5.1.1, "Known Issue With JDK 1.1.7"](#)
- [Section 5.1.2, "The Name "Query Builder" Is Not Always Translated"](#)
- [Section 5.1.3, "Users Can Access Resources After Password Reset Without Logging In"](#)

5.1.1 Known Issue With JDK 1.1.7

There is a known limitation with Java applets in JDK 1.1.7. When used with this release of Oracle Access Manager, applets with non-ASCII data can only be displayed properly on computers with a native-encoded operating system. Setting browser encoding will not work.

If you intend to use non-ASCII data, run Oracle Access Manager on computers with a native-encoded operating system.

5.1.2 The Name "Query Builder" Is Not Always Translated

In this release, the name "Query Builder" has been translated for different language locales in some places, and not in others. The term "Selector" is translated into respective locales everywhere.

5.1.3 Users Can Access Resources After Password Reset Without Logging In

You can enable users to access resources without re-authenticating after resetting a password. This information was omitted from the documentation.

To log users in after changing their password, the change password redirect URL must include `STLogin=%applySTLogin%` as a parameter .

The following is an example of a change password redirect URL that logs the user in:

```
/http://machinename:portnumber/identity/oblix/apps/lost_password_mgmt/bin/lost_password_mgmt.cgi?program=redirectforchangepwd&login=%login%%userid%&backURL=%HostTarget%%RESOURCE%%STLogin=%applySTLogin%&target=top
```

Note that the `STLogin=%applySTLogin%` parameter cannot be used with a form-based authentication scheme.

5.2 Installation and Upgrade Issues and Workarounds

To ensure success when upgrading older releases to Oracle Access Manager 10g (10.1.4.0.1), you must complete all preparation tasks and meet all requirements described in the *Oracle Access Manager Upgrade Guide*. The guide also provides step-by-step instructions that you can follow as you upgrade from releases as early as 5.2 to 10g (10.1.4.0.1).

This section describes the issues and workarounds for installation and upgrade:

- [Section 5.2.1, "Change the Transport Security Mode During Installation"](#)
- [Section 5.2.2, "Special Considerations for adding Language Packs to an Installation area with Space Characters"](#)
- [Section 5.2.3, "iPlanet Server Fails After Tuning"](#)
- [Section 5.2.4, "Oracle Internet Directory Servers Require Tuning After Installation"](#)
- [Section 5.2.5, "Support for DirX Has Been Deprecated"](#)
- [Section 5.2.6, ""Enter Password" String Does Not Display Correctly During Installation"](#)
- [Section 5.2.7, "Uninstalling a Language Pack With a "2" Designation Causes an Error"](#)

5.2.1 Change the Transport Security Mode During Installation

A transport security mode is a method of communication between two points, such as a client and a server. Oracle Access Manager offers the following transport security modes for communication between components, as discussed in the *Oracle Access Manager Installation Guide*:

- **Open:** Communication is not encrypted.
- **Simple:** Communication is encrypted with Oracle Access Manager's internal CA.
- **Cert:** Communication is encrypted with an external CA. With Cert mode, communications are encrypted using TLS v1, and both client and server must present an X.509 certificate (in base64 format) when establishing a connection.

By default, an Oracle Access Manager installation uses Open mode. This applies to directory connections and communication between Oracle Access Manager components, for example, the WebPass and Identity Server. In Open mode, the communication channel is open to eavesdroppers. Oracle recommends that you secure

your network using SSL communication with the directory and Certificate mode across Oracle Access Manager components.

The next release of the *Oracle Access Manager Installation Guide* will include the following recommendation for transport security:

"During installation, Oracle Access Manager components default to Open mode. However, this does not provide secure communication between components such as Identity Servers and WebPass nor Access Server and WebGate, nor for LDAP connections. In Open mode, the communication channel is susceptible to eavesdropping. To provide a secure deployment, Oracle recommends that you choose Certificate (Cert) mode for transport security between Oracle Access Manager components, and SSL-enabled security between Oracle Access Manager components and directory servers."

5.2.2 Special Considerations for adding Language Packs to an Installation area with Space Characters

Adding language packs to an installation directory containing space characters will not be successful. Note that this problem occurs only if both of the following are true:

- The product is installed in a directory containing space characters.
- A language pack is added after the initial installation.

This problem does not occur for language packs that are installed during the initial installation of the product

If you experience this problem, you can manually execute a command-line tool after running the language pack installer.

1. Open the `obupdatelang.log` file in the following directory:

```
<installdir>/oblix/tools/lang_tools
```

2. Navigate to the end of the file and inspect the lines starting with `prog` and `arguments`.

The command that you will run appears following the `prog` statement. The arguments for the command follow the `arguments` statement.

For example the `obupdatelang.log` file will contain statements similar to the following:

```
prog : C:\Program Files\Netpoint\identity\oblix\tools\lang_tools\obupdatelangds
arguments : -c oislp -i C:\Program Files\Netpoint\identity -f C:\Program
Files\Netpoint\identity\oblix\tools\lang_tools\obupdatelang_islp_AR.lst
```

3. Make note of the command and arguments, open a command prompt window, and go to the following directory:

```
C:\Program Files\Netpoint\identity\oblix\tools\lang_tools
```

4. Run the command, modifying the `-i` and `-f` switches so that the paths they specify are enclosed in quotes ("), as shown in the following example:

```
obupdatelangds -c oislp -i "C:\Program Files\Netpoint\identity" -f "C:\Program
Files\Netpoint\identity\oblix\tools\lang_tools\obupdatelangds"
```

5.2.3 iPlanet Server Fails After Tuning

After tuning Oracle Access Manager from the iPlanet administration console, the server fails to work. For example, after changing the number of threads in the native thread pool, the server fails to restart.

Do not use the iPlanet console for tuning. This can cause the server to remove any existing Oracle Access Manager configuration information. Use the following file to load the Oracle Access Manager Web components and retain the tuning parameters:

```
$Web_Server_home\config\magnus.conf
```

5.2.4 Oracle Internet Directory Servers Require Tuning After Installation

After installing Oracle Access Manager against an Oracle Internet Directory, you need to tune the directory to ensure adequate performance when processing search requests and other functions.

Use the following `ldapmodify` command to tune Oracle Internet Directory:

```
ldapmodify -D cn=orcladmin -w <adminPsswd> -h <host> -p <port> << eof
dn: cn=dsacnfig, cn=configsets, cn=oracle internet directory
changetype: modify
add: orclinmemfiltprocess
orclinmemfiltprocess:
(|(obuseraccountcontrol=activated)(!(obuseraccountcontrol=*))
orclinmemfiltprocess:
(|(!(obuseraccountcontrol=*)) (obuseraccountcontrol=activated))
eof
```

Where *<host>* and *<port>* refer to the Oracle Internet Directory installation host and port.

5.2.5 Support for DirX Has Been Deprecated

Support for the Siemens DirX directory server has been deprecated in this release. However, options to select and configure DirX appear on installation screens and on Identity System and Access System configuration pages in the System Console.

Ignore all Siemens DirX options in the product installer and configuration user interface.

5.2.6 "Enter Password" String Does Not Display Correctly During Installation

When running the installer in console mode using some language packs, the prompt for entering the LDAP password may be garbled.

The solution that works in most cases is to install all of the language support available on the computer where the Oracle Access Manager installation is being performed. Be sure all of the fonts that are required for the language are installed. Log in to the machine locally and choose the language to display on the login screen.

5.2.7 Uninstalling a Language Pack With a "2" Designation Causes an Error

You may be unable to remove (uninstall) a language pack with a designation 2. For example, you may not be able to uninstall using `_uninstAccessLP_ko-kr2` after using `_uninstAccessLP_ko-kr` (and vice versa).

The following information is a workaround for this problem.

Complete the following steps. Korean (ko-kr) is used as the language in the following example; your environment will vary:

1. Copy `_jvmAccessLP_ko-kr` to a backup folder.
2. Run `uninstaller.exe` under `_uninstAccessLP_ko-kr2`.
It should automatically remove both `_jvmAccessLP_ko-kr` and `_uninstAccessLP_ko-kr2`.
3. Copy `_jvmAccessLP_ko-kr` back to the original `Component_install_dir/WebComponent/access/` directory.
4. Run `uninstaller.exe` under `_uninstAccessLP_ko-kr`.
It should automatically remove `_jvmAccessLP_ko-kr` and `_uninstAccessLP_ko-kr`.
5. Restart the Identity Server and Access Server and Web component Web servers.

5.3 Removal Issues and Workarounds

This section describes removal issues and workarounds. It includes the following topic:

- [Section 5.3.1, "Removing Language Packs"](#)
- [Section 5.3.2, "Removing the Default Administrator Language"](#)
- [Section 5.3.3, "Removing Components and Reinstalling"](#)

5.3.1 Removing Language Packs

You must stop and restart servers after uninstalling language packs. For example, suppose you have an Identity Server and a WebPass installed with a Korean Language Pack. After uninstalling the Korean language pack on each component host, you must stop and restart both the Identity Server Service and the WebPass Web server instance. This will re-initialize corresponding components with the proper language support.

For more information about installing and removing language packs, see the *Oracle Access Manager Installation Guide*.

5.3.2 Removing the Default Administrator Language

Removing (uninstalling) the language pack associated with the default Administrator language that was chosen during installation is not supported. An error occurs if you remove this language pack and you may not be able to gain access to the Identity and Access Systems.

To recover, see the discussion of language pack issues in the Troubleshooting chapter of the *Oracle Access Manager Installation Guide*.

5.3.3 Removing Components and Reinstalling

If a component installation terminates (or is terminated by you) after component files were extracted to the designated installation directory, you should run the Uninstaller for that component and then remove the installation directory before attempting to reinstall in the same location. If you simply delete the installation directory and attempt to reinstall the component in the same location, the `vpd.properties` file is left in an inconsistent state and reinstalling will not work.

For example, suppose you terminate a WebGate installation after component files were extracted, then you remove the installation directory manually rather than using the WebGate uninstaller. In this case, the extracted files are deleted but the `vpd.properties` file is not. This leaves the `vpd.properties` file in an inconsistent state that prevents successful installation.

For more information about uninstalling, see the *Oracle Access Manager Installation Guide*.

5.4 Access System Issues and Workarounds

This section describes issues and workarounds for the Access System. It includes the following topics:

- [Section 5.4.1, "WebGate Diagnostics URL Incorrectly Report the Access Server Is Down"](#)
- [Section 5.4.2, "WebGate Is Unable to Connect to Its Associated Access Server"](#)
- [Section 5.4.3, "Memory Usage Rises After Configuring a Directory Server Profile"](#)
- [Section 5.4.4, "The Passthrough Challenge Parameter Does Not Work on a Domino Web Server"](#)
- [Section 5.4.5, "Steps for Integrating the Access System with OracleAS Single Sign-On 10.1.2.0.2"](#)
- [Section 5.4.6, "Return Type Parameters Are Case-Sensitive in This Release"](#)
- [Section 5.4.7, "Single Sign-On with Oracle Identity Management Fails"](#)

5.4.1 WebGate Diagnostics URL Incorrectly Report the Access Server Is Down

As discussed in the *Oracle Access Manager Access Administration Guide*, the WebGate diagnostics URL reports the status of the Access Server or Servers to which the WebGate is connected. In some cases, the landing page for this URL can report that the Access Server or Servers are down when in the servers actually are running.

This problem occurs when the number of Access Servers that are associated with a WebGate is higher than the value of WebGate's Maximum Connections property. In this type of situation, the WebGate diagnostics page displays a status of Down for all Access Servers that exceed the Maximum Connections irrespective of their status.

For example, suppose that you set the Maximum Connections value for WebGate A to 1 and you associate three Access Servers with it, AAA1, AAA2, and AAA3. The diagnostics page will indicate that AAA1 is up and AAA2 and AAA3 are down. If AAA1 is down, the page will indicate that AAA2 is up and AAA3 is down.

To fix this problem, ensure that there are more connections configured between the WebGate and the Access Servers than there are Access Servers.

To configure the Maximum Connections field:

1. In the Access System Console, click **Access System Configuration**, then click **AccessGate Configuration**.

The Search for AccessGates page appears.

2. Enter search criteria on this page, or click the **All** button.
3. Click **Go**.

AccessGates that match your search criteria are listed on this page.

4. Click the link for a WebGate.
The Details for AccessGate page appears.
5. Click **Modify**.
The Modify AccessGate page displays the settings for this WebGate.

5.4.2 WebGate Is Unable to Connect to Its Associated Access Server

If you have installed a WebPass or a WebGate on IIS 6 and enabled logging, the WebPass or WebGate may be unable to connect to its associated Identity or Access Server. In particular, this problem occurs when you send logs to an MPFileLogWriter. It does not occur when you send logs to a FileLogWriter.

The problem occurs with the MPFileLogWriter when there is no anonymous user with access to the directory that contains the log files. MPFileLogWriter uses a file named `<logfile name>.lck` to synchronize multiple processes that write to the corresponding log file. The MPFileLogWriter write-locks the.lck file before writing to the oblog.log file.

Configure an anonymous user with access to the directory that contains the log files. In some circumstances, the user context used to acquire the write-lock will be the IIS Anonymous web user. By default, this user is named `IUSR_<computer name>`, but you can configure any anonymous user for this purpose.

5.4.3 Memory Usage Rises After Configuring a Directory Server Profile

After configuring a directory server profile, the memory usage for the Access Server or Policy Manager becomes too high.

When you configure a directory server profile, you are prompted to provide a maximum session time. The default value for the session time is 0 (unlimited). This may cause a performance issue, because the size of the caches for LDAP connections to the Access Server and Policy Manager increase over time. Oracle Access Manager does not control these caches directly.

To prevent the cache size from causing a performance problem, set the value of the Maximum Session Time (Minutes) for the directory server profile to a finite value, for example, 10 hours, as follows:

1. From the Identity System Console click System Configuration, then click Directory Profiles.
2. Click the link for the profile that you want to modify.
3. In the Max. Session Time (Min.) field, set the value to 600.

5.4.4 The Passthrough Challenge Parameter Does Not Work on a Domino Web Server

There is a problem with specifying the `passthrough: challenge` parameter in some form-based authentication schemes. In particular, this parameter does not work on a Domino Web server when using the POST method for form-based login.

There is no solution for this problem at this time.

5.4.5 Steps for Integrating the Access System with OracleAS Single Sign-On 10.1.2.0.2

The *Oracle Access Manager Integration Guide* provides a chapter on integrating the Access System's single sign-on with OracleAS Single Sign-On. In addition to following the information in the Oracle Access Manager Integration Guide, you must also

complete the following procedure to integrate the Access System with OracleAS Single Sign-On 10.1.2.0.2.

To configure the integration:

1. Follow the steps in the chapter on integrating the Access System's single sign-on with OracleAS Single Sign-On in the Oracle Access Manager Integration Guide.
2. In the Access System Console, click **System Configuration**, then click **Server Settings**, and configure the following logout URL:

```
http://[host.domain]:[port]/pls/orasso/ORASSO.wvssso_app_admin.ls_logout?p_done_
url=http%3A%2F%2F[host.domain]%3A[port]
```

URL-encode the `p_done_url` value.

See the *Oracle Application Server Single Sign-On Administrator's Guide* for release 10.1.2.0.2 for details on configuring the logout link for single sign-on. A sample JSP that can be used for this purpose is included at the end of this release note.

3. If you use the sample JSP, go to the Access System Console, click **Access System Configuration**, then click **AccessGate Configuration**, and include the following in the **LogOutURLs** parameter for every WebGate in your environment:

```
/access/oblix/lang/en-us/style2/oblixlogo.gif
```

The following is a sample `logout.jsp` file:

```
<!-- Copyright (c) 1999, 2003, Oracle. All rights reserved. -->
<%@page autoFlush="true" session="false"%>
<%
// Declare English Message Strings
String msg1 = "Single Sign-Off";
String msg2 = "Application Name";
String msg3 = "Logout Status";
String msg4 = "ERROR: The return URL value not found.";
String msg5 = "ERROR: Logout URL for partner applications not found.";
// Get the user language preference
String userLocaleParam = null;
java.util.Locale myLocale = null;
// Get the user locale preference sent by the SSO server
try
{
userLocaleParam = request.getParameterValues("locale")[0];
}
catch(Exception e)
{
userLocaleParam = null;
}
if( (userLocaleParam == null) || userLocaleParam.equals("") )
{
myLocale = request.getLocale();
}
else
{
if(userLocaleParam.indexOf("-") > 0 )
{
// SSO server sent the language and territory value (e.g. en-us)
myLocale = new java.util.Locale(userLocaleParam.substring(0, 2),
userLocaleParam.substring(3, 5));
}
else
{
```

```

// SSO server sent only the language value (e.g. en)
myLocale = new java.util.Locale(userLocaleParam, "");
}
}
// The following two lines will be used only for the Multilingual support
with
// proper resource bundle class supplied
// java.util.ResourceBundle myMsgBundle
// = java.util.ResourceBundle.getBundle("MyMsgBundleClassName", myLocale);
// Get the message string in the appropriate language using the message key.
// Use this string to display the message in this page.
// String msg = myMsgBundle.getString("mesg_key");
%>
<html>
<body bgcolor="#FFFFFF">
<h1><%=msg1%></h1>
<%
String done_url = null;
int i = 0;
// Get the return URL value
try
{
done_url = request.getParameterValues("p_done_url")[0];
}
catch(Exception e)
{
done_url = "";
}
// Get the application name and logout URL for each partner application
try
{
%>
<b> <%=msg2%> <%=msg3%> </b>
<br>
// Substitute an actual host, domain, and port for
myhost.us.mydomain.com:7777
// that points to the WebGate.

<%
for(;;)
{
i++;
String app_name = request.getParameterValues("p_app_name"+i)[0];
String url_name = request.getParameterValues("p_app_logout_url"+i)[0];
%>
<%=app_name%>


<br>
<%
}
}
catch(Exception e)
{
if(done_url == null)
{
%>
<%=msg4%> <br>

```

```
<%  
  }  
  if (i>1)  
  {  
  %>  
<br> <a href="<%=done_url%>">Return</a>  
<%  
  }  
  else  
  {  
  %>  
<%=msg5%><br>  
<%  
  }  
  }  
  %>  
</body>  
</html>
```

5.4.6 Return Type Parameters Are Case-Sensitive in This Release

In this release, certain authentication and authorization action parameters are case-sensitive. For example, in previous releases you could set up a policy domain in the Policy Manager and include an authentication or authorization action that uses the `cookie` parameter. In this release, if you do this a cookie will not be set for the action. You can test this configuration issue by accessing the protected resource from a browser and monitoring the HTTP traffic to the browser.

The workaround for this issue is to use the following action type parameters in policies, preserving the case:

- `Cookie`
- `HeaderVar`

5.4.7 Single Sign-On with Oracle Identity Management Fails

If you attempt to implement single sign-on between Oracle Identity Management 9.0.2 and Oracle Access Manager 10.1.4.0.1, you may encounter a problem. If you configure authentication using HTTP headers instead of cookies, the headers are only supported if they use ASCII text. To integrate an HTTP header with non-ASCII data, you need to install a patch. Contact Oracle Support and ask for a patch for bug 5552617.

5.5 Identity System Workarounds and Issues

This section describes issues and workarounds for the Identity System. It includes the following topics:

- [Section 5.5.2, "Identity System Deletes a User Entry When an RDN is Modified"](#)
- [Section 5.5.3, "Auditing for the Identity System Ceases to Work"](#)
- [Section 5.5.4, "Identity Server Crashes if It Cannot Find a Style Sheet"](#)
- [Section 5.5.5, "WebPass Is Unable to Connect to Its Associated Identity Server"](#)
- [Section 5.5.6, "Memory Usage Rises for an Identity Server After Configuring a Directory Server Profile"](#)
- [Section 5.5.7, "Errors Are Found in the HTTP Logs After Setting Up the Identity System"](#)

- [Section 5.5.8, "Reports With Non-ASCII Characters Are Not Imported Correctly in Excel"](#)
- [Section 5.5.9, "Translation of Tab Names May be Incomplete"](#)
- [Section 5.5.10, "Non-ASCII Values for Certain Display Types Are Corrupted in the Identity System Console"](#)
- [Section 5.5.11, "Data Is Lost When Saving an Object Profile in Org. Manager"](#)

5.5.1 Identity System Deletes a User Entry When an RDN is Modified

The Identity System deletes user entries when you attempt to modify an RDN attribute value. The RDN is the leftmost attribute in a DN. Typically, the RDN attribute is `cn` or `Full Name`.

This problem occurs when you use Oracle Internet Directory as the back-end repository.

To fix this problem:

1. Edit the file `ldapreferentialintegrityparams.xml` in the following directory:

```
Identity_Server_installation_directory\identity\oblix\data\common
```

2. Change the value of the parameter `referential_integrity_using` from `oblix` to `ds`, as follows:

```
<NameValPair ParamName="referential_integrity_using" Value="ds"/>
```

3. Save the file.
4. Restart the Identity Server for the changes to take effect.
You should be able to modify the RDN attribute value without any problem.
5. If you have multiple instances of the Identity Server installed, make this change to every instance of the Identity Server.

5.5.2 Identity System Deletes a User Entry When an RDN is Modified

The Identity System deletes user entries when you attempt to modify an RDN attribute value. The RDN is the leftmost attribute in a DN. Typically, the RDN attribute is `cn` or `Full Name`.

This problem occurs when you use Oracle Internet Directory as the back-end repository.

To fix this problem:

1. Edit the file `ldapreferentialintegrityparams.xml` in the following directory:

```
Identity_Server_installation_directory\identity\oblix\data\common
```

2. Change the value of the parameter `referential_integrity_using` from `oblix` to `ds`, as follows:

```
<NameValPair ParamName="referential_integrity_using" Value="ds"/>
```

3. Save the file.
4. Restart the Identity Server for the changes to take effect.

You should be able to modify the RDN attribute value without any problem.

5. If you have multiple instances of the Identity Server installed, make this change to every instance of the Identity Server.

5.5.3 Auditing for the Identity System Ceases to Work

When you have auditing configured for multiple Real Application Cluster (RAC) databases, auditing will work correctly for a while. However, after shutting down and restarting a RAC instance other than the one that was shut down the last time, auditing stops.

To avoid this issue, restart the Identity Server.

5.5.4 Identity Server Crashes if It Cannot Find a Style Sheet

After you customize a style sheet, the Identity Server crashes or issues an error about a Win32 exception being caught.

If you have used backslash characters as path separators in your stylesheets in `xsl:include` constructs, replace the backslashes with forward slash characters. For example, you would want to change the following:

```
<xsl:include href=".\\style.xsl" />
```

To this:

```
<xsl:include href="./style.xsl" />
```

5.5.5 WebPass Is Unable to Connect to Its Associated Identity Server

If you have installed a WebPass on IIS 6 and enabled logging, the WebPass may be unable to connect to its associated Identity Server. In particular, this problem occurs when you send logs to an `MPFileLogWriter`. It does not occur when you send logs to a `FileLogWriter`.

The problem occurs with the `MPFileLogWriter` when there is no anonymous user with access to the directory that contains the log files. `MPFileLogWriter` uses a file named `<logfile name>.lck` to synchronize multiple processes that write to the corresponding log file. The `MPFileLogWriter` write-locks the `.lck` file before writing to the `oblog.log` file.

Configure an anonymous user with access to the directory that contains the log files. In some circumstances, the user context used to acquire the write-lock will be the IIS Anonymous web user. By default, this user is named `IUSR_<computer name>`, but you can configure any anonymous user for this purpose.

5.5.6 Memory Usage Rises for an Identity Server After Configuring a Directory Server Profile

After configuring a directory server profile, the memory usage for the Identity Server becomes too high.

When you configure a directory server profile, you are prompted to provide a maximum session time. The default value for the session time is 0 (unlimited). This may cause a performance issue, because the size of the caches for LDAP connections to the Identity Server increase over time. Oracle Access Manager does not control these caches directly.

To prevent the cache size from causing a performance problem, set the value of the Maximum Session Time (Minutes) for the directory server profile to a finite value, for example, 10 hours, as follows:

1. From the Identity System Console click System Configuration, then click Directory Profiles.
2. Click the link for the profile that you want to modify.
3. In the Max. Session Time (Min.) field, set the value to 600.

5.5.7 Errors Are Found in the HTTP Logs After Setting Up the Identity System

After completing the process described in the *Oracle Access Manager Installation Guide* chapter on setting up the Identity System, if you installed Japanese language packs you may see errors in the following log files:

```
ORACLE_OHS_HOME/Apache/Apache/logs/error_log.*
```

Where *ORACLE_OHS_HOME* is the installation directory for the Oracle HTTP Server. These errors have a format similar to the following example:

```
[Sun Jun  4 16:31:06 2006] [error] [client 12.345.678.99] [ecid:
1149406266:12.345.678.82:28663:0:3,0] File does not exist:
/home/as1014/as1014coreid/COREid/webcomponent_3/identity/oblix//apps/admin/
bin/com/oblix/data/resource.class
```

These errors have no impact, and can be ignored.

5.5.8 Reports With Non-ASCII Characters Are Not Imported Correctly in Excel

After modifying and exporting object class attributes, a `report.csv` file is created. In the Japanese Locale or Simplified Chinese Locale, there are encoding problems due to a Microsoft Excel limitation that cannot process CSV files containing data in UTF-8 encoding.

To process the exported report, complete the process below.

1. Rename `report.csv` to `report.txt`.
2. Open `report.txt` Excel 2003 (Excel 2000 does not support UTF-8 encoding).
3. In the text import wizard, choose encoding as UTF- 8 and comma as the field separator.
4. Click Finish.

5.5.9 Translation of Tab Names May be Incomplete

In multi-language environments, Configuration tab names in the Identity System Console (User Manager Configuration, Group Manager Configuration, Org. Manager Configuration) may be only partially translated. Only the word "Configuration" may be translated, not the application name before it.

For example, when viewing the Identity System Console using a Japanese browser, the application name "User Manager" on the User Manager Configuration tab is not translated. However in Simplified Chinese, the complete name "User Manager Configuration" is translated.

There is no solution for this problem at this time.

5.5.10 Non-ASCII Values for Certain Display Types Are Corrupted in the Identity System Console

In the Identity System Console, the display names that appear as values for items in the list of display types (radio button, checkbox, and so on) may be corrupt due to a known limitation with Java Applets and internationalized characters. The browser's JVM displays only those characters that are in the current locale. Internationalized characters are displayed correctly in applets only if you have set the browser to the same locale.

Set the browser to the locale used when setting the display name value.

5.5.11 Data Is Lost When Saving an Object Profile in Org. Manager

When saving new or modified information in an object profile in the Org. Manager application, some of the data is lost. This problem occurs in Org. Manager tabs that do not contain any panels.

To ensure that there is no loss of data when modifying object profiles in Org. Manager, you should configure at least one panel for the tab. This panel should contain the same attributes as the Header Panel for the tab.

For example, if the header panel contains two attributes named Location Title and Location Name, you would do the following:

1. From the Identity System landing page, select the Identity System Console.
2. Click Org. Manager Configuration.
3. Click Tabs.
4. Click the link for the tab where you want to add panels.
5. Click View Object Profile.
6. Click Configure Panels.
7. Click Create.
8. On the Create Panel page, provide a panel name and add the Location Title and Location Name attributes.

5.6 Directory Issues

This section describes issues and workarounds for the directory. It includes the following topics:

- [Section 5.6.1, "Error "There Is No Profile Configured for this Kind of Object""](#)
- [Section 5.6.2, "Issues With the Display of Messages in Some Languages"](#)
- [Section 5.6.3, "Support for eDirectory 8.7.3"](#)

5.6.1 Error "There Is No Profile Configured for this Kind of Object"

In Oracle Internet Directory, the orcladmin user (`dn: cn=orcladmin`) can be thought of as a pseudo user with administrative privileges. There is no LDAP entry corresponding to this user in Oracle Internet Directory. This user is part of special groups that are created in Oracle Internet Directory. The Identity Server requires that every user exist as an independent entry in the directory. When these special groups are viewed or modified using Group Manager, you may see following message "There is no profile configured for this kind of object."

If you have this issue, view and update these special Oracle Internet Directory groups using the Oracle Directory Manager application.

Note that there are some special groups in Oracle Internet Directory that exhibit cyclic behavior. Using Oracle Directory Manager to manage these groups is recommended, not the Group Manager or the Identity Server.

5.6.2 Issues With the Display of Messages in Some Languages

There may be an issue with the display of messages for some installations of Oracle Access Manager with Oracle Internet Directory using a native character set. For some supported languages in these environments, messages in the Oracle Access Manager message catalog that are not compatible with the native character set are not displayed properly.

Use the AL32UTF8 character set for Oracle Internet Directory instead of the native character set for the language.

5.6.3 Support for eDirectory 8.7.3

When conducting searches using Novell eDirectory 8.7.3, attribute access controls and searchbase filters do not work as expected. For example, using eDirectory 8.7.3, you can configure filters to return organizational units (ou's) below the top node of the DIT, as follows:

```
(&(objectclass=*)(!(|(objectclass=oblixconfig)(objectclass=oblixlocation)(objectclass=genSiteOrgPerson)(objectclass=genSiteGroup)))(objectclass=*))
```

However, these searches return information that you were trying to exclude. For example, users may be returned.

To workaroud this issue, apply the eDirectory patch 8.7.3.7. See the following URLs for details:

<http://www.novell.com>

http://support.novell.com/servlet/downloadfile?file=/uns/ftf/edir8737ftf_1.exe

5.7 Documentation Issues

This section describes issues and workarounds for documentation and online help. It includes the following topics:

- [Section 5.7.1, "Reference to Oracle Internet Directory Is Needed in Installation Preparation Checklist"](#)
- [Section 5.7.2, "Help Mentions WebGateStatic.lst But No Such File Exists"](#)
- [Section 5.7.3, "The obEnableCredentialCache Credential Mapping Parameter Is Misspelled"](#)
- [Section 5.7.4, "Warning Regarding Retrieving Authorization Data From an External Source"](#)
- [Section 5.7.5, "Active Directory MaxPageSize Parameter Stated as PageSize Parameter"](#)
- [Section 5.7.6, "Missing Parameter in globalparams.xml Documentation"](#)

5.7.1 Reference to Oracle Internet Directory Is Needed in Installation Preparation Checklist

In the next version of the *Oracle Access Manager Installation Guide*, Chapter 2, "Preparing for Installation" Table 2-3 will include Oracle Internet Directory in the Installation Preparation Checklists.

5.7.2 Help Mentions WebGateStatic.lst But No Such File Exists

Some language versions of the online help for the Access System contains an obsolete reference to a `WebGateStatic.lst` file, as follows:

"To ensure that the WebGate logs out users from Identity and Access applications when they click the Logout button, set the `LogoutUrls` parameter in `WebGateStatic.lst` to the same value as the SSO Logout URL. `WebGateStatic.lst` is located in

```
WebGate_install_dir/oblix/apps/Webgate/
```

As of version 10.1.4, the `WebGateStatic.lst` file is no longer present. Various parameters that were set in `WebGateStatic.lst` are now defined in the Access System Console.

The following procedure describes how to configure the `LogoutURLs` parameter. See the *Oracle Access Manager Access Administration Guide* for details.

To set the `LogoutUrls` parameter:

1. Launch the Access System Console and click Access System Configuration.
2. Click AccessGate Configuration in the left navigation pane.
3. Conduct a search for existing AccessGates and click the link for the AccessGate that you want to modify.
4. Modify the `LogoutURLs` parameter.

5.7.3 The obEnableCredentialCache Credential Mapping Parameter Is Misspelled

In the *Oracle Access Manager Access Administration Guide* chapter on configuring authentication, the `obEnableCredentialCache` parameter is misspelled as `EnableCredentialCache`.

Use the correct spelling, "`obEnableCredentialCache`" when configuring this parameter.

5.7.4 Warning Regarding Retrieving Authorization Data From an External Source

As described in the *Oracle Access Manager Access Administration Guide*, an authorization scheme can obtain data from an external source. This data is passed to a custom authorization plug-in. By obtaining external data (usually in the form of information about the user) authorization decisions can be made dynamically, based on user input.

For example, if a user goes to a form to purchase an item for \$1000, this \$1000 amount can be dynamically evaluated against a limit—perhaps stored in a database—to determine if the purchase is authorized.

The process of retrieving authorization data from an external source is sometimes known as a reverse action.

Note that when creating an authorization plug-in that uses a reverse action, the calls to retrieve reverse actions will not fail if no reverse actions are present. For example, the

following returns NULL for a list if there is no `user-agent` value in `RequestContext`:

```
ObASPluginList_t list =
pFnBlock->GetDataFn(pInfo->RequestContext, "user-agent");
```

Plug-ins should check if the data list returned for a reverse action (or anything else) is NULL before using it to retrieve individual data values. Even with a new Access Server, this situation could occur if the client did not specify a value for a reverse action.

This information will be added to the Authorization Plugin API documentation.

5.7.5 Active Directory MaxPageSize Parameter Stated as PageSize Parameter

The discussion on "Oracle Access Manager ADSI Configuration Files", in the *Oracle Access Manager Identity and Common Administration Guide*, Appendix B, Table B-2 Parameters and Values in `adsi_params` Files includes two `pagesize` parameter descriptions as follows:

- `pageSize`: Page size of results that ADSI request from the server.
- `pageSize`: Setting the `pageSize` value to a finite value (the default is 0) turns off LDAP referrals. This can improve performance when client applications perform directory searches.

Correction: The second `pageSize` parameter in the table will refer to the `MaxPageSize` parameter.

5.7.6 Missing Parameter in `globalparams.xml` Documentation

The following information has been added to the *Oracle Access Manager Customization Guide*, and related notes have been added to *Oracle Access Manager Identity and Common Administration Guide*.

The parameter `excludeOCsForTreeInApplet` specifies the list of object classes whose objects are excluded from display in the Identity System. For example, if you remove the group object class item from the list, the group objects will be visible in the Identity System applications.

By default, the Identity System does not display every object and attribute in the directory. This parameter enables you to expose object classes in the Identity System applications that would otherwise be hidden.

Oracle Application Server Single Sign-On

This chapter provides information about known issues and workarounds for Oracle Application Server Single Sign-On (OracleAS Single Sign-On). The following topics are included:

- [Section 6.1, "Installation, Installation and Upgrade Issues"](#)
- [Section 6.2, "General Issues"](#)

6.1 Installation, Installation and Upgrade Issues

This section describes the following issues and workarounds related to installation and upgrade:

- [Section 6.1.1, "Directory Considerations During Installation"](#)
- [Section 6.1.2, "Directory Considerations After Installation"](#)
- [Section 6.1.3, "Identity Management Grid Control Considerations During Uninstallation"](#)

6.1.1 Directory Considerations During Installation

You must perform the following steps when installing Oracle Application Server 10.1.4.0.1 Identity Management infrastructure components in an environment that uses an Identity Management High Availability (IMHA) Oracle Internet Directory LDAP cluster with a load balancing router. Failure to perform these steps can cause issues during installation.

This should also be the case for all Identity Management mid-tier installations in a distributed configuration.

To install when using an IMHA Oracle Internet Directory LDAP cluster with a load balancer or virtual server:

1. Prior to starting the installation, ensure that the load balancing router or Oracle Internet Directory virtual server sends all traffic to just one active Oracle Internet Directory instance for the duration of the installation process.

For example, you can configure for affinity (IP-based) routing to ensure that traffic from one IP address is always routed to the same destination.

2. After installation is complete, you can reconfigure your load balancer to use any routing algorithm that you want.

6.1.2 Directory Considerations After Installation

After you install and configure an OracleAS Cluster (Identity Management) environment, Application Server Control incorrectly indicates that some of the Identity Management components are down and not available. To remedy this problem, stop and then start the Application Server Control.

See Also: "Starting and Stopping the Application Server Control" in the *Oracle Application Server Administrator's Guide*

6.1.3 Identity Management Grid Control Considerations During Uninstallation

After uninstalling the Identity Management Grid Control plug-in for Oracle Management Service (Management Service), you must create a new configuration file in the Management Service Oracle home directory. Failure to create this file can cause problems after uninstalling the plug-in. The file enables Oracle Enterprise Manager 10g Grid Control (Grid Control) to find the configuration class for specific single sign-on monitoring pages. These pages are used for default Grid Control Management Service installations that do not have Identity Management Grid Control 10.1.4IM.

To avoid issues after uninstalling the Identity Management Grid Control Management Service plug-in:

1. Open a text editor and create a file with the following contents:

```
<consoleConfig>
  <integration name="oracle_sso_server"
    class="oracle.oimcontrol.sso.em.SSOIntegration"/>
</consoleConfig>
```

2. Save the file in the following location:

```
$ORACLE_HOME/j2ee/OC4J_EM/applications/em/em/WEB-INF/config/sso_server_intg.xml
```

3. Restart the Management Service server.

6.2 General Issues

This section describes the following general issues and workarounds:

- [Section 6.2.1, "A "Host Unavailable" Entry Appears on Non-English Monitoring Pages"](#)
- [Section 6.2.2, "Dynamic Global Logout Directives Must Pass the String "Oracle SSO""](#)
- [Section 6.2.3, "Multilevel Authentication Configuration May or May Not Require a Port Number"](#)

6.2.1 A "Host Unavailable" Entry Appears on Non-English Monitoring Pages

This bug applies only to the monitoring pages for single sign-on in Grid Control.

In browsers that are configured for non-English languages (for example, `ja`, `zh_CN`, `zh_TW`, `ko_KR`, or `fr`), an entry labeled "HOST Unavailable" is displayed in the general section of the Single Sign-On Service monitoring home page. This string appears in the language configured for the browser.

The "HOST Unavailable" entry is a link. If you click this link, the browser displays the message, "Error finding target UNAVAILABLE from the repository. The target does not exist or you may not have the access to the target."

You can safely ignore this error and its associated link.

6.2.2 Dynamic Global Logout Directives Must Pass the String "Oracle SSO"

If you use `mod_osso` for dynamic directive-based global logout, you must pass the string `"Oracle SSO"` as the response error message. The following is an example of a properly constructed directive:

```
request.getSession().invalidate();
response.setHeader("Osso-Return-Url", redirectURL);
response.sendError(470, "Oracle SSO");
```

If any string other than `"Oracle SSO"` is passed as the parameter to `sendError`, global logout does not occur.

6.2.3 Multilevel Authentication Configuration May or May Not Require a Port Number

In the current *OracleAS Single Sign-On Administrators Guide* section on multilevel authentication, the instructions indicate that you must include a port number when configuring an authentication level. However, if default ports are being used in the URL, you can omit the port number.

The following is the correct Step 2 of the procedure for configuring multilevel authentication:

Assign authentication levels to the root URLs of the two partner applications:

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

Be sure to include the backslash after the domain name.

If the URL of the partner application being called uses the default SSL or non-SSL port, the port is not specified in the URL. If this is the case, when defining the root URL of the partner application you do not have to include `:port`.

For example, suppose the following URLs are called for a partner application:

```
http://pa1.mydomain.com/partner application
https://pa2.mydomain.com/parnter application
```

In the `policy.properties` file, the following root URLs would be used:

```
pa1.mydomain.com = HighSecurity
pa2.mydomain.com = MediumSecurity
```

Oracle Identity Federation

This chapter describes issues associated with Oracle Identity Federation. It includes the following topics:

- [Section 7.1, "General Issues and Workarounds"](#)
- [Section 7.2, "Configuration Issues and Workarounds"](#)
- [Section 7.3, "Documentation Errata"](#)

7.1 General Issues and Workarounds

This section describes general issues and workarounds. It includes the following topics:

- [Section 7.1.1, "Credential Re-entry When Accessing a SiteMinder Protected Resource"](#)
- [Section 7.1.2, "Reauthentication after Session Timeout with OracleAS Single Sign-On and SAML 1.x or WS-Federation"](#)
- [Section 7.1.3, "Attribute Sharing with the Microsoft Internet Information Server"](#)
- [Section 7.1.4, "Redirection Loops with Oracle Access Manager"](#)
- [Section 7.1.5, "Truncated Text in Japanese Version of Oracle Universal Installer"](#)
- [Section 7.1.6, "Unused Assertion Profile With Invalid Attribute Mapping Can Cause SSO Failure"](#)
- [Section 7.1.7, "Signed SAML 1.0 Assertions Can Cause SSO Failures"](#)
- [Section 7.1.8, "Encrypting Network Connections"](#)
- [Section 7.1.9, "Spurious Certificate Verification Failure in Debug Log"](#)

7.1.1 Credential Re-entry When Accessing a SiteMinder Protected Resource

As of this release, if a user enters credentials to access a resource protected by SiteMinder, and subsequently tries to perform a single sign-on with the same browser using protocols supported by Oracle Identity Federation, the user is prompted to enter credentials a second time.

7.1.2 Reauthentication after Session Timeout with OracleAS Single Sign-On and SAML 1.x or WS-Federation

This issue concerns a scenario where Oracle Identity Federation is used as a service provider, OracleAS Single Sign-On is the user data store and an OracleAS Single

Sign-On session is created for a federated user using SAML 1.x or WS-Federation. When that session expires, the service provider's Oracle Identity Federation server tries to reauthenticate the session using SAML 2.0. If SAML 2.0 is not enabled on the service and identity providers, the reauthentication will fail, typically with a 500 Internal Server Error.

This problem can be avoided by configuring OracleAS Single Sign-On. Open the `ORACLE_HOME/sso/conf/policy.properties` file and protect all the partner applications with the default SSO server authentication plugin; configure the SASSO authentication plugin to have a higher security level than the OracleAS Single Sign-On server plugin.

With this configuration, when a user authenticated by SAML 1.x or WS-Federation protocol accesses a resource protected by OracleAS Single Sign-On, and the session times out, the user will be redirected to the OracleAS Single Sign-On server for local authentication instead of seeing an error from Oracle Identity Federation or an incorrect IdP.

7.1.3 Attribute Sharing with the Microsoft Internet Information Server

The attribute sharing feature cannot be used with Microsoft Internet Information Servers (IIS) with Oracle Access Manager WebGate agents installed. For this feature an authentication plugin sets an HTTP header with the SubjectDN from the client's X.509 certificate, and an authorization plugin retrieves the header to initiate a SAML attribute query. However, because of the way the IIS WebGate performs SSL client certificate authentication, the SubjectDN header cannot be retrieved by the authorization plugin. In this case the following error is reported at the user's browser:

```
Oracle Access Manager Operation Error Access to the URL
<targetURL> has been denied for user <OblixAnonymous user DN>.
```

Also, the following error messages are written to the `OBACCESS_INSTALL/access/oblix/config/logs/authz_attribute_plugin_log.txt` file:

```
SubjectDN header ObNullString
```

```
and
```

```
SubjectDN is missing. Assume local user and return Continue
```

7.1.4 Redirection Loops with Oracle Access Manager

When Oracle Identity Federation is used as an identity provider with the Oracle Access Manager user data store, a user initiating additional SAML 1.x or WS-Federation single sign-ons might experience a redirection loop at the browser.

This occurs if the Oracle Access Manager AccessGate configured for Oracle Identity Federation has an Idle Session Timeout less than the Maximum user session time. In this case, if the user waits for the idle session timeout to elapse and then initiates another SSO, the redirection loop will occur.

This can be avoided by setting the Oracle Identity Federation AccessGate's Idle Session Timeout equal to or greater than the Maximum user session timeout (which is the default setting).

7.1.5 Truncated Text in Japanese Version of Oracle Universal Installer

The following issue is observed during a Japanese-language installation session:

1. Start Oracle Universal Installer.
2. Choose the "Oracle Identity Federation 10g" installation option.
3. Proceed to the "Select Installation Method" page.

The text describing the first radio button ("Basic"), is truncated.

7.1.6 Unused Assertion Profile With Invalid Attribute Mapping Can Cause SSO Failure

If Oracle Identity Federation is used as an identity provider with an LDAP or RDBMS user data store, a configured SAML 1.x assertion profile with a non-existent user attribute will cause all single sign-ons (SSOs) using the SAML 1.x and WS-Federation profiles to fail, even if they do not use the invalid profile.

When a user logs into an Oracle Identity Federation identity provider with the LDAP or RDBMS user data store, Oracle Identity Federation attempts to retrieve all user attributes in all configured assertion profiles. If any of the attributes are invalid, the SSO will fail.

With the RDBMS data store, the user will receive a 500 Internal Server Error. If debug logging is enabled, the `federation.log` file will show the following error:

```
RDBMSBridge.authenticate(): ERROR - SQL Exception thrown by  
JDBC: java.sql.SQLException: ORA-00904: "<attribute name>":  
invalid identifier
```

With the LDAP data store, the user will receive an Identity Federation error with ID TSE007, and the `federation.log` file will show an error:

```
RESPONDER: ERROR User directory entry for <userDN> does not have  
the <assertion attribute> attribute <user attribute>. (RSE027)
```

The workaround is to correct the invalid user attribute in the offending assertion profile, or delete the offending assertion profile.

7.1.7 Signed SAML 1.0 Assertions Can Cause SSO Failures

Because SAML 1.0 does not fully specify how the XML Signature standard is to be used, Oracle Identity Federation cannot - within the context of a SAML response - correctly generate a signed SAML 1.0 assertion, nor verify a received signed SAML 1.0 assertion. Consequently, signatures on SAML 1.0 assertions used for the Artifact and POST SSO profiles are incorrect. If a user attempts to perform a single sign-on (SSO) using a SAML 1.x assertion profile with assertion signing enabled, and SAML 1.1 is not enabled for MyDomain or the destination domain, the service provider/destination site may not be able to verify the signature on the SSO assertion, causing the SSO to fail. If the destination site uses Oracle Identity Federation, the `federation.log` file will show:

```
RECEIVER: ERROR: An invalid SAML Response was received: XML  
SIGNER: ERROR: Invalid signature or altered contents
```

The workaround is to use the SAML 1.1 protocol instead of SAML 1.0. (In fact, one of the reasons for the SAML 1.1 revision was to allow better use of XML Signatures.)

Note: Signed assertions are not required, nor are they commonly used, for the SAML 1.x SSO profiles.

7.1.8 Encrypting Network Connections

By default, JDBC does not encrypt network connections between Oracle Identity Federation and the Oracle9i Database Server. Sites can optionally use Oracle Advanced Security to encrypt these connections.

In configuring Oracle Identity Federation to use Oracle Internet Directory or other LDAP servers to authenticate users, a site may choose whether to use SSL to connect to the LDAP server. If you do not use SSL, unencrypted passwords may be sent over network connections between Oracle Identity Federation and the LDAP server.

7.1.9 Spurious Certificate Verification Failure in Debug Log

When a signing certificate issued by a third-party CA is installed in the keystore for the SAML 1.x/WS-Federation part of Oracle Identity Federation, and debug logging is enabled, a spurious error is reported:

```
XML SIGNATURE: cert verify check: FAILED - java.security.SignatureException:  
Signature does not match.
```

The certificate verification being performed is appropriate only for self-signed certificates. This error does not affect the operation of Oracle Identity Federation and the log message can be ignored.

7.2 Configuration Issues and Workarounds

This section describes configuration issues and workarounds. It includes the following topics:

- [Section 7.2.1, "Administration Console Is Not Accessible After Changing Transient Data Store"](#)
- [Section 7.2.2, "Signing SAML Response with Assertion"](#)
- [Section 7.2.3, "Assertions Using SAML 1.x POST Method Fail in Japanese Locale"](#)
- [Section 7.2.4, "Using RDBMS as a User Data Store with a Login column ID of type CHAR"](#)
- [Section 7.2.5, "Some Peer Providers Are Not Displayed in Administration Console"](#)
- [Section 7.2.6, "SAML 2.0 Metadata AttributeRequesterDescriptor Not Supported"](#)
- [Section 7.2.7, "Problems Disabling Protocol Profiles in Administration Console"](#)
- [Section 7.2.8, "Metadata Service URLs With Query Parameters Not Supported"](#)

7.2.1 Administration Console Is Not Accessible After Changing Transient Data Store

You may be unable to access the Oracle Identity Federation administration console in this situation:

1. The command-line configuration assistant is executed to change the RDBMS database used for the transient data store. The command format is as follows:

```
java -jar install.jar -transient rdbms <parameters>
```
2. After the command is executed, the Oracle Identity Federation administration console is not accessible, and the federation logs or the OPMN logs show errors like the following:

```
Invalid username/password
```

This issue is seen when switching the Oracle Identity Federation transient store from one database to another, using a different username/password combination, or when using the same database but with different credentials.

This problem arises because Oracle Identity Federation is already set up for RDBMS transient data store, but when the command-line configuration assistant is executed, the database password does not get reset; this results in the invalid username/password error when trying to perform any Oracle Identity Federation operations.

Use these steps to work around the problem:

1. Log on to the Oracle Enterprise Manager 10g Grid Control Console.
2. Navigate to **OC4J_FED - > Administration - > Security**.
3. In the Users list, click the jazn.com/oif_db entry.
4. Enter the correct password to access the RDBMS.
5. Apply, and restart the OC4J_FED instance.

7.2.2 Signing SAML Response with Assertion

When an Oracle Identity Federation IdP is configured to send signed both Response messages and Assertions, only the Assertions are signed.

This affects SSO and attribute sharing profiles for the Liberty 1.x and SAML 2.0 protocols. This does not affect profiles where a Response message does not contain an Assertion.

7.2.3 Assertions Using SAML 1.x POST Method Fail in Japanese Locale

In the Japanese locale, assertions using the SAML 1.x POST method fail with this error:

```
ERROR: The SAML Response was not signed by the expected
authority (RVE013)
```

The problem is due to the translated strings for OU and ST in the Signing Certificate Subject DN and the Signing Certificate Issuer DN.

As a workaround to this problem, the OU and ST values need to be replaced with the equivalent English strings. You can obtain the English value of the strings from the Issuer and Subject DN in the MyDomain configuration.

7.2.4 Using RDBMS as a User Data Store with a Login column ID of type CHAR

The instructions in the *Oracle Identity Federation Administrator's Guide* (Section 5.4.2.1, Configuring an RDBMS as the User Data Store) for using an Oracle database as the repository for the user data store omit additional steps required when the database table has a Login ID column of type CHAR. These steps are necessary to account for the automatic padding applied in Oracle RDBMS for CHAR data (which is not done for VARCHAR2 data).

Take the following steps to create a data source for an Oracle database table when the Login ID column is of type CHAR:

1. Log in to the Enterprise Manager console of your Oracle Identity Federation instance and navigate to **OC4J_FED - > Administration - > Data Sources**.
2. Create a new data source using the following example as a guide:

```
Name: myDS
```

```
Data Source Class:  oracle.jdbc.pool.OracleDataSource
JDBC URL:          jdbc:oracle:thin:@stahs08.us.oracle.com:1521:ORCL
JDBC Driver:       oracle.jdbc.driver.OracleDriver
Username:          CUSTDATA
Password:          PASSWORD
Location:          jdbc/RDBMSUserDataSource
```

3. Apply the changes.
4. Restart the OC4J_FED instance.

Note: Do not enter any information in the Transactional(XA) Location and EJB Location fields.

7.2.5 Some Peer Providers Are Not Displayed in Administration Console

In the administration console (**Server Configuration > Circle of Trust** page and **Identity Federation > Trusted Providers** page), the only three types of entities displayed are:

- Identity Provider
- Service Provider
- Affiliation

If a provider's SAML 2.0 metadata does not contain either an `SPSSODescriptor`, `IdPSSODescriptor`, or `AffiliationDescriptor`, then it is not placed into any of these three categories.

For example, if a peer provider has just an `AttributeAuthorityDescriptor` in its metadata, it will not be displayed in the CoT page after loading. However, such a provider will still work properly at runtime, to the extent that the protocols published in its metadata are supported.

7.2.6 SAML 2.0 Metadata AttributeRequesterDescriptor Not Supported

An XML parsing error occurs when SAML 2.0 metadata containing an `AttributeRequesterDescriptor` element is loaded.

This results in a 500 `Internal Server Error` in the administration console.

There is no workaround for this issue.

7.2.7 Problems Disabling Protocol Profiles in Administration Console

Disabling a protocol profile in the administration console (for example, **Server Configuration > Identity Provider > SAML 2.0 > Enable Protocol Profiles**) only controls which profiles get published in the generated metadata. At runtime, requests for those profiles would proceed as usual.

There is no workaround for this issue.

7.2.8 Metadata Service URLs With Query Parameters Not Supported

If metadata loaded for a peer provider contains service URLs (for example, `AssertionConsumerService`) that include query parameters, Oracle Identity Federation fails to correctly redirect to those URLs during runtime execution of the protocol profiles.

7.3 Documentation Errata

This section describes documentation errata. It includes the following topic:

- [Section 7.3.1, "Incorrect Header in Oracle Identity Federation Online Help"](#)
- [Section 7.3.2, "Usage of Command-line Configuration Assistants"](#)

7.3.1 Incorrect Header in Oracle Identity Federation Online Help

Online help pages in Oracle Identity Federation are incorrectly labeled with the title "Oracle Help for the Web 2.0 Beta". The correct title should be "Oracle Identity Federation Administration Help" for the Administration Console, and "Oracle Identity Federation Monitoring Help" for the Monitoring Console.

7.3.2 Usage of Command-line Configuration Assistants

This note relates to the following sections of the *Oracle Identity Federation Administrator's guide*:

8.2.2 Command-Line Configuration Assistant to Change the Transient Data Store

8.2.3 Command-Line Configuration Assistant for Uninstallation

The document states that these configuration assistants take passwords on the command line as parameters. This practice is not secure and should be avoided.

Both these tools will prompt the user for LDAP and/or RDBMS passwords when they are not entered on the command line. For example, you can execute the `uninstall` tool with these parameters:

```
jdk/bin/java -jar fed/lib/uninstall.jar -uninstall -oh $ORACLE_HOME -removedfed
true -ldap false -ldaptype oid -ldapurl ldap://my.ldap.com -ldapusername USERNAME
-db false
```

The tool will then display the following, prompting you for an LDAP password:

```
Parsing parameters
Verifying parameters
Enter password for LDAP Username "USERNAME":
```

Note that the following parameter for the Command-Line Configuration Assistant to Change the Transient Data Store (Section 8.2.2.1 of the document) is not required:

`-dbpwd <PASSWORD>` - This is the RDBMS password. Required if an RDBMS is used for the transient data store.

The following parameters for the Command-Line Configuration Assistant for Uninstallation (Section 8.2.3.1 of the document) are not required:

`-ldappwd` - This is the password of the LDAP user.

`-dbpwd password` - The RDBMS password. Required if db is true

Both tools allow users to specify the passwords on the command line, but this practice is strongly discouraged. If you pass the passwords as parameters on the command line, a warning message will be displayed:

Caution: It is insecure practice to enter passwords on the command line. Please consult the latest product documentation for secure usage of this utility.

Future releases of Oracle Identity Federation will remove support for allowing passwords on the command line, and will only prompt for passwords.

Oracle Security Developer Tools

This chapter describes issues associated with Oracle Security Developer Tools. It includes the following topics:

- [Section 8.1, "General Issues and Workarounds"](#)

8.1 General Issues and Workarounds

This section describes general issue and workaround. It includes the following topic:

- [Section 8.1.1, "Oracle XML Security Does Not Handle the InclusiveNamespaces Tag"](#)

8.1.1 Oracle XML Security Does Not Handle the InclusiveNamespaces Tag

This bug relates to a parameter used to create a signature with Oracle Security Developer Tools.

An XML Signature can use either Inclusive or Exclusive Canonicalization to canonicalize the Reference or the SignedInfo:

- In Inclusive Canonicalization, all the specified and inherited namespaces are written out.
- In Exclusive Canonicalization, only namespaces that are actually used are written out.

The behavior of Exclusive Canonicalization can be modified by specifying the `InclusiveNamespaces` parameter, which is a list of namespaces that are exceptions, that is, namespaces which should be written out even if they are not used.

Because of this bug, the `InclusiveNamespaces` parameter is ignored when used for canonicalizing the SignedInfo (but considered when canonicalizing a reference). As a result, when you use the Oracle XML Security API of Oracle Security Developer Tools to create a signature that uses the `InclusiveNamespaces` parameter, the signature value will be computed incorrectly. Similarly, when you verify a signature that uses the `InclusiveNamespace` parameter, the verification will incorrectly return a false.

Oracle Internet Directory

This chapter describes issues associated with Oracle Internet Directory. It includes the following topics:

- [Section 9.1, "General Issues and Workarounds"](#)
- [Section 9.2, "Configuration Issues and Workarounds"](#)
- [Section 9.3, "Documentation Errata"](#)

9.1 General Issues and Workarounds

This section describes general issues and their workarounds. It includes the following topics:

- [Section 9.1.1, "Perform Full Database Backup After Administrative Changes to Oracle Internet Directory"](#)
- [Section 9.1.2, "Comment Out ACL Attributes Not Defined in the Schema"](#)
- [Section 9.1.3, "Specify DN of the DIT When Dumping Directory Entries for an Advanced Replication Agreement"](#)

9.1.1 Perform Full Database Backup After Administrative Changes to Oracle Internet Directory

If you use standard database backup and restore procedures, such as those performed by the Oracle Application Server Backup and Recovery Tool, you must perform a full database backup after any of the following administrative tasks:

- Using the `bulkload` bulk management tool
- Using the `catalog` bulk management tool
- Installing Oracle Internet Directory
- Upgrading Oracle Internet Directory to a major release version or patchset
- Installing an LDAP application against Oracle Internet Directory, such as Oracle Collaboration Suite, that modifies the `cn=catalogs` entry to add `orclindexedattribute`

If you do not perform a full backup after using the `bulkload` bulk management tool, you might encounter unrecoverable errors when performing a restore. The `bulkload` utility performs a direct path load, which does not generate redo logs. If you do not perform a full backup after performing a `bulkload`, and later perform a restore that attempts to apply archived redo logs, you might encounter errors that cannot be fixed.

If you do not perform a full backup after any of the other four tasks, you might encounter recoverable errors when performing a restore. Performing any of those tasks might create indexes with the `NOLOGGING` option, which means that redo logs are not created for the index. If you do not perform a full backup after one of these operations, and later perform a restore that attempts to apply archived redo logs, you might see errors upon restart of Oracle Internet Directory. Specifically, you would see ORA-1578 and ORA-2640 errors in `oidmon.log` or `oidldapd*.log`. In this case, shut down Oracle Internet Directory and recreate all Oracle Internet Directory database indexes by typing:

```
bulkload connect="conn_str" index="TRUE"
```

9.1.2 Comment Out ACL Attributes Not Defined in the Schema

With the 10g (10.1.4.0.1) release, Oracle Internet Directory introduces a new restriction for Access Control Lists (`orclaci` and `orclentrylevelaci` attributes). Specifically, you cannot specify attribute names that are not defined in directory schema. As a result, while adding or migrating entries from previous Oracle Internet Directory releases, the load operation will fail if any entries have attribute names that are not defined in the directory schema.

To avoid this problem, in the LDIF file, comment out any ACLs that have undefined attributes.

For example, the following 10g Release 2 (10.1.2) entry uses undefined attributes that are identified with bold text:

```
orclaci: access to attr=(orclUserApplnProvStatus,orclUserApplnProvStatusDesc,  
orclUserProvFailureCount) by group="cn=oracledasedituser,cn=groups,  
cn=OracleContext,dc=us,dc=oracle,dc=com" (read,search,write,compare) by  
group="cn=oracledascreateuser,cn=groups,cn=OracleContext,dc=us,dc=oracle,  
dc=com" (read,search,write,compare) by self (read,search,nowrite,compare)  
by * (none)
```

To avoid this problem, comment the entry as follows, before loading or verifying the LDIF file.

```
# orclaci: access to attr=(orclUserApplnProvStatus,orclUserApplnProvStatusDesc,  
# orclUserProvFailureCount) by group="cn=oracledasedituser,cn=groups,  
# cn=OracleContext,dc=us,dc=oracle,dc=com" (read,search,write,compare) by  
# group="cn=oracledascreateuser,cn=groups,cn=OracleContext,dc=us,dc=oracle,  
# dc=com" (read,search,write,compare) by self (read,search,nowrite,compare)  
# by * (none)
```

9.1.3 Specify DN of the DIT When Dumping Directory Entries for an Advanced Replication Agreement

When you add a new directory to a directory replication group, you copy entries from an existing directory to the new directory using the `ldifwrite` and `bulkload` tools.

Normally, the easiest way to do this is to specify a replication agreement DN as the `basedn` argument to `ldifwrite`. This causes the `ldifwrite` tool to dump all entries that are replicated by the specified replication agreement. Then you can load the entries to another replicated directory using `bulkload` tool.

In release 10g (10.1.4.0.1), this functionality does not work when the replication agreement DN is `orclagreementid=000001,cn=replication` configuration, which is the DN of an Advanced replication agreement. The

workaround is to explicitly specify the DN of the DIT that you want to copy as the base DN argument to `ldifwrite`.

9.2 Configuration Issues and Workarounds

This section describes configuration issues and their workarounds. It includes the following topic:

- [Section 9.2.1, "Set Language Before Using bulkload"](#)

9.2.1 Set Language Before Using bulkload

If your server locale is not English, set `NLS_LANG` to `AMERICAN_AMERICA.AL32UTF8` before running `bulkload`.

9.3 Documentation Errata

This section describes documentation errata. It includes the following topics:

- [Section 9.3.1, "Bad Links in Online Help Pages"](#)
- [Section 9.3.2, "Missing Line Break in sqlplus Command"](#)
- [Section 9.3.3, "Errors in oracle.ldap.util.Subscriber.createUser\(\) Documentation"](#)
- [Section 9.3.4, "Missing Example: How to Decode a Mime-Encoded Header Set by mod_sso"](#)
- [Section 9.3.5, "Error in Identity Management Grid Control Plug-in Context-Sensitive Help"](#)
- [Section 9.3.6, "Missing Note: The labeledURI Attribute host:port is for Syntax Purposes Only"](#)
- [Section 9.3.7, "Missing Example: Listing All the Attributes in the Directory by Using ldapsearch"](#)
- [Section 9.3.8, "Incorrect Environment Variables in Plug-in Debugging Examples"](#)
- [Section 9.3.9, "Figure Errors in Replication Concepts Chapter"](#)

9.3.1 Bad Links in Online Help Pages

The document links from the **Related Documents** help pages for Identity Management Grid Control Plug-in and Oracle Internet Directory Server Manageability are broken. Please navigate to the documents from <http://www.oracle.com/technology/documentation>.

9.3.2 Missing Line Break in sqlplus Command

The following command line appears in the HTML version of Appendix I of *Oracle Internet Directory Administrator's Guide*, Section I.6.2, "Tasks To Be Performed on the New Advanced Replication Node," Step 18:

```
$> sqlplus rep_admin_db_account_name/password@db_conn_str_of_new_nodeSQL> exec
dbms_repcat.drop_master_repgroup( gname => 'LDAP_REP' )
```

There should be a line break before `SQL>`. That is, the command should be:

```
$> sqlplus rep_admin_db_account_name/password@db_conn_str_of_new_node
SQL> exec dbms_repcat.drop_master_repgroup( gname => 'LDAP_REP' )
```

9.3.3 Errors in oracle.ldap.util.Subscriber.createUser() Documentation

There are errors in the description of the

`oracle.ldap.util.Subscriber.createUser()` method, in both the *Oracle Internet Directory API Reference* and the chapter entitled "Using the Java API Extensions to JNDI" in the *Oracle Identity Management Application Developer's Guide*.

- In the description of `createUser()` in the *Oracle Internet Directory API Reference*, all instances of the term `useMandatoryAttr` should be changed to `useMandatoryObjectclasses`.

The following sentence in the *Oracle Internet Directory API Reference* is incorrect:

"Objectclasses are automatically picked up and do not need to be included in `ModPropertySet`."

You must include `objectclasses` in `ModPropertySet` when `useMandatoryObjectclasses` is set to `false`.

- The code sample in the *Oracle Internet Directory API Reference* contains the line:

```
User newUser = sub.createUser( ctx, mps, false );
```

The line should be changed to:

```
User newUser = sub.createUser( ctx, mps, true );
```

Otherwise, the code will throw an exception due to the missing `objectclass` attribute.

- Similarly, in the chapter entitled "Using the Java API Extensions to JNDI" in the *Oracle Identity Management Application Developer's Guide*, the line:

```
User newUser = sub.createUser( ctx, mps );
```

should be changed to:

```
User newUser = sub.createUser( ctx, mps, true );
```

9.3.4 Missing Example: How to Decode a Mime-Encoded Header Set by `mod_sso`

If the user name or other HTTP header is multibyte and set by `mod_osso`, then that header must be decoded using mime decoding. The chapter entitled "Developing Applications for Single Sign-On" in the *Oracle Identity Management Application Developer's Guide* should contain a Java example showing how to do this.

The following code fragment shows how to decode a mime-encoded multibyte user name obtained from a servlet request object:

```
import javax.mail.internet.MimeUtility;
...
String mimeUserName = request.getRemoteUser();
String userName = MimeUtility.decodeText(mimeUserName);
```

9.3.5 Error in Identity Management Grid Control Plug-in Context-Sensitive Help

The Directory Server User Statistics Help page contains the following sentence: "You can add a monitored user to the table by using Oracle Directory Monitor or by using

the command line." It should say Oracle Directory Manager instead of Oracle Directory Monitor.

9.3.6 Missing Note: The labeledURI Attribute host:port is for Syntax Purposes Only

The following note should be added to the section entitled "Schema Elements for Creating a Dynamic Group" in the Dynamic Groups chapter of *Oracle Internet Directory Administrator's Guide*:

Note: In the labeledURI attribute, the *host:port* section is present for syntax purposes alone. Irrespective of the host and port settings in the labeledURI attribute, the directory server always computes members of dynamic group from the local directory server. It cannot retrieve members from other directory servers.

9.3.7 Missing Example: Listing All the Attributes in the Directory by Using ldapsearch

This example should be added to the "Directory Entries Administration" chapter in *Oracle Internet Directory Administrator's Guide*.

Use the following command line to list of all the attributes, including those that do not have values:

```
ldapsearch -b "cn=subschemasubentry" -s base "objectclass=*
```

9.3.8 Incorrect Environment Variables in Plug-in Debugging Examples

In the "PL/SQL Server Plug-ins" chapter in *Oracle Identity Management Application Developer's Guide* and the "Oracle Internet Directory Plug-In for Password Policies" chapter in *Oracle Internet Directory Administrator's Guide*, all pathnames beginning with \$ORACLE/ should actually begin with \$ORACLE_HOME/.

9.3.9 Figure Errors in Replication Concepts Chapter

The chapter entitled "Oracle Internet Directory Replication Concepts" in *Oracle Internet Directory Administrator's Guide* contains the following errors:

- In Figure 29-10, the direction of the arrow labeled 4' should be reversed. Also, four of the numbers in the figure should be changed as shown in [Table 9-1](#).

Table 9-1 Numbers to Change in Figure 29-12

| Incorrect Number | Correct Number |
|------------------|----------------|
| 7 | 6 |
| 6 | 6' |
| 7 | 7' |
| 7' | 8 |

- In the text for Figure 29-12, the sentence beginning with "When Node 4 fails, you can fail over Node 4" should be changed to "When Node 2 fails, you can fail over Node 4."

- In the text for Figure 29-14, the excluded subtree, described as `cn=user1 , cn=hr , c=us`, should be `cn=users , cn=hr , c=us`.

Oracle Application Server Certificate Authority

This chapter describes issues associated with Oracle Application Server Certificate Authority. It includes the following topic:

- [Section 10.1, "Documentation Errata"](#)

10.1 Documentation Errata

This section describes documentation errata. It includes the following topics:

- [Section 10.1.1, "Java Classes for Custom Policy Plug-in Must Use JDK 1.4.2"](#)
- [Section 10.1.2, "Incorrect Class Name in Custom Policy Example"](#)

10.1.1 Java Classes for Custom Policy Plug-in Must Use JDK 1.4.2

The *Oracle Application Server Release Notes*, in the chapter titled "Managing Policies in Oracle Application Server Certificate Authority", describes how to develop custom policy plug-ins. The section titled Steps in Creating a New Policy Plug-in does not specify the version of JDK that should be used to compile Java classes for custom policy plug-ins. The version currently supported is JDK 1.4.2. Change Step 2 in the instructions to say:

"Save the java class implemented in step 1 and compile using JDK 1.4.2, after adding the `$ORACLE_HOME/oca/lib/oca-1_3.jar` file to the java CLASSPATH and obtaining the class file."

Using a different version of JDK may result in errors such as a "500 Internal Server Error."

10.1.2 Incorrect Class Name in Custom Policy Example

The *Oracle Application Server Release Notes*, in the chapter titled "Managing Policies in Oracle Application Server Certificate Authority", describes how to develop custom policy plug-ins. The example program listing in the section An Example of a Custom Policy Plug-in, Line 3 contains an incorrect class name:

```
3: import oracle.security.oca.policy.custom.OCACustomPolicyplugin;
```

The correct class name is

`oracle.security.oca.policy.custom.OCACustomPolicyPlugin`. Replace Line 3 with the following text:

```
3: import oracle.security.oca.policy.custom.OCACustomPolicyPlugin;
```

Oracle Delegated Administration Services

This chapter describes issues for both the Oracle Delegated Administration Services (DAS) and the Oracle Internet Directory Self-Service Console. It includes the following topics:

- [Section 11.1, "General Issues and Workarounds"](#)
- [Section 11.2, "Administration Issues and Workarounds"](#)

11.1 General Issues and Workarounds

This section describes general issues and their workarounds for Oracle Delegated Administration Services. It includes the following topics:

- [Section 11.1.1, "Installation Process Does Not Enable SSL for Oracle Delegated Administration Services"](#)
- [Section 11.1.2, "Using Single Wildcard Characters to Search for Entries Fails to Return Results"](#)
- [Section 11.1.3, "Oracle Internet Directory Self-Service Console Link Does Not Work in Oracle Identity Manager Grid Control Plug-in"](#)

11.1.1 Installation Process Does Not Enable SSL for Oracle Delegated Administration Services

By default, the installation process does not enable SSL for Oracle Delegated Administration Services. Following the installation process, Oracle recommends that you enable SSL mode for Oracle Delegated Administration Services by following the instructions in *Oracle Application Server Administrator's Guide*.

11.1.2 Using Single Wildcard Characters to Search for Entries Fails to Return Results

If you enter a single percent sign (%) or asterisk (*) wildcard character when searching for users or groups in the Oracle Internet Directory Self-Service Console, no results are returned. To return a list of all users or groups, do not enter any characters in the search box in the Search for Users or Search for Groups windows.

11.1.3 Oracle Internet Directory Self-Service Console Link Does Not Work in Oracle Identity Manager Grid Control Plug-in

When an Oracle Delegated Administration services instance is configured to use SSL, or if you change the host and port where the instance is deployed, the Oracle Internet Directory Self-Service Console link does not work in Oracle Identity Manager Grid

Control Plug-in. To resolve this issue, perform the following steps to manually configure the Oracle Internet Directory Self-Service Console link on the Oracle Identity Manager Grid Control Plug-in page.

1. Start Oracle Enterprise Manager 10g Grid Control Console.
2. Click the **Targets** tab, and then click the **Identity Management** subtab.
3. Select the Oracle Delegated Administration Services instance that you need to update and click **Configure**.
4. Modify the properties as necessary.

11.2 Administration Issues and Workarounds

This section describes administration issues and their workarounds for Oracle Delegated Administration Services. It includes the following topic:

- [Section 11.2.1, "Disabling Password Change and Reset Functionality"](#)
- [Section 11.2.2, "Resetting Oracle Application Server Single Sign-On Passwords Redirects Users to Oracle Delegated Administration Services Home Page"](#)

11.2.1 Disabling Password Change and Reset Functionality

To disable password change and reset functionality, assign a value of false to the `RESET_PASSWD_ENABLED` parameter in the `$ORACLE_HOME/ldap/das/das.properties` file. This removes the Forged Your Password? link from the Oracle Internet Directory Self-Service Console home page and the Manage My Password link from the My Profile tab.

Disabling password change and reset functionality only applies to users; the Forged Your Password? link on the Oracle Internet Directory Self-Service Console home page and the Manage My Password link on the My Profile tab are always available to administrators, regardless of the value assigned to the `RESET_PASSWD_ENABLED` parameter.

11.2.2 Resetting Oracle Application Server Single Sign-On Passwords Redirects Users to Oracle Delegated Administration Services Home Page

Various application, including OracleAS Portal, use Oracle Delegated Administration Services to reset Oracle Application Server Single Sign-On passwords. Users can reset their own passwords by clicking on a link in the source application, which opens the Reset My Single Sign-On Password page in Oracle Internet Directory Self-Service Console. However, when users click the OK button after resetting their passwords, or if they click the Cancel button to abort the password change process, they are redirected to the Oracle Delegated Administration Services home page instead of to the referring application page.

To redirect users to a location other than the Oracle Delegated Administration Services home page, append a query string containing the correct return URLs to the link on the referring application page. Include in the query string two `name=ovalue` pairs for the `doneURL` and the `cancelURL` attributes. The `doneURL` attribute identifies the redirect URL to call when users click the OK button and the `cancelURL` attribute identifies the redirect URL to call when users click the Cancel button. The following example demonstrates how to build a URL to the Change Application Password page that includes the `doneURL` and the `cancelURL` attributes:

```
http://host:port/oiddas/ui/oracle/ldap/AppStep1ResetPwd?
```

cancelURL=http://www.domain.com&doneURL=http://www.domain.com

Oracle Directory Integration Platform

This chapter describes the issues associated with Oracle Directory Integration Platform. It includes the following topics:

- [Section 12.1, "Configuration Issues and Workarounds"](#)
- [Section 12.2, "Administration Issues and Workarounds"](#)

12.1 Configuration Issues and Workarounds

This section describes configuration issues and their workarounds for Oracle Directory Integration Platform. It includes the following topics:

- [Section 12.1.1, "Configuration Requirements for Synchronizations with Domain-Level Mappings"](#)
- [Section 12.1.2, "Directory Integration Assistant Throws "LDAP: error code 2 - Decoding Error" When Uploading an Additional Configuration Information File"](#)
- [Section 12.1.3, "Reconfiguring the Oracle Password Filter for Microsoft Active Directory Generates Errors"](#)
- [Section 12.1.4, "In a High Availability Environment Using Multimaster Replication, Provisioning Events May not Be Propagated or May Be Duplicated"](#)
- [Section 12.1.5, "Manual Step Required After Configuring Oracle Directory Integration Platform from Oracle Enterprise Manager"](#)
- [Section 12.1.6, "Securing the Windows Registry Before Installing the Oracle Password Filter for Microsoft Active Directory"](#)

12.1.1 Configuration Requirements for Synchronizations with Domain-Level Mappings

For import and export synchronization with OpenLDAP and for export synchronization to Sun Java System Directory, if you are using domain-level mapping during synchronization and synchronizing attributes that contain the `dn` values then you must modify the mapping rules. For example, to synchronize groups with domain-level mappings, you must modify the mappings for `member`, `uniquemember`, and `owner` entries, which typically contain `dn` values.

If you plan to create the synchronization profiles using the express configuration operation of the Directory Integration Assistant, then perform the following steps:

1. Open in a text editor the mapping file for the third-party directory with which you will synchronize:
 - **OpenLDAP export synchronization:** `$ORACLE_HOME/ldap/odi/samples/openldapexp.domainmap.master`

- **OpenLDAP export synchronization:** `$ORACLE_HOME/ldap/odi/samples/openldapimp.domainmap.master`
 - **Sun Java System Directory export synchronization:** `$ORACLE_HOME/ldap/odi/samples/iplanetexp.domainmap.master`
2. Modify the contents of the preceding mapping files for the third-party directory with which you are synchronizing so they read as follows:

```
member: : :groupofnames:member: :groupofnames: dnconvert(member)
uniquemember: : :groupofuniquenames:uniquemember: :groupofuniquenames:
dnconvert(uniquemember)
owner: : :groupofuniquenames:owner: :groupofuniquenames: dnconvert(owner)
```

If you have already created synchronization profiles for a third-party directory, then perform the following steps:

1. Open in a text editor the import and export mapping files for the third-party directory with which you are synchronizing.
2. Modify the contents of the import and export synchronization mapping files so they read as follows:

```
member: : :groupofnames:member: :groupofnames: dnconvert(member)
uniquemember: : :groupofuniquenames:uniquemember: :groupofuniquenames:
dnconvert(uniquemember)
owner: : :groupofuniquenames:owner: :groupofuniquenames: dnconvert(owner)
```

12.1.2 Directory Integration Assistant Throws "LDAP: error code 2 - Decoding Error" When Uploading an Additional Configuration Information File

This error occurs because the file size of the Additional Configuration Information file for Synchronization Profiles cannot exceed 4 KB. To resolve this issue, perform the following steps to change the type of the `OrclODIPAgentConfigInfo` attribute from `DirectoryString` to `Binary`:

1. Run the following command to start Oracle Directory Manager:


```
oidadmin
```
2. In the navigator pane, expand **Oracle Internet Directory Servers**, and then *directory server instance*.
3. Select **Schema Management**. The Schema Management tab pages appear in the right pane.
4. In the right pane, select **Attributes**.
5. Click the **Name** column to order the attributes alphabetically.
6. Locate and select the **OrclODIPAgentConfigInfo** attribute, and then click **Edit**.
7. Change the **Syntax** option from `DirectoryString` to `Binary`, and then click **OK**.
8. Use Directory Integration Assistant to upload the Additional Configuration Information file.

12.1.3 Reconfiguring the Oracle Password Filter for Microsoft Active Directory Generates Errors

When you install or reconfigure the Oracle Password Filter for Microsoft Active Directory, you may see the following errors on the command line:

```
User created failed
Delete failed failed
```

The preceding errors occur when the default password that is used to reconfigure the Oracle Password Filter for Microsoft Active Directory does not meet the password policy requirements of the Microsoft Active Directory domain. To resolve this issue, create a file named `password.txt` in the directory where you installed the Oracle Password Filter for Microsoft Active Directory. Add to the `password.txt` file a single line containing a password that meets the password policy requirements of the Microsoft Active Directory domain. To secure the `password.txt` file, set its file permissions so that only administrative users can access it. Note that the password stored in the `password.txt` file does not represent a major security risk because its sole purpose is to create and then delete a user to test connectivity between the Oracle Password Filter and Microsoft Active Directory.

12.1.4 In a High Availability Environment Using Multimaster Replication, Provisioning Events May not Be Propagated or May Be Duplicated

In multimaster replication, the last change number is stored locally on an Oracle Internet Directory node. In a high availability environment, if that node fails, and the provisioning profile is moved to another Oracle Internet Directory node, then the last applied change number in the profile becomes invalid. That number in the profile must then be reset manually on the failover node. Even then, however, events may not be propagated or may be duplicated.

12.1.5 Manual Step Required After Configuring Oracle Directory Integration Platform from Oracle Enterprise Manager

After configuring Oracle Directory Integration Platform from Oracle Enterprise Manager, the `ConnectDescriptor` property for the Oracle Directory Integration Platform target in the `targets.xml` file is assigned a blank value. You must perform the following steps to assign the appropriate database connect descriptor to the `ConnectorDescriptor` property:

1. On the computer that is running the Oracle directory integration server, open the `$ORACLE_HOME/network/admin/tnsnames.ora` file in a text editor.
2. Note the database connect descriptor information in the `tnsnames.ora` file. For example, the database connect descriptor information in the following `tnsnames.ora` file is the value assigned to the `ASDB` property:

```
ASDB = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST =
host.mycompany.com) (PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME =
database.mycompany.com)))
```

The database connect descriptor in the preceding statement is the following value:

```
DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST =
host.mycompany.com) (PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME =
database.mycompany.com)))
```

3. On the computer that is running the Oracle directory integration server, open the `$ORACLE_HOME/sysman/emd/targets.xml` file in a text editor.
4. Search for the target with a type of `oracle_eps_server` and a name attribute of `iasinstance_name_DIP`.
5. In the entry, locate the `ConnectDescriptor` property and assign to it the database connect descriptor information from the `tnsnames.ora` file.

6. Execute the following commands to restart Oracle Enterprise Manager:

```
$ORACLE_HOME/bin/emctl stop iasconsole  
$ORACLE_HOME/bin/emctl start iasconsole
```

7. Follow the directions in the *Oracle Identity Management Integration Guide* to restart Oracle Directory Integration Platform.

12.1.6 Securing the Windows Registry Before Installing the Oracle Password Filter for Microsoft Active Directory

The Oracle Password Filter for Microsoft Active Directory stores operational information in the Windows registry. Before installing or configuring the Oracle Password Filter for Microsoft Active Directory, Oracle strongly recommends that you perform the following steps to secure the Windows registry:

1. Create a text file named `orclidmpwf.txt` that contains the following text:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\orclidmpwf [1 5 17]
```

2. Click the Windows **Start** menu and select **Run**. The Run dialog box displays.
3. Enter `cmd` in the Run dialog box and click **OK**. The command prompt window opens.
4. Run the following command to secure the Windows registry:

```
regini path\orclidmpwf.txt
```

5. Type `exit` and press **Enter** to close the command prompt window.

12.2 Administration Issues and Workarounds

This section describes administration issues and their workarounds for Oracle Directory Integration Platform. It includes the following topics:

- [Section 12.2.1, "Default Mapping Rule Can Be Simplified in Single-Domain Microsoft Active Directory Deployments"](#)
- [Section 12.2.2, "Oracle Directory Integration Platform Not Sending Provisioning Events Due to Purged Change Log Entries"](#)
- [Section 12.2.3, "Oracle Internet Directory Field Unavailable in Oracle Identity Manager Grid Control Plug-in"](#)
- [Section 12.2.4, "Synchronization from Novell eDirectory or OpenLDAP Fails When the Oracle Internet Directory Container is Within the Default Realm"](#)

12.2.1 Default Mapping Rule Can Be Simplified in Single-Domain Microsoft Active Directory Deployments

In deployments with only a single domain of Microsoft Active Directory, you can simplify the default mapping rule installed with Oracle Directory Integration Platform.

The default mapping rule is:

```
sAMAccountName,userPrincipalName: :  
:user:orclSAMAccountName:  
:orclADUser:toupper(trunc1(userPrincipalName,'@'))+"$"+sAMAccountName
```

If your deployment has a single domain of Active Directory, then you can simplify the default mapping rule to this:

```
sAMAccountName: : :user:orclSAMAccountName::orclADUser
```

12.2.2 Oracle Directory Integration Platform Not Sending Provisioning Events Due to Purged Change Log Entries

If you use time-based change log purging with version 3.0 provisioning profiles, change logs entries are purged before the Oracle directory integration platform propagates the changes to any provisioning-integrated applications. This occurs because Oracle Directory Integration Platform does not create version 3.0 provisioning profile entries in the default `cn=subscriber` profile, `cn=changelog subscriber, cn=oracle internet directory change log subscriber` container.

To resolve this problem, create a container in the default change log subscriber container for each version 3.0 provisioning profile and assign a value of 0 to each profile's `orclLastAppliedChangeNumber` attribute. The following sample LDIF file creates a provisioning profile container in the default change log subscriber container and assigns a value of 0 to the `orclLastAppliedChangeNumber` attribute:

```
dn: cn=profile_name,cn=changelog subscriber,cn=oracle internet directory
orclsubscriberdisable: 0
orcllastappliedchangenumber: 0
objectclass: orclChangeSubscriber
```

12.2.3 Oracle Internet Directory Field Unavailable in Oracle Identity Manager Grid Control Plug-in

If the Oracle directory integration server and the Oracle Internet Directory LDAP server are installed on a different computers, then the Oracle Internet Directory field will be unavailable in the Oracle Identity Manager Grid Control Plug-in. Perform the following steps to resolve this issue:

1. On the computer that is running the Oracle Internet Directory LDAP server, open the `$ORACLE_HOME/sysman/emd/targets.xml` file in a text editor.
2. Search for the target with a type of `oracle_ldap` and note the value assigned to the name attribute. This value is typically in the form `iasinstance_name_LDAP`.
3. On the computer that is running the Oracle directory integration server, open the `$ORACLE_HOME/sysman/emd/targets.xml` file in a text editor.
4. Search for the target with a type of `oracle_eps_server` and a name attribute of `iasinstance_name_DIP`.
5. In the entry, locate the `ASSOC_TARGET_NAME` attribute beneath the `AssocTargetInstance` node. The value assigned to the `ASSOC_TARGET_NAME` attribute will be in the form `iasinstance_name_LDAP`.
6. Assign to the `ASSOC_TARGET_NAME` attribute the same value that is assigned to the name attribute of the `oracle_ldap` target in the `targets.xml` file on the computer that is running the Oracle Internet Directory LDAP server.

12.2.4 Synchronization from Novell eDirectory or OpenLDAP Fails When the Oracle Internet Directory Container is Within the Default Realm

Synchronization from Novell eDirectory or OpenLDAP to Oracle Internet Directory fails when the Oracle Internet Directory container is within the default realm. To resolve this issue, perform the following steps to create the necessary ACLs:

1. Create a new file in a text editor.
2. Enter the following statements, which add the Oracle Internet Directory container to the `cn=odipgroup,cn=odi,cn=oracle internet directory` group. Be sure to replace *host* with the host name (without the domain name) that is running the Oracle directory integration server.

```
dn: cn=odipgroup,cn=odi,cn=oracle internet directory
changetype: modify
add: uniquemember
uniquemember: cn=odisrv+orclhostname=host,cn=registered instances,cn=directory
integration platform,cn=products,cn=oraclecontext
```

3. Save the file as **reconacs.ldif**.
4. Run the following command to upload the `reconacs.ldif` file:

```
$ORACLE_HOME/bin/ldapmodify -h OID_host -p OID_port
-D "DN of privileged OID user" -w "password of privileged OID user"
-v -f reconacs.ldif
```