Oracle® Application Server

Release Notes

10*g* (10.1.4.0.1) for HP-UX Itanium

B32101-06

March 2010

ORACLE®

Oracle Application Server Release Notes, 10*g* (10.1.4.0.1) for HP-UX Itanium

B32101-06

Contents

5 Oracle Access Manager

14 Oracle Adaptive Access Manager

15 Oracle Role Manager

16 Oracle Identity Manager

Preface

This preface includes the following topics:

Audience

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

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at

http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

For more information, see these Oracle resources:

- Oracle Application Server Documentation on Oracle Application Server Disk 1
- Oracle Application Server Documentation Library 10*g* (10.1.4)

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in 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*. In addition to the new topics, the following three new chapters have been added:

- Chapter 14, "Oracle Adaptive Access Manager"
- Chapter 15, "Oracle Role Manager"
- Chapter 16, "Oracle Identity Manager"

The new topics are in the following chapters:

- Chapter 5, "Oracle Access Manager"
- Chapter 7, "Oracle Identity Federation"
- Chapter 9, "Oracle Internet Directory"
- Chapter 10, "Oracle Virtual Directory"
- Chapter 12, "Oracle Delegated Administration Services"

Chapter 5, "Oracle Access Manager"

- Section 5.1, "About Installation Packages, Patch Sets, Bundle Patches, and Newly Certified Agents"
- Section 5.2.1, "New Location for the Platform Support Matrix"
- Section 5.2.7, "Login.html Not Found if Browser Language is Not Supported"
- Section 5.5.11, "webgate.so Not Found Error After Form-based Login"
- Section 5.9.33, "Update for Apache v2 for WebGate on UNIX with the mpm_worker_module"

Chapter 7, "Oracle Identity Federation"

- Section 7.1.1, "Oracle Identity Federation Configuration Assistant Fails in SSL Mode"
- Section 7.4.3, "Update to Section 4.2.6.2 Creating a Custom Authentication Engine"

Chapter 9, "Oracle Internet Directory"

- Section 9.1.4, "Data Manipulation at Database Level is Not Supported"
- Section 9.3.16, "External Authentication Scripts Have .pls Extension"
- Section 9.3.17, "Patch Notes 10g (10.1.4.3.0) Contains Incorrect Instruction to Apply a Patch"

Chapter 10, "Oracle Virtual Directory"

- Section 10.1.1, "Creating oraInst.loc File During Installation of Oracle Virtual Directory 10g (10.1.4.3.0) on AIX"
- Section 10.2.1, "Correction for Access Control Rules Documentation"

Chapter 12, "Oracle Delegated Administration Services"

- Section 12.1.4, "Attributes Set to "Searchable" Always Appear on the Search Result Page"

1 Introduction

This chapter introduces Oracle Application Server Release Notes, 10*g* (10.1.4). It includes the following topics:

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/`

In addition to these release notes, please also see Patch Notes 10*g* (10.1.4.3.0) and Note 743141.1 Oracle Identity Management 10*g* (10.1.4.3) Patch Set Notes Addendum for information about the following Identity Management components:.

- Oracle Internet Directory
- Oracle Directory Integration Platform
- Oracle Application Server Single Sign-On
- Oracle Identity Federation
- Oracle Delegated Administration Services
- Oracle Application Server Certificate Authority

1.2 Purpose of this Document

This document contains the release information for Oracle Application Server 10*g* (10.1.4). It describes differences between Oracle Application Server and its documented functionality. It has been updated to the most recent 10.1.4 release or patch set for each component.

Oracle recommends you review its contents before installing, or working with the product. You should also review the Release Notes or Readme for the most recent 10.1.4 release for each component.

When you install Oracle Identity Management 10*g* (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 10*g* 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 10*g* (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 10*g* (10.1.4.0.1) Identity Management components be used from the CD Pack. Please check the certification matrix on My Oracle Support at https://support.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 10*g* (10.1.4) is available at:https://support.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
```

2

Installation and Upgrade Issues

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

2.1 Installation Issues

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

2.1.1 Workaround if HTTP Server Configuration Assistant Fails

If the HTTP Server Configuration Assistant fails during installation, try the following workaround:

1. Keep the installer open.
2. Open a shell and log in as root.
3. Change permissions for the *ORACLE_HOME*/Apache/Apache/bin/.apachectl file:
   a. Change to the directory containing the .apachectl file.

      ```
      > cd ORACLE_HOME/Apache/Apache/bin
      ```

      ORACLE_HOME is the directory where you are installing Oracle Application Server.

   b. Change the owner to root.

      ```
      > chown root .apachectl
      ```

   c. Change the permissions.

      ```
      > chmod 6750 .apachectl
      ```

4. In the installer, select the HTTP Server Configuration Assistant and click the Retry button.

   The HTTP Server Configuration Assistant should complete successfully now.

2.1.2 IPv6 Not Supported

This release of Oracle Application Server is not certified to run on machines that are configured with IPv6. You have to install and run this release of Oracle Application Server on machines that are configured with IPv4.

2.1.3 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"
```

2.1.4 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.

2.1.5 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.

2.1.6 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>
```

2.1.7 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 workaround this issue, retry the failed configuration assistant from the installation.

2.1.8 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.

2.1.9 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.

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

In some non-English locale Oracle Application Server installations the Oracle Enterprise Manager 10*g* 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 <a href="http://%s_hostName%:%s_oemConsolePort%" > 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,

2.1.11 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 workaround this problem, set the NLS parameter as follows:

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

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

2.1.12 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_SMTP`
- `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.

2.1.13 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.

2.1.14 OIDCA Fails Due to Misconfiguration in /etc/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.

2.1.15 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 $ORACLE_HOME/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
```

2.1.16 Error Messages in log files

When you install Oracle Identity Federation, the following error message is written to the `InstallAction*.log` and `make.log` files:

```
Building 64bit libttsh.so
... ...
ld: I/O error, file "/mnt1/astest/fed_bsc_rc4drop4/rdbms/lib/sllfls.o": There
is no such file or directory
Fatal error
```

You can ignore this error.

> **Note:** This error message appears for both Basic and Advanced installations of Oracle Identity Federation.

2.2 Upgrade Issues

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

- Section 2.2.1, "Clarification of When to Run the Metadata Repository Upgrade Assistant"
- Section 2.2.2, "Upgrade of Identity Management Installation to 10.1.4.0.1"
- Section 2.2.3, "Additional Step Required When Upgrading OracleAS Metadata Repository Release 9.0.4.3 to 10.1.4.0.1"
- Section 2.2.4, "Configuring Port Values for the Load Balancer and Oracle Internet Directory When Upgrading Oracle Application Server Cluster (Identity Management)"
- Section 2.2.5, "Harmless Error Messages During OracleAS Metadata Repository Upgrade"
- Section 2.2.6, "Metadata Repository Container Version"
- Section 2.2.7, "Issues When Using the ldifwrite Command to Back Up the Oracle Internet Directory"
- Section 2.2.8, "Upgrade of OracleAS Cold Failover Clusters Fails While Running Configuration Assistant"

2.2.1 Clarification of When to Run the Metadata Repository Upgrade Assistant

When you are upgrading to 10*g* Release 2 (10.1.4.0.1), the Oracle Universal Installer upgrades the OracleAS Identity Management schemas in your database to 10*g* Release 2 (10.1.4.0.1). This procedure is documented in Chapter 7 of the 10*g* Release 2 (10.1.4.0.1) *Oracle Application Server Upgrade and Compatibility Guide*.

However, Oracle Universal Installer does not upgrade the other component schemas in the OracleAS Metadata Repository, such as the OracleAS Portal and OracleAS Wireless schemas.

To determine whether or not you need to run the Metadata Repository Upgrade Assistant (MRUA) to upgrade the component schemas, consider the following:

- If all the Oracle Application Server middle tiers in your Oracle Application Server environment are currently 10*g* Release 2 (10.1.2) middle tiers, then it is not necessary to run MRUA, because the component schemas should already be 10*g* Release 2 (10.1.2) schemas.

  However, you can use the 10*g* Release 2 (10.1.4.0.1) MRUA to do the following:

  - Verify that the proper component schemas are installed and valid
  - Verify that the database that hosts the OracleAS Metadata Repository has been upgraded to a supported version.

- If you are currently running Oracle Application Server 10*g* (9.0.4) middle tiers, then refer to Chapter 5 of the *Oracle Application Server Upgrade and Compatibility Guide* to determine whether or not you need to upgrade your middle tiers to 10*g* Release 2 (10.1.2). If you must upgrade your middle tiers to 10*g* Release 2 (10.1.2), then you must first run MRUA to upgrade the component schemas to 10*g* Release 2 (10.1.2).

2.2.2 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 10*g* 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 10*g* 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 10*g* 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;
```

2.2.3 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 10*g* (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 My Oracle Support at `https://support.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.

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

The procedure for upgrading to 10*g* (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 10*g* (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.

2.2.5 Harmless Error Messages During OracleAS Metadata Repository Upgrade

When you upgrade your OracleAS Metadata Repository *ORACLE_HOME* to 10*g* (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.

2.2.6 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 10*g* (10.1.4.0.1) release. Upgrades from the 10*g* (10.1.4.0.1) release to the OracleAS Portal (10.1.4.0.0) release is therefore supported.

2.2.7 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.

2.2.8 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, "Possible Error Message When Decommissioning a 10.1.4.0.1 Oracle Home After Upgrade"
- Section 2.3.2, "Incorrect Line Breaks in MRUA Sample Output"
- Section 2.3.3, "Incorrect Global Database Naming Standard"

2.3.1 Possible Error Message When Decommissioning a 10.1.4.0.1 Oracle Home After Upgrade

Section 10.2, "Task 2: Decommission the OracleAS Identity Management Source Oracle Home," in the *Oracle Application Server Upgrade and Compatibility Guide* includes instructions for removing the source OracleAS Identity Management instance from the OracleAS Farm. The goal of this procedure is to remove the 10*g* (10.1.2) instance from the list of Oracle Application Server instances in the farm after you have completed the upgrade to 10*g* (10.1.4.0.1).

However, in some cases, when you run the `dcmctl leavefarm` command, as documented in that section, the command fails with the following error:

```
ADMN-705002
```

This error can be safely ignored; proceed to the next step in the procedure. There is no harm in leaving the 10*g* (10.1.2) Oracle home in the list of instances for the farm and in most cases the instance will be removed when you deinstall the instance with Oracle Universal Installer, as described in the next step of the procedure.

2.3.2 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
```

2.3.3 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.

3

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. If 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 10*g* (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 workaround 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 10*g* 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:

   ```
   (UNIX) Oracle_Home/config/ias.properties
   (Windows) 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 Consoleincludes 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.

4

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, "Upgrade to OracleAS Guard Release 10.1.2.2.1"
- Section 4.1.2, "Problem Performing a Clone Instance or Clone Topology Operation"
- Section 4.1.3, "OracleAS Guard Release 10.1.2.1.1 Cannot Be Used with Oracle RAC Databases"
- Section 4.1.4, "OracleAS Guard Returned an Inappropriate Message When It Could Not Find the User Specified Database Identifier"

4.1.1 Upgrade to OracleAS Guard Release 10.1.2.2.1

Oracle recommends that you upgrade your systems to release 10.1.2.2.1 of OracleAS Guard using the standalone OracleAS Guard kit 10.1.2.2.1 installation kit, which is available on Oracle Technology Network at:

`http://www.oracle.com/technology/index.html`

4.1.2 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.

4.1.3 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.

4.1.4 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 that the Oracle instance SID, there was no indication that this was the problem.

Now if OracleAS Guard is unable to locate the oratab entry (on Unix) or the system registry service (on Windows) 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:

```
On Unix systems:

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

On Windows systems:

ASG_SYSTEM-100: An Oracle database is identified by its system identifier (SID)
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"
- Section 4.2.2, "Database SIDs Must be the Same for Database Peers at Primary and Standby Sites"
- Section 4.2.3, "Use All Uppercase Characters for Database Initialization Parameters to Avoid Instantiate and Sync Problems"
- Section 4.2.4, "Use the Same Port for ASG on the Production and Standby Sites to Avoid clone instance Operation Problems"
- Section 4.2.5, "Use Fully Qualified Path Names with the add instance Command"
- Section 4.2.6, "ASG Cloning is Not Supported when the Number of Oracle Homes is Different at the Primary and Standby Hosts"
- Section 4.2.7, "Entries in TNSNAMES.ORA File that Lack Domain Names Cause Disaster Recovery Problems"

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.

4.2.2 Database SIDs Must be the Same for Database Peers at Primary and Standby Sites

The SIDs must be the same for database peers at a primary site and standby site(s) in a Disaster Recovery topology.

4.2.3 Use All Uppercase Characters for Database Initialization Parameters to Avoid Instantiate and Sync Problems

Use all uppercase characters for database initialization parameters.

In the following example, the database initialization parameter, service, that is used in the archive log destination parameter is in all uppercase characters (SERVICE):

```
log_archive_dest_2="SERVICE=SIDM valid_for=(online_logfiles,primary_role)
db_unique_name=SIDM"
```

But in the following example, the database initialization parameter, service, that is used in the archive log destination parameter is in lowercase characters (service):

```
log_archive_dest_2="service=SIDM valid_for=(online_logfiles,primary_role)
db_unique_name="SIDM"
```

When the database initialization parameter is not in all uppercase characters, error messages similar to the following can occur during an `instantiate topology` or `sync topology` operation:

```
stajo05: -->ASG_DUF-4950: An error occurred on host "stajo05" with IP
"140.87.25.33" and port "7890"
stajo05: -->ASG_SYSTEM-100: String index out of range: -9
stajo05: -->ASG_DUF-3760: Failed to query archive log destination
information.
stajo05: -->ASG_IAS-15753: Error preparing to instantiate the topology on
host "stajo05"
stajo05: -->ASG_DUF-3027: Error while executing Instantiating each instance
in the topology to standby topology at step - prepare step.
```

4.2.4 Use the Same Port for ASG on the Production and Standby Sites to Avoid clone instance Operation Problems

Use the same port for ASG on the primary site and standby site(s) to avoid error messages such as the following during a `clone instance` operation:

```
3-May 15:45:43  >>clone instance prodsso1 to stbyinfra1
3-May 15:45:43  stamx11: -->ASG_DUF-4950: An error occurred on host
"stamx11" with IP "140.87.21.201" and port "7890"
stamx11: -->ASG_DUF-3601: Error connecting to server host 152.68.64.213
on port 7890
stamx11: -->ASG_DUF-3512: Error creating remote worker on node 152.68.64.213:7890.
```

The dsa.conf file contains ASG configuration information, and it is configured into the Application Server instance's backup/restore IP configuration. The dsa.conf file configuration is handled symmetrically between Application Server instances. Due to this, the dsa.conf file from a production site's instance will be synchronized to the corresponding standby site's instance.

The port numbers between the production and standby instance pairings should match for ASG.

4.2.5 Use Fully Qualified Path Names with the add instance Command

As a best practice, use fully qualified path names with the `add instance` command.

4.2.6 ASG Cloning is Not Supported when the Number of Oracle Homes is Different at the Primary and Standby Hosts

The ASG `clone topology` and `clone instance` commands are not supported by DR configurations if there are a different number of Oracle Homes at the primary and standby hosts.

As part of the cloning operation, the Oracle Inventory for each host is cloned. Therefore, the assumption is that the Oracle Home configuration is symmetrical for any host that is being cloned.

For a full description of supported Disaster Recovery asymmetric topologies, refer to Section 5.1.3.2 of the *Application Server High Availability Guide* for release 10.1.3.2.0.

4.2.7 Entries in TNSNAMES.ORA File that Lack Domain Names Cause Disaster Recovery Problems

In previous 10.1.x releases, database entries in the TNSNAMES.ORA file were created without the domain name.

Disaster Recovery may experience problems with `instantiate topology` or other ASG operations if any database entries in the TNSNAMES.ORA file lack domain names.

For example, this entry in the TNSNAMES.ORA file lacks the domain name and could cause problems for Disaster Recovery:

```
ORCL1 =
 (DESCRIPTION =
   (ADDRESS_LIST =
     (LOAD_BALANCE = yes)
     (ADDRESS = (PROTOCOL = TCP)(HOST = idmdrtest)(PORT = 1521))
   )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl1.pdx.com)
     )
   )
 )
```

In this case, to prevent problems with Disaster Recovery, add the domain name (PDX.COM) to the TNSNAMES.ORA entry (bolded below):

```
ORCL1.PDX.COM =
 (DESCRIPTION =
   (ADDRESS_LIST =
     (LOAD_BALANCE = yes)
```

```
     (ADDRESS = (PROTOCOL = TCP)(HOST = idmdrtest)(PORT = 1521))
   )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl1.pdx.com)
     )
   )
 )
```

By adding the domain name to TNSNAMES.ORA file entries, you may be able to avoid error messages such as the following that can occur during an `instantiate topology` operation:

```
>>instantiate topology to voidhost1

idmdrtest.pdx.com 10.196.6.80:7892 (home /home/oracleqa/DREDG/immr10142)
     HA directory exists for instance im1.idmdrtest.pdx.com
     HA directory exists for instance orcl1

idmdrtest.pdx.com 10.196.6.150:7892 (home /home/oracleqa/DREDG/immr10142)
     HA directory exists for instance im1.idmdrtest.pdx.com
     HA directory exists for instance orcl1

idmdrtest.pdx.com 10.196.6.80:7892
   Verifying that the topology is symmetrical in both primary and standby
configuration

idmdrtest.pdx.com 10.196.6.80:7892 (home /home/oracleqa/DREDG/immr10142)
    This is primary infrastructure host
idmdrtest.pdx.com: -->ASG_DUF-4950: An error occurred on host
"idmdrtest.pdx.com" with IP "10.196.6.80" and port "7892"
idmdrtest.pdx.com: -->ASG_ORACLE-300: ORA-12560: TNS:protocol adapter error
idmdrtest.pdx.com: -->ASG_DUF-3700: Failed in SQL*Plus executing SQL
statement:  connect sys/******@orcl1.pdx.com as sysdba;.
idmdrtest.pdx.com: -->ASG_DUF-3502: Failed to connect to database
orcl1.pdx.com.
idmdrtest.pdx.com: -->ASG_IAS-15753: Error preparing to instantiate the
topology on host "idmdrtest.pdx.com"
idmdrtest.pdx.com: -->ASG_DUF-3027: Error while executing Instantiating each
instance in the topology to standby topology at step - prepare step.

>>disconnect
```

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.
```

5

Oracle Access Manager

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

See Also: The following documents for more information:

- *Oracle Access Manager Release Notes 10g (10.1.4.3.0) For All Supported Operating Systems E12496-02* for known issues with the full-installer release
- *Oracle Access Manager Patch Set Notes, Release 10.1.4 Patch Set 2 (10.1.4.3.0) for All Supported Platforms* for enhancements, bug fixes, and known issues with the patch set: oam_101430_readme.pdf
- *Oracle Access Manager Patch Set Notes, Release 10.1.4 Patch Set 1 (10.1.4.2.0) for All Supported Platforms* for enhancements and bug fixes available with this patch set: oam_101420_readme.pdf

5.1 About Installation Packages, Patch Sets, Bundle Patches, and Newly Certified Agents

This section provides information and distinctions on the following Oracle Access Manager product packages:

5.1.1 Full Installer Packages

Oracle provides full installer packages for major Oracle Access Manager releases:

- 10*g* (10.1.4.3)
- 10*g* (10.1.4.0.1)

> **Note:** Oracle Access Manager 10*g* (10.1.4.2.0) was a patch set only.

Each full installer package provides the libraries and files that comprise a complete software distribution and implement all product functionality. Full installer packages are provided for every component on supported platforms. All of the components have been tested and are certified to work with one another across supported platforms.

> **Note:** You can use 10*g* (10.1.4.3) installers to create a fresh Oracle Access Manager installation only. You can apply the 10*g* (10.1.4.3) patch set to update 10*g* (10.1.4.2.0) components as described in Section 5.1.2.1, "Updating Oracle Access Manager 10g (10.1.4) with the Latest Patch Sets".

An Oracle Media Pack is an electronic version of Oracle software products on physical media (DVDs). Physical Oracle Media Packs are available to any customer working with a Sales Representative. In addition, you can order a physical Media Pack from the Oracle store. Shop online at: `http://oracle.com`.

Virtual DVDs and Media Packs are available as follows:

- From Oracle Technology Network (OTN) at:

  `http://www.oracle.com/technology/software/products/middleware/htdocs/fmw_11_download.html`

  Use the following links to download Oracle Access Manager 10*g* (10.1.4.3):

  - **Access Manager Core Components (10.1.4.3.0)**

    See Also: *Oracle Containers for J2EE Security Guide* to implement SSO for Oracle Fusion Middleware 11g using the OAM Configuration tool (available with 10*g* (10.1.4.3) core components) and the OAM Identity Assertion Provider (available with 10*g* (10.1.4.3) WebGates for OHS 11g).

  - **Access Manager WebGate (10.1.4.3.0)**
  - **Policy Manager and WebPass on Third Party and non-OHS 11g Web Servers**
  - **Access Manager Language Packages (10.1.4.3.0)**
  - **GCC Libraries**

    > **Note:** Get Oracle Access Manager 10*g* (10.1.4.3) WebGates for third-party and non-OHS 11g Web servers from:
    >
    > `http://www.oracle.com/technology/software/products/ias/htdocs/101401.html`

- From Oracle edelivery at:

  http://edelivery.oracle.com/EPD/Search/get_form

  Oracle edelivery provides access to Oracle Fusion Middleware Media Packs that mirror the contents of the physical Media Pack bundle.

5.1.2 Patch Sets, Bundle Patches, and Patch Set Exceptions

Table 5–1 provides a brief overview of the differences between a standard patch set (10*g* (10.1.4.2.0), for instance), a bundle patch, and a patch set exception.

Table 5–1 Bundle Patches, Patch Sets, and Patch Set Exceptions

Mechanism	Description
Patch Set	A patch set is a mechanism for delivering fully tested and integrated product fixes that can be applied to installed components of the same release. Each patch set provides the libraries and files that have been rebuilt to implement bug fixes (and new functions, if any). All of the fixes and functions in the patch set have been tested and are certified to work with one another on specified platforms. Patch sets include all of the fixes available in previous bundle patches (or patch set exceptions) for the release. A patch set might not be a complete software distribution and might not include packages for every component on every platform. **See Also**: Section 5.1.2.1, "Updating Oracle Access Manager 10g (10.1.4) with the Latest Patch Sets".
Bundle Patch	A bundle patch is an official Oracle patch for Oracle Access Manager components on baseline platforms. Bundle patches are released on a regular basis, *after* one product release and *before* the next. Each bundle patch includes the libraries and files that have been rebuilt to implement one or more fixes and functions. All of the fixes and functions in the bundle patch have been tested and are certified to work with one another. Regression testing has also been performed to ensure backward compatibility with all Oracle Access Manager components in the bundle patch, and with earlier WebGates Each bundle patch is cumulative: the latest bundle patch includes all fixes in earlier bundle patches for the same release and platform. Fixes delivered in bundle patches are rolled into the next release: all 10*g* (10.1.4.2.0) bundle patch fixes are included in Oracle Access Manager release 10*g* (10.1.4.3). **See Also**: Section 5.1.2.2, "Retrieving the Latest Bundle Patch".
Patch Set Exception (PSE)	Each PSE was an official Oracle patch; however, a PSE was *not* a complete product distribution and did not include packages for every component on every platform. Each PSE (also known as a *one off* or *hot fix*) addressed only one issue for a single component; typically (*but not always*) only for a single platform. A PSE included only the libraries and files that had been rebuilt to implement a specific fix for a specific component. Each PSE was cumulative, but did not undergo extensive regression testing and certification by QA. Individual PSE releases were not tested to work together with other PSE releases. **Note**: The bundle patch mechanism has replaced the patch set exception mechanism.

5.1.2.1 Updating Oracle Access Manager 10*g* (10.1.4) with the Latest Patch Sets

Your starting Oracle Access Manager release determines the patch sets you need, as described in Table 5–2.

Table 5–2 Updating Oracle Access Manager

If Your Starting Release is ...	You Must ...
10*g* (10.1.4.0.1)	Perform both steps in the following procedure to: 1. Apply the 10*g* (10.1.4.2.0) patch. 2. Apply the 10*g* (10.1.4.3) patch.
10*g* (10.1.4.2.0)	Skip Step 1 and apply only the 10*g* (10.1.4.3) patch

Note: See the patch set notes for 10*g* (10.1.4.2.0) and 10*g* (10.1.4.3) for details about enhancements and bug fixes available with each release, as well as any known issues.

To obtain the latest patch sets

1. 10*g* (10.1.4.2.0) **Patch**:
   a. Go to My Oracle Support and log in as usual:

      `https://support.oracle.com`

   b. Click **Patch ID or Number**.
   c. In the empty field, enter**5957301**, and then click **Search**.
   d. In the **Patch Search Results** table, click the number beside the item that corresponds to your platform.
   e. **Readme**: Click the **View Readme** button to display the Release Notes, which you can print.
   f. **Download**: Click the **Download** button to acquire the packages.
   g. **Installation**: See the Readme (oam_101420_readme.pdf) for all prerequisites, patch install, post-patching instructions, and more.
2. 10*g* (10.1.4.3) **Patch**:
   a. Go to My Oracle Support and log in as usual:

      `http://support.oracle.com`

   b. Click **Patch ID or Number**.
   c. In the empty field, enter**8276055**, and then click **Search**
   d. In the **Patch Search Results** table, click the number beside the item that corresponds to your platform.
   e. **Readme**: Click the **View Readme** button to display the Release Notes, which you can print.
   f. **Download**: Click the **Download** button to acquire the packages.
   g. **Installation**: See the Readme (oam_101430_readme.pdf) for all prerequisites, patch install, post-patching instructions, and more.

5.1.2.2 Retrieving the Latest Bundle Patch

Oracle releases bundle patches to correct any reported issues in your deployment. Oracle recommends that you obtain and apply the latest bundle patch.

To download a 10*g* (10.1.4.3) bundle patch

1. On the machine that will host the bundle patch files, create a temporary directory to contain the platform-specific bundles that you will download. For example:

   Unix : /home/*10143BPnn*/tmp
   Windows: C:*10143BPnn*\tmp

2. Go to My Oracle Support and log in as usual:

   `http://support.oracle.com`

3. Click the **Patches & Updates** link.
4. Click **Product or Family (Advanced Search)** and fill in the search criteria. For example:
   a. From the **Product is** list, click **Oracle Oblix COREid**.
   b. From the **Release is** list, click **Oracle Access Manager 10.1.4.3**.
   c. From the following list, select **Platform**.
   d. From the list of platforms, select all that apply.
   e. Click the **Search** button.
   f. In the **Patch Search Results** table: Locate the latest bundle patch (top of the list) and click the corresponding number.
5. **Readme**: Click the **View Readme** button to display the Release Notes, which you can print.
6. **Download**: Click the **Download** button to retrieve the packages.
7. **Installation**: See the Readme (oam_101430_bp*nn*_doc.pdf) for all prerequisites, patch install, post-patching instructions, and more.

5.2 General Issues

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

5.2.1 New Location for the Platform Support Matrix

Oracle continually certifies Oracle Access Manager support with various third-party platforms, Web server releases, directory server releases, and applications. For the latest support details, see the certification matrix that is available at:

`http://www.oracle.com/technology/products/id_mgmt/coreid_acc/pdf/oracle_access_manager_certification_10.1.4_r3_matrix.xls`

5.2.2 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.

5.2.3 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.

5.2.4 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
```

To implement automatic login after password change with a form-based authentication scheme, you must configure the challenge parameter `creds` by supplying the user name credential parameter as the first token, the password credential parameter as the second token, then any other credential parameters.

5.2.5 Time Management and Daylight Savings Time

Time management includes changes for daylight savings time. In the United States, the Energy Policy Act of 2005 was signed into law to extend daylight saving time. In calendar year 2007, the effective dates for daylight savings are going to change. Under the new rules, DST in the U.S. will start on the second Sunday in March and end the first Sunday in November. In the past, daylight savings time started on the first Sunday in April and ended the last Sunday in October. This change also affects Canada.

USA 2007 Daylight Saving Time (DST) Compliance for Oracle Access Manager: No patches are required for the Identity Server or Access Server to accommodate daylight savings time changes. However, Oracle Access Manager interacts with other components that may be impacted by DST changes such as Web servers, applications servers, LDAP directories and databases. Check your vendor documentation and ensure that any required patches are applied to other affected components.

Follow the recommendations of Operating System vendors for any required DST changes. In addition, ensure that system clocks of computers hosting Oracle Access Manager components are synchronized as discussed in the *Oracle Access Manager Installation Guide*.

For more information about the impact of USA 2007 DST compliance for Oracle Database and Oracle Fusion Middleware products, see Note: 397281.1 on the My Oracle Support Web Site:

https://support.oracle.com

5.2.6 Caveat to Create a Password Policy with Change on Reset Enabled

A caveat has been added to *Oracle Access Manager Identity and Common Administration Guide*, chapter on "Configuring Global Settings," in the section on "Creating Password Policies for a Specific Domain." See Step 16 of the procedure "To create a password policy" for the following new note.

16. Select Change on Reset if you want to force users to change the password the first time they log in to the system after an administrator resets the password.

By default, the Change on Reset flag is not set. During self-registration, the Change on Reset flag is not set.

This field is applicable to both the Identity and Access Systems. For the Access System only, you can also configure a redirect URL for password change. See "Configuring Password Redirect URLs" on page 7-66 for details.

Note: Use of password policies in the Access System with change on reset functionality enabled and without specifying a Password Change Redirect URL will cause the login prompt to redisplay. This prevents users from changing passwords and ultimately logging in.

5.2.7 Login.html Not Found if Browser Language is Not Supported

Out of the box, Oracle Access Manager internationalized login pages support 27 languages. After customizing external pages, however, you might have only a subset of the 27 supported languages for your Oracle Fusion Applications. For instance, you might have added translation text to your HTML pages that can be translated to only a select few languages.

To avoid additional changes, you must remove support for the unsupported languages in three locations, as follows:

1. Perl Script configuration (config.pl file): Update the Config.pl Language Mapping array to remove unsupported languages: simply comment out unsupported language lines.

   Note: Perl Script configuration refers to the config.pl file, which is copied to the Web server directory during installation.

   ---

2. JavaScript configuration: Remove unsupported languages from Language Array to eliminate their display in Language Selection LOV: simply comment out the lines for unsupported languages.
3. *WebGate_install_dir*: Manually remove (or simply move) directories containing unsupported languages. For example, if you have no support for Korean (and Greek), remove *WebGate_install_dir*/access/oblix/lang/ko-kr (and /lang/el-gr).

5.3 Installation and Upgrade Issues and Workarounds

To ensure success when upgrading older releases to Oracle Access Manager 10*g* (10.1.4), 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 6.1.1.

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

5.3.1 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."

5.3.2 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

5.3.3 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=dsaconfig, cn=configsets, cn=oracle internet directory
changetype: modify
add: orclinmemfiltprocess
orclinmemfiltprocess:
(|(obuseraccountcontrol=activated)(!(obuseraccountcontrol=*)))
orclinmemfiltprocess:
(|(!(obuseraccountcontrol=*))(obuseraccountcontrol=activated))
eof
```

In the sample command, <*host*> and <*port*> refer to the Oracle Internet Directory installation host and port.

> **Note:** Be sure to include a space after the attribute orclinmemfiltprocess: and at the start of each continuation line of the attribute value. There is no line break between the attribute orclinmemfiltprocess: and the continuation line. Repeat the above step for each additional Oracle Internet Directory Server that you install

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

5.3.4 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.

5.3.5 "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.

5.3.6 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.

5.3.7 Simple Mode Password File Not Converted During Upgrade

If the earlier Access Server is in Simple mode before the upgrade, during the upgrade the password.lst file might not be converted to password.xml. The result is that the Access Server cannot be started in the Services Window unless you use the command-line parameters to convey the passphrase on startup. Also, after upgrading a WebGate in Simple mode and starting the Web server, the following error may appear:

```
"Exception thrown during WebGate initialization"
Error^Oracle AccessGate API is not initialized.
```

The initial Access System page appears. However, clicking on any link results in a "Server error" in the browser (no error number) with the above error echoed to the console. The system cannot be accessed.

The upgraded area does not have the updated password.xml file.

> **Note:** In releases before 10*g* (10.1.4), the password file is named and formatted as password.lst. Starting with release 10*g* (10.1.4), the password file is named and formatted as password.xml

The following information is a workaround for this problem when the same Simple mode password is being used in the Identity System. In this case, you can copy the password.xml file from the upgraded Identity Server to the upgraded Access Server and WebGate as described in the following procedure.: "Workaround when the same Simple mode password is used in the Identity System". You will be asked about the password immediately after selecting Simple mode.

However, if the password is not the same on the Identity Server as it is on the Access Server, skip to the following procedures. Again, you will be asked about the password immediately after selecting Simple mode:

- Workaround when the Simple mode password is different on the Identity System and Access Server
- Workaround when the Simple mode password is different on the Identity System and WebGate

Workaround when the same Simple mode password is used in the Identity System

1. If the same Simple mode password is being used in the Identity System, copy the password.xml file as follows:

   From: <*upgraded_IdentityServer_install_dir*>/oblix/config/password.xml
   To: <*upgraded_AccessServer_install_dir*>/oblix/config /password.xml
   and
   To: <*upgraded_WebGate_install_dir*>/oblix/config/password.xml

2. Start the Access Server.
3. Restart the WebGate Web server.

If the Access System Simple mode password is not the same as the Identity System Simple mode password, you must change the password using the following tools and procedures.

<*AccessServer_install_dir*>/access/oblix/tools/configureAAAServer
<*WebGate_install_dir*>/access/oblix/tools/configureWebGate

Workaround when the Simple mode password is different on the Identity System and Access Server

1. Go to the folder where configureAAAserver is located. For example:

   ```
   AccessServer_install_dir\access\oblix\tools\configureAAAServer
   ```

2. Run the following executable:

   ```
   configureAAAServer chpasswd AccessServer_install_dir
   ```

3. Responds to prompts as directed on the screen.
4. Restart the Access Server.

Workaround when the Simple mode password is different on the Identity System and WebGate

1. Go to the directory:

   WebGate_install_dir\access\oblix\tools\configureWebGate

   where *WebGate_install_dir* is the directory in which WebGate is installed.

2. Run the following command:

   ```
   configureWebGate -i WebGate_install_dir -t WebGate -k
   ```

   The -k option results in only prompts for the password for Simple or Cert mode transport security.

3. Respond to prompts on the screen.
4. Restart the WebGate Web server.

For more information about the configureAAAServer and configureWebGate tools, see the *Oracle Access Manager Access Administration Guide*.

5.3.8 Unnecessary Message Asks for SDK Migration Bundles During Upgrade

During an upgrade, the 10*g* (10.1.4.0.1) installer asks for migration bundles and instructs you to place these in a specific directory. The following information provides a workaround for this problem:

Ignore the following message, which will be removed from the Software Developer Kit (SDK) installer.

```
Please download and extract COREid 6.5 migration bundles

To ensure success when upgrading a COREid 6.5 installation, you
need to perform the following steps before you continue. For
information, see the Oracle Access Manager Upgrade Guide chapter
on preparing your environment.

1) Log in to the download Web site.

   http://www.oracle.com/support/contact.html

Retrieve appropriate _msg and _param files for the older version of this
component.

For example:
Netpoint_65_orig_en_<Component>_msg.zip
Netpoint_65_orig_<Component>_param.zip

Note: Retrieve only the files that are relevant to your older installation.
Files for version 6.5 include _65_ in their name; files for version 6.5.2 or
later include _652_ in their name.

Press ENTER to read the text [Type q to quit].

3) Extract or unzip these files in to your <Component Installation Directory>.

 For example:
 <Component Installation Directory>/identity
 <Component Installation Directory>/access

A directory named "orig" is created during this process. For example:
```

```
<Component Installation Directory>/identity/oblix/orig.
<Component Installation Directory>/access/oblix/orig.

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
```

5.3.9 Unable to Locate Bundles Needed for COREid 6.x Upgrades

The *Oracle Access Manager Upgrade Guide* discussion on preparing release 6.x environments includes details about obtaining specific COREid 6.x bundles from the installation media before upgrading. However, the files are not available on the media.

The following information is a workaround for this problem. Before you upgrade from a COREid 6.x installation to 10*g* (10.1.4), you must perform the following steps to download the missing packages, which contain text files for use on any platform.

> **Note:** My Oracle Support was formerly MetaLink.

1. In your browser, enter the My Oracle Support URL and log in:

   `https://support.oracle.com`

2. Click **Patches & Updates**, then click **Patch ID or Number**.
3. In the **Patch ID or Number** field, enter **`5724938`**, then click the **Search** button.

   The results of your search for Patch 5724938 are displayed with the description: UNABLE TO LOCATE MIGRATION BUNDLE FOR 6.5-10.1.4 UPGRADE.

   > **Note:** The Platform is automatically specified as Microsoft Windows 2000 because the bundles contain only text files that can be used on any platform; there are no binary files.

4. Click the **Download** button and follow instructions on the screen.
5. Before you continue upgrading review following discussions, then extract files and finish preparing components as described in *Oracle Access Manager Upgrade Guide*:

   - Packages for Release 6.5.0.x
   - Packages for Release 6.5.2.x Patch

   > **Note:** As described in "Ignore Bundles for Release 6.5 with Multi-language Capability" on page 5-14, multi-language bundles are not needed and are not available.

Packages for Release 6.5.0.x

A new package has been added for release 6.5: Netpoint_65_orig_en_AccessServerSdk_msg.zip. Before you upgrade from Oracle Access Manager 6.5.0.x, you must download and add the following packages to your original *Component_install_dir*.

Extract 65-orig Packages to the Original *Component_install_dir*
Netpoint_65_orig_en_COREid_Server_msg.zip
Netpoint_65_orig_COREid_Server_param.zip
Netpoint_65_orig_en_Access_Manager_msg.zip
Netpoint_65_orig_Access_Manager_param.zip
Netpoint_65_orig_en_WebPass_msg.zip
Netpoint_65_orig_WebPass_param.zip
Netpoint_65_orig_en_Access_Server_msg.zip
Netpoint_65_orig_Access_Server_param.zip
Netpoint_65_orig_en_WebGate_msg.zip
Netpoint_65_orig_WebGate_param.zip
Netpoint_65_orig_en_AccessServerSdk_msg.zip

Packages for Release 6.5.2.x Patch

Two new packages have been added for 6.5.2: Netpoint_652_orig_AccessServerSdk_param.zip and Netpoint_652_orig_en_AccessServerSdk_msg.zip. If you originally installed release 6.5.0.x, then patched to 6.5.2.x, you must download and add the following packages to your original *Component_install_dir* before the upgrade.

Extract 652_orig Packages to the Original *Component_install_dir*
Netpoint_652_orig_en_COREid_Server_msg.zip
Netpoint_652_orig_COREid_Server_param.zip
Netpoint_652_orig_en_WebPass_msg.zip
Netpoint_652_orig_WebPass_param.zip
Netpoint_652_orig_en_Access_Manager_msg.zip
Netpoint_652_orig_Access_Manager_param.zip
Netpoint_652_orig_en_Access_Server_msg.zip
Netpoint_652_orig_Access_Server_param.zip
Netpoint_652_orig_en_WebGate_msg.zip
Netpoint_652_orig_WebGate_param.zip
Netpoint_652_orig_AccessServerSdk_param.zip
Netpoint_652_orig_en_AccessServerSdk_msg.zip

Ignore Bundles for Release 6.5 with Multi-language Capability

The *Oracle Access Manager Upgrade Guide* states that certain multi-language packages may be required for an upgrade from release 6.5 to 10*g* (10.1.4). However, multi-language bundles are not needed and are not available. Ignore information in the *Oracle Access Manager Upgrade Guide* on "Preparing Multi-Language Installations."

5.3.10 Problem with Automatic Directory Updates During Identity Server or Policy Manager Installation

When using Novell eDirectory, an error occurs during directory server updates for Identity Server installation. If you have a separate directory for policy data, this error also occurs during Policy Manager installation:

```
"Error 16: Unable to update Identity System Configuration - Unknown LDAP error
occurred."
```

The index is applied with one exception for the `obLPMname` attribute, even though the error message may give the impression that the entire operation has failed.

The following is a workaround for this problem. For more information, see your Novell eDirectory documentation.

1. Dismiss the error message.
2. Using the Novell index management tool, manually index the `obLPMname` attribute for equality.

5.3.11 Challenge Parameter Rows Discarded During the Master Access Manager Upgrade

After you upgrade from Oracle Access Manager 7.0.4 to 10.1.4.0.1, any authentication scheme that contains multiple challenge parameter rows are truncated. Only the first challenge parameter row remains. The others are deleted.

Note: This problem was fixed in release 10.1.4.2.0. After upgrading to 10.1.4.2.0, all challenge parameters are preserved.

See Also: Section 5.1.2.1, "Updating Oracle Access Manager 10g (10.1.4) with the Latest Patch Sets"

5.3.12 No Translation Support for the SNMP Agent Installshield

There is no translation support for the SNMP agent installshield wizard.

5.3.13 Installation of Identity Server 10.1.4.0.1 With Sun Java Directory Server 6.0

Problem

Installation of a 10*g* (10.1.4) Identity Server with Sun Java Directory Server 6.0 fails when you are defining directory details. The following error will occur if you specify Sun Directory Server 5.x, and you supply the Sun Directory Server 6 hostname, port number, and credentials, and choose Yes to automatically update the LDAP server schema configuration:

```
Error 32: LDAP Invalid credentials. Or invalid directory type supplied. Or no such
object.
```

This can also occur when installing the Policy Manager with the Sun Directory Server 6.

Cause

Certification of the Sun Java Directory Server 6.0 with Oracle Access Manager 10*g* (10.1.4) occurred after 10*g* (10.1.4.0.1) was released. As a result, during Identity Server

installation there is no option to select Sun Java Directory Server 6.0. If Sun Directory Server 5.x is selected, the configuration fails when performing an automatic schema update.

When installing with Sun Java Directory Server 6.0, the automatic schema update option cannot be used. The schema must be updated manually.

Solution

1. Install Oracle Access Manager as described in the *Oracle Access Manager Installation Guide*, and choose the Sun Directory Server 5.x option.
2. Provide the Sun Directory Server 6 hostname, port number, and credentials.
3. Using either the Sun Java System Directory Server 6.0 Management Console, or ldapmodify command line, load the Oracle Access Manager schema and index files into Sun Java System Directory Server 6.0 using the following ldif files:

   LDAP server instance hosting user data only:

   ```
   IdentityServer/identity/oblix/data.ldap/common/iPlanet_user_schema_add.ldif
   IdentityServer_installdir/identity/oblix/data.ldap/common/iPlanet5_user_index_
   add.ldif
   ```

   LDAP server instance hosting user data and configuration data (or configuration data and policy data, or policy data only):

   ```
   installdir/identity|access/oblix/data.ldap/common/iPlanet_oblix_schema_add.ldif
   installdir/identity|access/oblix/data.ldap/common/iPlanet5_oblix_index_add.ldif
   ```

   In the previous path name, the pipe between identity | access indicates "or". If you are installing the Identity Server the path will be the *IdentityServer_installdir*/identity and if you are installing Policy Manager the path will be *PolicyManager_installdir*/access.

   Note: For an example of the ldapmodify command, see the Sun document at: http://docs.sun.com/app/docs/doc/819-0995/6n3cq3avf?a=view

4. Proceed to Identity Server or Policy Manager setup, as usual.

   Note: Oracle Support strongly recommends that you apply the latest patch sets and bundle patch immediately after installation. For more information, see Section 5.1, "About Installation Packages, Patch Sets, Bundle Patches, and Newly Certified Agents".

5.4 Removal and Rollback Issues and Workarounds

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

5.4.1 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*.

5.4.2 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*.

5.4.3 Rollback Issues After Upgrading to Oracle Access Manager 10*g* (10.1.4)

Changes in the way Oracle Access Manager 10*g* (10.1.4) uses the obVer attribute in oblixOrgPerson and oblixConfig may result in rollback issues following an upgrade from an earlier release to 10*g* (10.1.4). This will be documented in the next release of the *Oracle Access Manager Upgrade Guide*. For more information, see Section 5.9, "Documentation Issues".

The following workaround will solve the rollback issue and will be documented in the next release of the *Oracle Access Manager Upgrade Guide*.

- Section 5.4.3.1, "Halting On-the-fly User Data Migration Phase 1"
- Section 5.4.3.2, "Halting On-the-fly Migration of User Data: Phase 2"
- Section 5.4.3.3, "Restarting On-the-fly User Data Migration"

5.4.3.1 Halting On-the-fly User Data Migration Phase 1

When you upgrade from an earlier release to Oracle Access Manager 10*g* (10.1.4), the configuration data stored in the `oblix` tree of the directory server is migrated automatically and the value of the obVer attribute is changed to 10.1.4.0. However, user data is not migrated until the first login following the upgrade. This means that the obVer attribute value remains less than 10.1.4.0 in user data (in the OblixOrgPerson class).

Unless you temporarily halt the immediate (also known as on-the-fly) user data migration as described in the task overview, the first time a user logs in after the upgrade to 10*g* (10.1.4) that user entry is immediately migrated. Any existing challenge and response values for that user are encoded (@1# is appended to the end) and the obVer attribute value for that user is changed to 10.1.4.0 in the OblixOrgPerson class. However the rollback process does not revert these changes. If you rollback to the previous release, the obVer value in the user entry in the OblixOrgPerson class remains 10.1.4.0 and challenge and response values remain encoded format.

Phase 1 must be performed after backing up data and before preparing host machines for the upgrade, as described in Chapter 5 of the *Oracle Access Manager Upgrade Guide*. Phase 1 includes setting the obVer attribute for the Master Administrator entry and then upgrading the schema and data to 10*g* (10.1.4). Phase 2 occurs after the schema

and data upgrade. In Phase 2, you remove the Challenge and Response semantic types at both the tab level and the object class level.

Before performing the following Phase 1 procedure, there are several conditions to take into account:

- If OblixOrgPerson does not exist in the objectclass list of the user entry, then you must first add it as described in step 1. Otherwise, start with step 2.
- After performing the last step, the lost password management feature will not work.

  After temporarily halting on-the-fly migration of user data at first login, Oracle recommends that you stop processing or performing the following actions to ensure that user data will maintain backward compatibility:

  - Stop processing workflow tickets: for example, create user, change attributes, and the like.
  - Stop modifying Challenge and Response attributes from the Modify Profile page.

To temporarily stop the immediate migration of user data (Phase 1)

1. Add OblixOrgPerson to the Master Administrator's user entry, if needed:

   ```
   ldapmodify.exe  -h <Host> \
   -p <Port>
   -D <Bind DN>
   -w <Bind Password> \
   -f <ldif file containing attribute to be added>
   ```

   The format of LDIF file to be created when adding OblixOrgPerson to the objectclass list is as follows. This example is for the Netscape Directory Server:

   ```
   dn: <Administrator DN>
   changetype: modify
   add: objectclass
   objectclass: OblixOrgPerson
   ```

2. Set the obVer attribute for the Master Administrator entry in the LDAP directory server to 7.0.4 using the following command:

   ```
   ldapmodify.exe  -h <Host> \
   -p <Port>
   -D <Bind DN>
   -w <Bind Password> \
   -f <ldif file containing attribute to be modified>
   ```

   The format of LDIF file to be created is as follows. This example is for the Netscape Directory Server:

   ```
   dn: <Administrator DN>
   changetype: modify
   replace: obver
   obver: 7.0.4
   ```

3. Finish remaining preparation tasks as described Chapter 5 the *Oracle Access Manager Upgrade Guide*.
4. Perform a schema and data upgrade for your deployment as described in Chapter 6 the *Oracle Access Manager Upgrade Guide* to, which includes instructions to

perform Phase 2 of this procedure. For more information, see Section 5.4.3.2, "Halting On-the-fly Migration of User Data: Phase 2".

5.4.3.2 Halting On-the-fly Migration of User Data: Phase 2

Before you perform Phase 2, you must have completed all activities in Chapter 5 as well as the following tasks described in Chapter 6 of the *Oracle Access Manager Upgrade Guide*. Chapter 6 prerequisite tasks include:

- Upgrading the Schema and Data with the Master Identity Server
- Upgrading the Master WebPass
- Verifying the Identity System Schema and Data Upgrade
- Uploading Directory Server Index Files
- Backing Up Upgraded Identity Data

Note: You must perform Phase 2 before any administrator or user login, even if you have a joint Identity and Access System deployment.

During Phase 2 you must remove the Challenge and Response semantic types at both the tab level and the object class level.

Caution: When you finish this Phase 2 procedure, lost password management will not work.

When you finish Phase 2, Oracle recommends that you stop processing or performing the following actions to ensure that user data will maintain its backward compatibility:

- Stop processing workflow tickets: for example, create user, change attributes, and the like.
- Stop modifying Challenge and Response attributes from the Modify Profile page.

To temporarily stop the immediate migration of user data (Phase 2)

1. After upgrading the schema and data, change the value of obVer in the configuration base to 7.0.4 as follows:

```
ldapmodify.exe  -h <Host> \
-p <Port>
-D <Bind DN>
-w <Bind Password> \
-f <ldif file containing attribute to be modified>
```

   A bind DN for configuration data (also known as the configuration DN) is similar to the searchbase for user data. The configuration bind DN must be specified to identify the node in the DIT under which the Oracle Access Manager schema and all configuration data is stored for the Identity and Access Systems.

   The format of LDIF file to be created is as follows. This example is for the Netscape Directory Server:

```
dn: o=oblix,<configuration DN>
changetype: modify
replace: obver
obver: 7.0.4
```

2. Restart the master Identity Server.
3. Go to the Identity System Console by specifying the URL for your environment, and then log in as the Master Administrator. For example:

   ```
   http://hostname:port/identity/oblix
   ```

   In the URL example, *hostname* refers to machine that hosts the WebPass Web server; port refers to the HTTP port number of the WebPass Web server instance; /identity/oblix connects to the Identity System Console.
4. **Tab Level**: Remove the Challenge and Response semantic types at the tab level, as follows:
   a. Click Identity System Console, click User Manager Configuration, and then click Tabs.
   b. From the Existing Tabs listed on the page, select Employees to display information about this Person class tab on the View Tab page.

      Note: Object Classes on the View Tab page may include OblixOrgPerson and others (gensiteorgperson, for example). The obVer attribute is a member of only the OblixOrgPerson class. There is no impact to other object classes.

   c. On the View Tab page, click Modify Attributes to open the Modify Attributes page.
   d. From the Attribute list select the attribute that is configured with Challenge as the Semantic Type, set the Semantic Type to None and click Save.
   e. From the Attribute list select the attribute that is configured with Response as the Semantic Type, set the Semantic Type to None and click Save.
   f. Click Done.
5. **Object Class Level**: Remove the Challenge and Response semantic types at the object class level, as follows:
   a. Click Identity System Console, click Common Configuration, and then click Object Classes.
   b. Select the person object class from the list, then click Modify Attributes to open the Modify Attributes page.
   c. From the Attribute list select the attribute that is configured with Challenge as the Semantic Type, set the Semantic Type to None and click Save.
   d. From the Attribute list select the attribute that is configured with Response as the Semantic Type, set the Semantic Type to None and click Save.
   e. Click Done.

For details about restarting user data migration after validating that your deployment is successfully upgraded, see Section 5.4.3.3, "Restarting On-the-fly User Data Migration".

5.4.3.3 Restarting On-the-fly User Data Migration

Before you perform this task, you must have performed all in-place upgrade tasks and validated that your entire upgraded deployment is operating as expected to ensure that no rollback is needed.

You use the procedure here to restart immediate (on-the-fly) user data migration:

- When immediate (on-the-fly) user data migration was temporarily halted.
- After validating that your upgraded deployment is operating as expected and that no rollback to the earlier release is needed

> **Note:** If you roll back to an earlier release after performing activities here, any user data that has been migrated will not be reverted.

In the following procedure you must reconfigure the attributes used for challenge and response at both the tab level and the object class level.

To restart one-the-fly user data migration

1. **Tab Level**: Reconfigure the Challenge and Response semantic types at the tab level, as follows:
   a. Click Identity System Console, then click User Manager Configuration, click Tabs.
   b. Select Employees from the list, then click Modify Attributes to open the Modify Attributes page.
   c. From the Attribute list select the attribute that is used for Challenge, set the Semantic Type to Challenge and the Display Type to Single Line Text, then click Save.
   d. From the Attribute list select the attribute that is used for Response, set the Semantic Type to Response and the Display Type to Password, then click Save.
   e. Click Done.
2. **Object Class Level**: Reconfigure the Challenge and Response semantic types at the object class level, as follows:
   a. Click Identity System Console, then click Common Configuration, click Object Classes.
   b. Select the person object class from the list, then click Modify Attributes to open the Modify Attributes page.
   c. From the Attribute list select the attribute that is used for Challenge, set the Semantic Type to Challenge and the Display Type to Single Line Text, then click Save.
   d. From the Attribute list select the attribute that is used for Response, set the Semantic Type to Response and the Display Type to Password, then click Save.
   e. Click Done.
3. Set the obVer attribute for oblixConfig (the configuration data root node in the LDAP directory server) to 10.1.4.0 as follows:

```
ldapmodify.exe  -h <Host> \
-p <Port>
-D <Bind DN>
-w <Bind Password> \
```

```
-f <ldif file containing attribute to be modified>
```

The format of LDIF file to be created is as follows. This example is for the Netscape Directory Server:

```
dn: o=oblix,<configuration DN>
changetype: modify
replace: obver
obver: 10.1.4.0
```

4. Restart all upgraded Identity Servers and Access Servers.

5.5 Access System Issues and Workarounds

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

5.5.1 Disabling the User Cache for the Access Server

As discussed in the *Oracle Access Manager Access Administration Guide*, you can configure a user cache for the Access Server. The guide omits the value you supply to disable this cache.

Provide a value of -1 in the Maximum Elements in User Cache field for the Access Server to disable the cache.

5.5.2 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.

5.5.3 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.

5.5.4 An Authentication Action for Form-Based Authentication Redirects to a Non-Secure Page

You can specify a redirection action for authentication or authorization success or failure. However, if you specify this action relative to the Web server, it may fail when the WebGate being used is installed on an Oracle HTTP Server version 2.

For example, you may be redirected using an HTTP redirect instead of HTTPS when you do the following:

1. In the Policy Manager, create a policy to protect a resource.

2. Protect the resource using a form-based authentication scheme.

3. Specify a redirection action for authorization success.
4. In a browser, enter the URL for the protected resource.
5. Provide login credentials when presented with the login form.

To work around this problem, add the following lines in the Virtual host definition section of the ssl.conf file:

```
LoadModule certheaders_module modules/mod_certheaders.so
AddCertHeader HTTPS
AddCertHeader SSL_CLIENT_CERT
SimulateHttps On
```

5.5.5 Access Server 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.

5.5.6 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.

5.5.7 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.wwsso_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 mesg = 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.
<img
src="http://myhost.us.mydomain.com:7777/access/oblix/lang/en-us/style2/oblixlo
go.gif">
<%
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%>

<img src="<%=url_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>
```

5.5.8 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`

5.5.9 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*g* (10.1.4), 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.

5.5.10 Policy Manager API Support Used Incorrectly in Help and Access System Console

The "AM Service State" in previous Access System Console pages was renamed to "Access Management Service". In 10.1.4 Access Server and AccessGate configuration pages, "Access Management Service" appears correctly.

However, the following product areas incorrectly refer to "Policy Manager API Support" rather than "Access Management Service":

- Access Server Cluster configuration page
- Help for Access Server and AccessGate configuration pages

> **See Also:** Section 5.9.31, "Policy Manager API Support Should Read Access Management Service"

5.5.11 webgate.so Not Found Error After Form-based Login

After successful authentication, if you click the Back button in the browser window, you might get an error for access/oblix/apps/webgate/bin/webgate.so.

When form-based authentication is used, Oracle Access Manager creates a form login cookie that holds information about the requested resource. On successful authentication, the state of the cookie changes. When the user clicks the Back button, the login form appears. When reposted, the form login cookie no longer holds redirection details.

The ObSSOCookie is also sent with the form login cookie.The ObSSOCookie is correctly checked. As the form login cookie state changes, the form-based authentication does not occur and the form action is considered as a request for the resource.

5.6 Identity System Workarounds and Issues

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

5.6.1 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 left-most 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.

5.6.2 Auditing for the Identity System Ceases to Work

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

To avoid this issue, restart the Identity Server.

5.6.3 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" />
```

5.6.4 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.

5.6.5 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.

5.6.6 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.

5.6.7 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.

5.6.8 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 browser, the application name "User Manager" on the User Manager Configuration tab might not be translated.

There is no solution for this problem at this time.

5.6.9 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.

5.6.10 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.

5.6.11 Incorrect Path Provided to the UDDI Files

The *Oracle Access Manager Developer Guide* states that sample UDDI registration programs in .NET and Java format are provided in the following locations:

webpass_install_dir\oblix\WebServices\UDDI\dotnet

and

webpass_install_dir\oblix\WebServices\UDDI\java

However, the actual paths are as follows

webpass_install_dir\oblix\WebServices\samples\UDDI\dotnet

and

webpass_install_dir\oblix\WebServices\samples\UDDI\java

5.6.12 Incorrect Path Setting for Running Sample WSDL Code

The *Oracle Access Manager Developer Guide* section on "Invoking a WSDL-Based Web Service Using Java" states that when compiling and running the sample code, you set the path to your Access Manager SDK installation as follows:

```
set PATH=f:\temp\AccessServerSDK\oblix\lib;F:\j2sdk1.4.2_05\bin;path
```

However, you actually set the path to your Access Manager SDK installation as follows:

```
set PATH=AccessServerSDK_install_dir\oblix\lib;F:\j2sdk1.4.2_05\bin;%PATH%
```

Where *AccessServer_install_dir* is the directory where the Access Server was installed.

5.6.13 User Creation Might Fail When You Have Multi-byte Characters in the Password

Problem:

When you create a user with multi-byte characters in the password using a non-English keyboard, user creation might fail. You might see the error: Directory Server Password Policy violated.

Cause

This problem will occur when you have the 7-bit check plug-in enabled for the "uid" and "userpassword" attributes. In this case, modifying a password for an existing user forces the "7-bit check" for the newly entered password. If the newly entered password contains multi-byte characters, then it does not qualify as "7-bit clean". The product is designed to function in this way.

For example, when creating a workflow, the values are stored under the "obcontainerId=workflowInstances,o=Oblix,o=company,c=us" node. The password value is stored as "obattrvals: <value>" and is encoded as "7-bit clean". When the Approver approves the workflow, the password value is decrypted and stored under the "userpassword" attribute.

Solution

The following solution is now documented in the *Oracle Access Manager Identity and Common Administration Guide*, "Troubleshooting" section in Appendix F.

If you want "7-bit check" to be enabled for workflow steps you need to write your own plug-ins.

> **Note:** Your directory server might not support the 7-bit check. In any case, you must be able to create a user with multi-byte characters.

If you want a user password (or any other attribute) to contain multi-byte characters, you must disable the "7-bit check" for the specific attribute. The following procedure refers to steps for a Sun (formerly iPlanet) directory server. Your details and steps might be different. See your vendor documentation for more information.

To disable the 7-bit check

1. Log in to your directory server as an administrator.
2. Click your directory server instance under "Server Group".
3. Go to the configuration tab for the directory server instance.

4. Expand the "Plug-ins" node to display the list of plug-ins that are applied to your directory server instances.
5. Click "7-bit check" to display the list of attributes that are acted upon by this plug-in.
6. Remove the required attributes or disable the plug-in entirely, as follows:
   - Remove "obattrvals".
   - Disable the plug-in by clicking the Advanced button and set "nsslapd-pluginenabled" to "off".

5.6.14 Modifying Challenge and Response Phrases for Lost Password Management from a Panel

A user can modify the challenge and response used for lost password management by modifying phrases in his own user profile. However, changing the Challenge/Response using a Selection box in a Panel results in an unexpected error:

```
Challenge phrase is blank. Provide values for all challenge phrases
```

> **Note:** Ignore this topic if you have a fresh installation of Oracle Access Manager 10g (10.1.4.3), which includes the latest changes to basic.xsl and misc.js. You have no previous customizations to update and need not perform any of the steps here.

To help resolve this issue, changes have been made to basic.xsl (a typical wrapper stylesheet) and misc.js (a system-level file used by many stylesheets). These updated files reside in LPMChallengeResponsePatch.zip and are available with bundle patch 10.1.4.2.0-BP04. These files and the changes they contain need to be introduced in your deployment.

LPMChallengeResponsePatch.zip is included in each platform zip file for the 10.1.4.2.0-BP04 bundle patch. You can obtain the patch and the LPMChallengeResponsePatch.zip as described in following steps. However, you will not actually use any other bundle patch components.

To download Patch ID 7113405 in the 10.1.4.2.0-BP04 bundle patch

1. On the machine that will host the bundle patch files, create a temporary directory to contain the platform-specific bundles that you will download. For example:

   Unix : /home/*10142BP04*/tmp
   Windows: C:*10142BP04*\tmp

2. Go to My Oracle Support and login as usual:

   `https://support.oracle.com`

3. Follow instructions in Section 5.1.2.2, "Retrieving the Latest Bundle Patch" to retrieve Patch ID 7113405.
4. In the temporary directory where you stored the downloaded zip file, unzip to extract component-specific bundles and LPMChallengeResponsePatch.zip.
5. Refer to usage instructions in the topic "Details for Bug 6804657" in the companion *Oracle Access Manager Bundle Patch Notes.*

6. For more information, see "Error When Resetting the LPM Challenge or Response Phrase" in the troubleshooting chapter of the *Oracle Access Manager Identity and Common Administration Guide*.

5.6.15 Workflow Buttons Might Appear Disabled with Firefox 3.5 on Linux

In the Workflow Definition applet, Defined Steps panel, “Defined steps” buttons such as New, Modify, Delete Step, and Insert Step, can appear disabled when using Firefox 3.5.x under Linux with newer JRE versions. However these buttons are functionally working.

5.7 Third-Party Integration Issues

This section describes issues and workarounds for third-party integrations. It includes the following topics:

5.7.1 Users Receive Errors When Accessing WebLogic Resources

Users can receive errors when using the WebLogic Application Server version 9.2 with the Oracle Access Manager 10.1.4 SSPI Connector.

Specifically, users can receive a "not authorized" error when accessing pages that they should be able to according to the policies configured in Oracle Access Manager.

When you deploy an application on WebLogic 9.2, be sure that you deploy it with the appropriate deployment descriptors for Web applications. The deployment descriptors for Web applications are web.xml and weblogic.xml. Also be sure to deploy the application with deployment descriptors for EJB applications. The files ejb-jar.xml and weblogic-ejb-jar.xml are the deployment descriptors for EJB applications.

5.7.2 The Deploy Link on the WebLogic Console Does Not Respond to Users Without a Role

After configuring the WebLogic Server SSPI Connector, if a non-administrative user selects the Deploy link, the WebLogic Server Console may not respond. That is, the Deploy link no longer responds to users who are logged in without a role.

The problem manifests differently in different environments:

- When the connector is deployed against a WebLogic Server instance running on RedHat Enterprise Linux AS4.0 or Solaris 10, if no application was previously deployed, the link does respond to users without a role.

- When the connector is configured against a WebLogic Server instance running on Solaris 8, the link fails to respond whether or not an application had been previously deployed.

The error also differs slightly depending on your version or WebLogic Server. On WebLogic Server 8.1, the following WebLogic Console error message is shown, "User does not have access to this page." No WebLogic Console error message is displayed on WebLogic Server 9.2. Instead, the user receives the message, "The page cannot be displayed."

There is no workaround at this time.

5.7.3 No Error Is Displayed When You Create a WebLogic Group that Already Exists

When using WebLogic Console for WebLogic Server 9.2 on Red Hat Enterprise Linux AS 4.0 & Solaris 10, if you create a group that already exists, the WebLogic Server Console does not display an error message. The group creation page appears without an error message. However, an exception stack trace is generated.

There is no known workaround at this time

5.7.4 Double-Byte Language Packs Do Not Work with the WebLogic SSPI Connector

When you install the WebLogic SSPI connector, you are prompted to choose a language. If you select Japanese, Simplified Chinese, or Traditional Chinese, the installation appears to complete successfully. However, the files are not successfully extracted and no directory for the selected language is created in *install_dir*/connector/oblix/lang.

If you try to extract the language pack for a previously installed connector, an error message similar to the following is displayed, "Please specify existing Access installation directory for installing Oracle Access Manager 10.1.4.0.1 Access System Japanese Language Pack. Please specify a directory name or press Enter."

If you then try to specify the installation directory of the SSPI connector, you receive the following message, "This directory does not exist. Please enter a valid Oracle Access Manager installation location."

Without the language pack properly installed and the appropriate properties files extracted, the `configureWebgate`, `configureAccessGate`, and `PolicyDeployer` tools display characters incorrectly.

In this release, affected Japanese, Simplified Chinese, and Traditional Chinese characters are replaced with English characters.

5.7.5 Integrating with Oracle Application Server Single Sign-On

In the *Oracle Access Manager Integration Guide*, the chapter on "Configuring the Access System for OracleAS Single Sign-On 10.1.2.0.2" is incomplete. The following is correct information on this topic.

1. Follow the steps in the rest of the chapter on "Configuring the Access System for OracleAS Single Sign-On 10.1.2.0.2".
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.wwsso_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 following 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 mesg = 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.
<img
src="http://myhost.us.mydomain.com:7777/access/oblix/lang/en-us/style2/oblixlo
go.gif">
<%
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%>

<img src="<%=url_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>
```

5.7.6 File Needed for Registrytester Not Bundled with IBM WebSphere Application Server 6.1

Before you enable the NetPointWASRegistry, you need to run the registryTester program to ensure that the NetPointWASRegistry is registered and can successfully connect to the Identity System. A file required to run the registrytester was available in the *WAS_install_dir*. Today, however, the file is not bundled with the Oracle Access Manager Connector for WebSphere. As a result, you cannot run the registrytester with the Oracle Access Manager Connector for WebSphere 6.1.

Workaround: Copy the com.ibm.ws.runtime_6.1.0.jar file which is available in *WAS_INSTALL_DIR*\plugins, then set the classpath in the RegistryTester.bat/RegistryTester.sh file accordingly. For example:

```
set CLASSPATH=.:${CLASSPATH}:${INSTALL_DIR}/oblix/lib/NetPointWASRegistry.jar
:${INSTALL_DIR}/oblix/lib/jobaccess.jar
:${WAS_INSTALL_DIR}/lib/wssec.jar
:${WAS_INSTALL_DIR/lib/sas.jar
:${WAS_INSTALL_DIR}/lib/j2ee.jar
:${WAS_INSTALL_DIR}/java/jre/lib/security.jar
:${WAS_INSTALL_DIR}/java/jre/lib/xml.jar
%WAS_INSTALL_DIR%\plugins\com.ibm.ws.runtime_6.1.0.jar
```

5.8 Directory Issues

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

- Section 5.8.1, "Error "There Is No Profile Configured for this Kind of Object""
- Section 5.8.2, "Issues With the Display of Messages in Some Languages"
- Section 5.8.3, "Support for eDirectory 8.7.3"

> **See Also:** Section 5.9.29, "Updating Novell eDirectory Schema Details"

5.8.1 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.

5.8.2 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.

5.8.3 Support for eDirectory 8.7.3

When conducting searches using Novel 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)(objectcl
ass=genSiteOrgPerson)(objectclass=genSiteGroup)))(objectclass=*))
```

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

To workaround this issue, apply the eDirectory patch 8.7.3.7. See the following URL for details:

http://www.novell.com

5.9 Documentation Issues

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

5.9.1 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.

5.9.2 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/`"

Beginning with 10*g* (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.

5.9.3 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.

5.9.4 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.

5.9.5 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.

5.9.6 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.

5.9.7 Incorrect obver Attribute Value Stated in Documentation

Procedures in the *Oracle Access Manager Upgrade Guide* to verify Identity and Access System schema upgrades, instruct you to view the configuration node in the configuration directory server and confirm that the value of the `obver` attribute is `10.1.4.0.1`. However, the actual attribute value is `10.1.4.0`.

In the next release of the *Oracle Access Manager Upgrade Guide*, the following procedures will be corrected to reflect the actual attribute value of `10.1.4.0`:

To verify the schema and data upgrade

1. Check to ensure that the schema contains 10*g* (10.1.4) attributes `obPolicyEnabled` and objectclass `oblixLPMPolicy`.
2. View the configuration node in the configuration directory server and confirm that the value of the `obver` attribute is `10.1.4.0`.

To verify the Access System schema and data upgrade

1. Using your directory administration console, confirm that the schema contains all the object classes and attributes as defined in the *Oracle Access Manager Schema Description*.

2. Using your directory administration console, verify that all the indexes have been added.
3. **Different Directory Server Instances**: Perform the steps in the following list to ensure that the schema was also updated:
   - View the configuration node in the configuration directory server and confirm that the value of the `obver` attribute is `10.1.4.0`.
   - Check to ensure that the schema contains 10*g* (10.1.4) attributes `obPolicyEnabled` and objectclass `oblixLPMPolicy`.

5.9.8 Changes in System Behavior for obVer Missing in Manuals

Changes in system behavior for the obVer attribute were not noted in the *Oracle Access Manager Schema Description* and the *Oracle Access Manager Upgrade Guide*.

The following information will be added to the next release of the *Oracle Access Manager Schema Description*:

- oblixConfig class: This value is used by the Identity and Access Servers with the Lost Password Management feature.
- OblixOrgPerson class: A value of 10.1.4.0 or greater in oblixOrgPerson indicates that the challenge phrase and response attributes are encoded with a delimiter of @*n*# between multiple values. In the encoding, *n* is the number of the challenge or response.

  For more information about multiple challenge and response attributes, see the *Oracle Access Manager Identity and Common Administration Guide*. For implications when upgrading from an earlier release to Oracle Access Manager 10*g* (10.1.4), see the *Oracle Access Manager Upgrade Guide*.

The following information will be added to the next release of the *Oracle Access Manager Upgrade Guide* in the chapter that provides a summary of system behaviors.

The obVer attribute identifies the current Oracle Access Manager release and is one of several attributes in the class description of many Oracle Access Manager schema objects. For example, the obVer attribute is part of oblixPanel, oblixConfig, oblixLocation, oblixMetaAttribute, oblixEnum, and OblixOrgPerson to name only a few.

Until release 10*g* (10.1.4), the obVer attribute was purely informational. However starting with release 10*g* (10.1.4), the obVer attribute is used by the Identity and Access Servers to support encoding of multiple challenge phrase and response attributes for lost password management. In this case, Oracle Access Manager 10*g* (10.1.4) reads the obVer attribute in:

- oblixConfig class: The structural class defines the container node for the Oracle Access Manager configuration data.

  In oblixConfig, the obVer attribute always exists and indicates the current product release.
- OblixOrgPerson class: The auxiliary class used for associating Oracle Access Manager person information with the class configured as the structural person object class. The next release of the *Oracle Access Manager Schema Description* will include the following details:

  In OblixOrgPerson obVer may or may not exist. When obVer does not exist in a user entry, the value is assumed to be less than 10.1.4.0.

Oracle Access Manager 10*g* (10.1.4) uses the obVer value in the OblixOrgPerson class in the following ways:

- An obVer vale of less than 10.1.4.0 indicates that there is a single value for the challenge phrase and the response with no encoding. For example:

```
ChallengeAttribute: what is your name?
ResponseAttribute: xxxxxxxx (encrypted form of Ramakrishna)
```

- An obVer value of 10.1.4.0 or greater indicates that the challenge phrase and response attributes are encoded (with @*n*# as a delimiter between multiple values, where *n* is the number of the challenge or response). For example:

```
ChallengeAttribute: what is your name?@1#what is your school name?@2#
ResponseAttribute: xxxxxxxx (where xxxxxxxx is the encrypted form of the
                            name@1#SGschool@2#)

ChallengeAttribute: what is your name?@1#
ResponseAttribute: xxxxxxxx (where xxxxxxxx is the encrypted form of the
                            name@1#
```

When you upgrade from an earlier release to Oracle Access Manager 10*g* (10.1.4), configuration data stored in the `oblix` tree is migrated automatically and the value of the obVer attribute is changed to 10.1.4.0. However, user data is not migrated until the first login following the upgrade. This means that the obVer attribute value remains less than 10.1.4.0 in user data (in the OblixOrgPerson class). In this case, during the first login the user data is migrated and:

- The existing challenge phrase and response values are encoded (@1# is appended to the existing values automatically).
- The value of the obVer attribute in user data (the OblixOrgPerson class) is set to the value of the obVer attribute in migrated configuration data in the root node of the `oblix` tree (oblixConfig).

Caution: The first time a user logs in after the upgrade, that user entry is migrated immediately. Any existing challenge and response values for that user are encoded (@1# is appended to the end) and the obVer attribute value is changed to 10.1.4.0. However if you restore your earlier release, the rollback process does not revert these changes. If you rollback to your previous release, the obVer value in the user entry in the OblixOrgPerson class remains 10.1.4.0 and challenge and response values remain encoded format.

To temporarily stop the immediate user data migration (also known as on-the-fly migration) and avoid possible rollback issues, see Section 5.4.3, "Rollback Issues After Upgrading to Oracle Access Manager 10g (10.1.4)".

5.9.9 Items Needed for WebLogic 9.2 Application Server Certification

With the latest support for the Security Provider for WebLogic SSPI on WebLogic 9.2, information in the *Oracle Access Manager Integration Guide* must include new details. Specifically in the discussion on preparing the WebLogic environment in the chapter on "Integrating the Security Provider for WebLogic SSPI."

The note beneath step 1 and additions to subsections b and c beneath step 12 of the following procedure will appear in the *Oracle Access Manager Integration Guide* to with Release 10.1.4 Patch Set 1 (10.1.4.2.0).

To prepare the environment

1. Copy the mbean jar file from one of the following locations:

   From

   install_dir/oblix/lib/mbeantypes

   to

   WebLogic_Home/server/lib/mbeantypes

   Note: If you are using WebLogic 9.2, copy `wl8NetPointSecurityProviders_Upgraded.jar`. If you are using WebLogic 8.1, copy `wl8NetPointSecurityProviders.jar`. If you are using WebLogic 7.0 SP2 and later, copy `wl7NetPointSecurityProviders.jar`.

2. Copy the following files from your *Security_Provider_install_dir* to your WebLogic domain folder:

   NetPointProvidersConfig.properties

   NetPointResourceMap.conf: only for the WebLogic Server domain

3. Ensure that the following Admin credentials are set in clear text in the NetPointProvidersConfig.properties file:

   OB_AdminUserName=admin

   OB_AdminUserCreds=password

   If the NetPointProvidersConfig.properties file has a clear text password, the SSPI reads in the password, encrypts it, and rewrites the properties file with the encrypted password.

   Note: NetPointProvidersConfig.properties file formatting is lost when Oracle Access Manager rewrites the file with the encrypted password. You may want to save a copy of the NetPointProvidersConfig.properties file. Also, ensure that all parameters are correctly filled as mentioned in the *Oracle Access Manager Integration Guide*.

   You complete the next step if the SSPI talks to a WebPass that is protected by a WebGate. Otherwise, skip to step 5.

4. **WebPass Protected by WebGate:** Complete the following activities when the Oracle Access Manager SSPI talks to a WebPass protected by a WebGate:

   a. In the NetPointProvidersConfig.properties file, ensure that OB_WebPassIsProtected is set to true. The OB_CookiePath and OB_CookieDomain parameters are configured correctly.

   b. From the Access System Console, click Access System Configuration, click AccessGate Configuration in the left navigation pane, click the link for the WebGate that protects the WebPass, and in the IPValidation field select the Off option.

In Oracle Access Manager 10*g* (10.1.4), the WebGateStatic.lst file no longer exists. The options in this file have moved to the Access System Console. See *Oracle Access Manager Access Administration Guide* for details.

Note: If you want to set IPValidation to True, configure the IPValidationExceptions parameter to contain the IP address.

---

c. Restart the Web server.

Note: Ensure that the security level in this authentication scheme is the same level or a lower level than the one specified in the WebLogic authentication scheme

---

Next, you need to determine if the machine hosting WebPass is running SSL. If it is, complete step 5. Otherwise, skip to step 6.

5. **WebPass Host SSL-Enabled:** Determine if the machine hosting WebPass is running SSL, and if so, complete the following steps:

   a. Open the NetPointProvidersConfig.properties file and set OB_ WebPassSSLEnabled = True.

   b. Obtain the CA certificate from the certificate authority to which the Web server hosting the WebPass or WebGate running in SSL mode has registered, and place it in ca.cer file.

   c. Use the keytool in JAVA_HOME\bin or JAVA_HOME\jre\bin to add the following ca certificate to cacerts keystore present in:

   ```
   JAVA_HOME\jre\lib\security folder for weblogic jdk
   keytool -import -alias ca -file ca.cer -keystore JAVA_HOME\jre\lib\
   security\cacerts
   ```

6. Add the following environment variables in the WebLogic Server startup script before the command that starts the server:

   Add the following to the CLASSPATH:

   ```
   /install_dir/oblix/lib/wlNetPoint.jar
   /install_dir/oblix/lib/bcprov-jdk14-125.jar
   /install_dir/oblix/lib/xerces.jar
   /install_dir/oblix/lib/jobaccess.jar
   ```

7. Add the following environment variables in the WebLogic Server startup script before the command that starts the server:

   HP-UX: Add the following to SHLIB_PATH:

   ```
   install_dir/oblix/lib
   ```

   Portal Domain: The CLASSPATH and PATH variables should be added just after the SAVE_JAVA_OPTIONS environment variable in the startWebLogic.cmd script (On Unix, it is the startWebLogic.sh script).

8. On Linux, set the LD_ASSUME_KERNEL environment variable to 2.4.19, as follows:

   ```
   LD_ASSUME_KERNEL=2.4.19
   export LD_ASSUME_KERNEL
   ```

9. Remove the boot.properties file from the WebLogic domain directory.

   This will cause the startWebLogic script described in the next step to prompt for username and password.

10. In the WebLogic domain directory, edit the appropriate startup script:

    Unix: The script is startWeblogic.sh

    Ensure the following paths are set in the script:

    ```
    /install_dir/oblix/lib/wlNetPoint.jar
    /install_dir/oblix/lib/bcprov-jdk14-125.jar
    /install_dir/oblix/lib/xerces.jar
    /install_dir/oblix/lib/jobaccess.jar
    ```

11. In the WebLogic domain directory, start the WebLogic Server using the appropriate startup script:

    Unix: This command is startWeblogic.sh

    Using the WebLogic 8.1 Domain Configuration Wizard, you can create instances of a new WebLogic 8.1 domain, for example, mydomain, and a new WebLogic 8.1 server, for example, myserver. You can also create instances of a new WebLogic 8.1.3 Portal domain, for example, portalDomain, and a new WebLogic 8.1.3 portal, for example, portalServer.

12. Set up a Realm that uses Oracle Access Manager security providers, as follows:

    a. Open a new console window and set the Weblogic environment by executing setEnv.cmd.

       Unix: Source the setEnv.sh script present in the server domain directory.

       Portal Domain: Use the setDomainEnv.cmd script (on Unix it is the setDomainEnv.sh script).

    b. Run the following script and ensure that it has the correct username, password, and URL values:

       Unix: *install_dir*/setupNetPointRealm.sh

       Note: To use policies based on roles for Web and EJB applications in WebLogic SSPI, run the `setupNetPointRealm` tool with the `sspi_role` parameter.

       For example:

       ```
       install_dir\setupNetPointRealm.cmd sspi_role
       ```

       Portal Domain: Run the script with parameter "portal".

       WebLogic Server 7.0: The script does not work and NetPointRealm must be set manually.

       WebLogic Application Server 9.2 on Unix: Set the `domName` variable in the `install_dir/setupNetPointRealm.properties` file. Then run the `install_dir/setupNetPointRealm_wl92.sh` script.

    c. Log in to the WebLogic Admin Console, navigate to Domain, Security, Realms and:

       * Verify that NetPointRealm is set as the default.

* Verify that the security providers are set properly in NetPointRealm.

Use the following steps for WebLogic Server 9.2:

* Click Lock and Edit in the WebLogic Admin Console.
* Navigate to NetpointRealm, Providers, Certification Path, WebLogicCertPathProvider. Select the Current Builder option to use the WebLogicCertPathProvider as the current builder. Click Activate Changes to activate all changes.
* Set NetPointRealm as the default realm.

  In the left pane, select your domain to open the Settings page for your domain. Click the Security tab; click General; select NetPointRealm as the default security realm; click Save; click Activate Changes to activate all changes.

d. **Script Fails:** If the script fails, you must manually add the Oracle Access Manager security realm (NetPointRealm):

* Go to Domain, Security, Realms and select "Configure a new Realm".
* For the option "Check Roles and Policies for", ensure that "All Web Applications and EJBs" is selected.
* Navigate to Providers, Authentication, and configure a new Authenticator and Identity Asserter.
* **Identity Asserter:** Select the Token Type ObSSOCookie and in the Details tab, uncheck "Base64Decoding Required".
* **Portal Domain:** Set the control flag of Authenticator to OPTIONAL and also configure a Default Authenticator.
* Navigate to Providers, Authorization and configure a new Authorizer(for the portal domain, only configure a Default Authorizer).

  For role based policies, you also need to configure a Default Authorization Provider. Navigate to Providers, Authorization and configure a Default Authorization Provider.
* For role based policies, navigate to Providers, Adjudication and configure a new Adjudication Provider.
* Navigate to Providers, Role Mapping and configure a new Role mapper (for the portal domain, only configure a Default Role mapper).
* Navigate to Providers, Credential Mapping and configure a new Default Credential mapper.
* Navigate to Domain, Security and select this realm as the default realm.

13. **Portal Server Domain:** Complete the following steps to configure a WebLogic Portal domain:

a. Restart the server using the same WebLogic credentials that were used earlier.

b. In the WebLogic Server Console, navigate to Domain, Security, Realms, NetPointRealm, Providers, Authentication, and:

* Remove the Default Authenticator.
* Change the control flag for Authenticator to REQUIRED.

c. Using the Group Manager, create a group in Oracle Access Manager that maps to the Admin role in the BEA WebLogic Server and contains all the administrators for the BEA Portal.

For example:

BEA_Administrators

d. Create a user (portaladmin) and add it to the BEA_Administrators group; later you login as this user (portaladmin) when restarting the server.

e. In the WebLogic Server Console Admin Console, navigate to Security, Realms, NetPointRealm and:

* Click Groups to display all Oracle Access Manager groups.
* Search for the BEA Admin group that was created in this step. You can use a wild card in the search.
* Copy the group name.

f. Click Global Roles, Admin role, Conditions tab and:

* Add a Role Condition where the caller is a member of the group.
* Paste in the group name you copied.

g. Change the role condition from "and" to "or", then click Apply.

h. Repeat this procedure for the PortalSystemAdministrator role.

Note: Other BEA roles can be mapped to Oracle Access Manager groups/users. When you restart the WebLogic Server, it is important that you are logged in as a user in the Oracle Access Manager group associated with the BEA Admin role.

---

14. Restart the WebLogic Server.

The next time you log in to the WebLogic console, provide Master Oracle Access Manager Administrator credentials. You will be authenticated using NetPointRealm.

15. If you are using identity assertion as the authentication mechanism that protects Web applications:

a. Install a WebGate on the proxy Web server. See the *Oracle Access Manager Integration Guide* for an illustration of this type of installation.

b. Configure the Oracle Access Manager policies that protect the Web applications to use HTTP as the resource type instead of wl_url.

Note: There is one exception to the resource type configuration. The WebLogic administration console always uses form login. The /console policy must use the resource type wl_url.

---

16. If anything other than an Oracle Access Manager form-based authentication scheme protects the policies configured with the HTTP resource type, configure a challenge redirect parameter to redirect the user to another Web server that has WebGate installed.

Note: If you do not complete this step, the user will have to refresh the browser to access the desired page because the ObSSOCookie set by the WebGate in the HTTP request has not yet been sent to the WebLogic server.

17. Continue with following procedure in the *Oracle Access Manager Integration Guide* as needed.

5.9.10 Corrected Default Path Names in *Oracle Access Manager Installation Guide*

The *Oracle Access Manager Installation Guide* states incorrect default path names for components, as shown in Table 5–3.

Table 5–3 Erroneous Default Installation Path Names

Component	Installation Directory
Identity Server	Windows: \Program Files\OracleAccessManager\identity Unix: /opt/oracleaccessmanager/identity In This Guide: *IdentityServer_install_dir*\identity
WebPass	Windows: \Program Files\OracleAccessManager\WebComponent\identity Unix: /opt/oracleaccessmanager/WebComponent/identity In This Guide: *WebPass_install_dir*\identity
Access Server	Windows: \Program Files\OracleAccessManager\access Unix: /opt/oracleaccessmanager/access In This Guide: *AccessServer_install_dir*\access
Policy Manager	Windows: \Program Files\OracleAccessManager\WebComponent\access Unix: /opt/oracleaccessmanager/WebComponent/access In This Guide: *PolicyManager_install_dir*\access
WebGate	Windows: \Program Files\OracleAccessManager\WebComponent\access Unix: /opt/oracleaccessmanager/WebComponent/access In This Guide: *WebGate_install_dir*\access

In the next release of this manual, with Release 10.1.4 Patch Set 1 (10.1.4.2.0), the path names will be corrected as shown in Table 5–4.

Table 5–4 Correct Default Installation Path Names

Component	Installation Directory
Identity Server	Windows: \Program Files\NetPoint\identity Unix: /opt/NetPoint/identity In This Guide: *IdentityServer_install_dir*\identity
WebPass	Windows: \Program Files\NetPoint\WebComponent\identity Unix: /opt/NetPoint/WebComponent/identity In This Guide: *WebPass_install_dir*\identity

Table 5–4 (Cont.) Correct Default Installation Path Names

Component	Installation Directory
Access Server	Windows: \Program Files\NetPoint\access Unix: /opt/NetPoint/access In This Guide: *AccessServer_install_dir*\access
Policy Manager	Windows: \Program Files\NetPoint\WebComponent\access Unix: /opt/NetPoint/WebComponent/access In This Guide: *PolicyManager_install_dir*\access
WebGate	The default WebGate installation directory path name varies depending upon your platform and Web server type. For example: Win32 ISAPI WebGate: \Program Files\NetPoint\Webgate Win32 OHS2 WebGate: \Program Files\NetPoint\WebComponent Win32 NSAPI WebGate: \Program Files\NetPoint\WebGat Linux Apache2 WebGate: /opt/netpoint/webgate Linux OHS2 WebGates: /opt/netpoint/webgate In This Guide: *WebGate_install_dir*\access

5.9.11 OIS and Access Server Service Start is Automatic by Default

The *Oracle Access Manager Installation Guide* chapter "Installing the Identity Server" incorrectly states that the Identity Server and Access Server services are set to start manually by default in step 6 of the procedure that describes finishing the Identity Server installation:

- **Windows**: Open the Services Window then locate and start the Identity Server service.

  By default, the Identity Server (also known as the Oracle Identity Server (OIS)) starts manually, but you can set its startup type to Automatic. See the Microsoft Windows Help for details.

- **Unix**: Execute the following command:

  */IdentityServer_install_dir/*identity/oblix/apps/common/bin/start_ois_server

To correct this statement, the *Oracle Access Manager Installation Guide* that is available with Release 10.1.4 Patch Set 1 (10.1.4.2.0) will include the following updated information in step 6:

- **Windows**: Open the Services Window and confirm that the Identity Server service is started.

  By default, the Identity Server (also known as the Oracle Identity Server (OIS)) starts automatically. To change the default to manual start, see the Microsoft Windows Help for details.

- **Unix**: Execute the following command to start the Identity Server service:

  */IdentityServer_install_dir/*identity/oblix/apps/common/bin/start_ois_server

Also, the procedure on finishing the Access Server installation in the chapter on "Installing the Access Server", includes similar information which is now corrected.

5.9.12 Certificate Utility Flags Incorrect for Oracle Virtual Directory SSL Listener

The *Oracle Access Manager Installation Guide* chapter on "Setting Up Oracle Access Manager with Oracle Virtual Directory", contains a procedure to configure the Oracle Virtual Directory SSL Listener. Step 8 of this procedure contains an incorrect command-line syntax.

The incorrect syntax line will be changed to the following and a new note will be added for clarification:

8. Import the root CA to the Identity Server using the following command:

```
certutil -d IdentityServer_install_dir\identity\oblix\config -A -n ldap -a
-t "C,," -i root_ca_file
```

Note: In the certutil command, the -t (trusted arguments) flag should be followed by the trust attributes that will be assigned to the certificate, enclosed in double-quotes.

5.9.13 Tuning Oracle Internet Directory for Oracle Access Manager

The Oracle Access Manager Installation Guide describes how to use the `ldapmodify` command to tune Oracle Internet Directory. However, if you tune Oracle Internet Directory 10.1.2 or earlier using the `ldapmodify` command as described in the chapter on installing the Identity Server, you will receive the following error message:

```
"Attribute orclinmemfiltprocess is not supported in schema."
```

The `orclinmemfiltprocess` attribute is not supported in the schema until Oracle Internet Directory 10.1.4. As a result, you cannot use the `ldapmodify` command to tune Oracle Internet Directory.

The next release of the Oracle Access Manager Installation Guide will make this clear.

5.9.14 Obtaining/Updating Sample Adapter and Mapping Templates for Oracle Virtual Directory

The chapter on integrating Oracle Virtual Directory with Oracle Access Manager in the Oracle Access Manager Installation Guide states that Oracle-provided sample adapter and mapping template files are available in the DNConversionToolkit and must be obtained and stored in the Oracle Virtual Directory Manager using the steps provided.

However, Oracle Virtual Directory 10.1.4 and later provides sample Oracle Access Manager templates and mappings out-of-the-box in Oracle Virtual Directory Manager. These sample adapter templates are available automatically in the Adapter Template list of Oracle Virtual Directory Manager.

The next release of the Oracle Access Manager Installation Guide will include the following information:

Oracle Virtual Directory 10.1.4 and later provides sample Oracle Access Manager templates and mappings out-of-the-box in Oracle Virtual Directory Manager. Depending on the Oracle Virtual Directory release you are using, proceed as follows:

- Skip the topic "Obtaining/Updating Sample Adapter and Mapping Templates" if you are using Oracle Virtual Directory 10.1.4 and later, and instead proceed to the next applicable topic for your environment. Later in this chapter you will see how to use the adapter and mapping templates.

- Continue with the information and steps in this topic if you are using a release of Oracle Virtual Directory before 10.1.4, or if you choose to use the sample adapter and mapping templates in the Oracle Access Manager distribution.

5.9.15 Typographical Error in the Solution for "The Login Form Appears Repeatedly"

The troubleshooting chapter of the *Oracle Access Manager Access Administration Guide* contains a typographical error in the solution for The Login Form Appears Repeatedly." This will be corrected in the next release of the *Oracle Access Manager Access Administration Guide*.

Incorrect: To verify whether a user has a valid session, you can type the following in the browser's location:

```
javascript:altert(document.cookie)
```

Correct: To verify whether a user has a valid session, you can type the following in the browser's location:

```
javascript:alert(document.cookie)
```

5.9.16 Added Required Database User Privileges to Upload Schema in Oracle Access Manager Configuration Manager

The *Oracle Access Manager Configuration Manager Installation and Administration Guide* did not mention the privileges required by the database user to upload the Oracle Access Manager Configuration Manager schema after adding repository details.

The 10.1.4.2.0 version of the manual, available with Release 10.1.4 Patch Set 1 (10.1.4.2.0), will include the following information to correct this issue.

Upload Schema Button appears only when there is no Oracle Access Manager Configuration Manager schema present in the Oracle Database repository. For a successful schema upload, the database user needs the following system privileges: Create Table, Create Sequence, Create Trigger, and Create Procedure.

5.9.17 Added Audit File Renaming Steps to *Oracle Access Manager Upgrade Guide*

A new discussion is added to the release 10.1.4.2.0 *Oracle Access Manager Upgrade Guide* that is available with Release 10.1.4 Patch Set 1 (10.1.4.2.0). The following new procedure describes how to rename audit file path names after upgrading multiple Identity Servers.

After upgrading Identity Servers from releases earlier than 7.0, you must perform this task to correct the path name of audit files. If you have upgraded from release 7.x, you can skip this activity.

When upgrading the master Identity Server and the schema and data from any release earlier than 700, the audit file name is changed by prefixing the path to the master Identity Server.

If your deployment includes multiple Identity Servers, the audit file name for each will be prefixed by the same Identity Server installation directory path as the Identity Server from which the data upgrade is performed. The result is that your original configuration is lost during the Identity Server upgrade. For example, suppose you have two Identity Server instances with audit files stored as follows:

D:\611\ois_one\identity\oblix\engine\auditfile_1.lst
D:\611\ois_two\identity\oblix\engine\auditfile_2.lst

After the upgrade, however, both audit files will be stored in the directory path of the master Identity Server (611\ois_one). For example:

D:\611\ois_one\identity\oblix\engine\auditfile_1.lst
D:\611\ois_one\identity\oblix\engine\auditfile_2.lst

To recover your audit files after upgrading multiple Identity Servers, you must perform the following task to change audit file paths to reflect the appropriate path to specific Identity Server instances.

To recover your original audit files after upgrading Identity Servers

1. Go to the Identity System Console and log in as usual.

   `http://hostname:port/identity/oblix`

   where *hostname* refers to machine that hosts the Web server; *port* refers to the HTTP port number of the WebPass Web server instance; and /identity/oblix connects to the Identity System Console.

2. From the Identity System Console, click System Configuration, then click Identity Servers.
3. Select the name of an upgraded Identity Server to display the information for this instance.
4. Check the Audit File Name field, to see if the path name is correct.

   If the path name is correct, click Cancel and then repeat steps 3 and 4 to check the audit file path name for another instance. If the path name is not correct, proceed to step 5.

5. Click the Modify button at the bottom of the page.
6. On the Modify page, change the path name in the Audit File Name field to the correct path for this instance and then click Save. For example:

   From: D:\611\ois_one\identity\oblix\engine\auditfile_2.lst
   To: D:\611\ois_**two**\identity\oblix\engine\auditfile_2.lst

7. Restart the Identity Server whose details you just updated.
8. Repeat all steps in this procedure for each upgraded Identity Server instance.

5.9.18 Corrected Path Details for Oracle Virtual Directory Schema Files

The discussion on extending directory schemas in the *Oracle Access Manager Installation Guide* states the location of vde_user_schema_add.ldif and aduserschema.ldif files as being in the *IdentityServer_install_dir*\identity\oblix\tools\DNConversionToolkit\tools\DataAnyWhere\OblixUserSchema. The DNConversionToolkit was provided with release 10*g* (10.1.4.0.1). However, the following location is also available and was documented in a later version of the *Oracle Access Manager Installation Guide*:

IdentityServer_install_dir\identity\oblix\tools\DataAnyWhere\OblixUserSchema\vde_user_schema_add.ldif

IdentityServer_install_dir\identity\oblix\tools\DataAnyWhere\OblixUserSchema\aduserschema.ldif

5.9.19 Corrected LDAPModify Syntax for Oracle Virtual Directory

The discussion on extending directory schemas in the *Oracle Access Manager Installation Guide* omits the VDE_user_schema_add.ldif file name in the ldapmodify command syntax. The manual currently states the following syntax:

```
ldapmodify -h host -p port -D bind-dn -w password -a -f
```

This syntax will be corrected as follows in the 10.1.4.2.0 version of the *Oracle Access Manager Installation Guide* that is available with Release 10.1.4 Patch Set 1 (10.1.4.2.0):

```
ldapmodify -h host -p port -D bind-dn -w password -a -f VDE_user_schema_add.ldif
```

5.9.20 Added SSL Requirements When Upgrading Schema and Data with Master Access Manager

The *Oracle Access Manager Upgrade Guide* does not mention that SSL-enabled communication with the directory server might be a requirement for the master Access Manager component that is installed and used for the schema and data upgrade.

The following information is added to the chapter on preparing for schema and data upgrades in the release 10.1.4.2.0 *Oracle Access Manager Upgrade Guide* that is available with Release 10.1.4 Patch Set 1 (10.1.4.2.0):

When your original Access Manager component is configured to use SSL-enabled communication with the directory server, the master that you add must also be configured to use SSL-enabled communication with the directory.

The following information is added to help you when troubleshooting data access issues in the release 10.1.4.2.0 *Oracle Access Manager Upgrade Guide* that is available with Release 10.1.4 Patch Set 1 (10.1.4.2.0):

If you receive a "Cannot find <person> Object Class" error after upgrading the schema and data, the problem may be that the master Access Manger component used to upgrade the schema and data did not use the same transport security as the original component. When your original Access Manager component is configured to use SSL-enabled communication with the directory server, the master that you add must also be configured to use SSL-enabled communication with the directory.

5.9.21 Corrected Path Names for Schema Index Files in Oracle Access Manager Upgrade Guide

The *Oracle Access Manager Upgrade Guide* states an incorrect path when uploading the schema index files for Sun (formerly iPlanet) directory, Novell eDirectory (NDS), and Oracle Internet Directory after data migration. This will be corrected in the section on "Uploading Directory Server Index Files" in the 10.1.4.2.0 *Oracle Access Manager Upgrade Guide* that is available with Release 10.1.4 Patch Set 1 (10.1.4.2.0).

The corrected paths are:

IdentityServer_install_dir/identity/oblix/data.ldap/common

PolicyManager_install_dir/access/oblix/data.ldap/common

5.9.22 Corrected Environment URL in Oracle Access Manager Configuration Manager Installation and Administration Guide

The description of the Environment URL in the chapter on migrating configuration data changes in the *Oracle Access Manager Configuration Manager Installation and Administration Guide* is incorrect and has been changed as described here.

Original Description

The Add Environment page provides fields where you can enter other information, including Environment Name, optional Description, Host Name and Port, Configuration DN, User DN, Password, and the URL for the LDAP Directory environment. When defining an environment name and description, you can use any combination of uppercase and lowercase alphanumeric characters, as well as spaces and punctuation.

The Add Environment page provides fields where you can enter other information, including Environment Name, optional Description, Host Name and Port, Configuration DN, User DN, Password, and the (optional) URL for the relevant Oracle Access Manager deployment for this environment. When defining an environment name and description, you can use any combination of uppercase and lowercase alphanumeric characters, as well as spaces and punctuation.

Environment URL: The URL to the LDAP directory. For example:

```
http://141.144.74.35:3333/access/oblix/
```

Corrected Description

The Add Environment page provides fields where you can enter other information, including Environment Name, optional Description, Host Name and Port, Configuration DN, User DN, Password, and the (optional) URL for the relevant Oracle Access Manager deployment for this environment. When defining an environment name and description, you can use any combination of uppercase and lowercase alphanumeric characters, as well as spaces and punctuation.

Environment URL: The URL to the relevant Oracle Access Manager deployment for this environment. For example:

```
http://141.144.74.35:3333/access/oblix/
```

5.9.23 Missing Challenge Parameter `"realmunique:yes"`

After integrating Oracle Access Manager and Oracle SSO, and implementing global logout from Oracle SSO, logout does not remove the ObSSOCookie cookie. When the user clicks logout and tries to go back to the protected URL, the user is the still logged in.

When using "`Basic over LDAP`" authentication, the browser will return the cached credential following a timeout. A new challenge parameter `"realmunique:yes"` was introduced in Oracle COREid 7.0.4.2 to correct the problem. However, the information is not described in recent manuals.

A future release of the *Oracle Access Manager Integration Guide* will include new information.

See Also: Knowledge Base Note 443493.1

To access Knowledge Base Note 443493.1

1. Go to My Oracle Support and login as usual:

   `https://support.oracle.com`

2. Click **Knowledge** (upper-left corner).
3. In the Search Knowledge Base field (upper right corner), enter **`443493.1`**.
4. Click the title on the results page: `After Integration of Oracle Access Manager and Oracle SSO Logout Does Not Rem...`
5. Review the article.

5.9.24 Misleading Title for Enabling Client Cert on IIS in *Oracle Access Manager Installation Guide*

The *Oracle Access Manager Installation Guide* provides a misleading title in the chapter on installing WebGate, Chapter 9.

Incorrect Title

Enabling SSL on the IIS Web Server

The correct title will appear in the 10.1.4.3.0 version of the book. The information has moved into a separate chapter on Installing Web Components with the IIS Web Server, Chapter 19.

Correct Title

Enabling Client Cert on the IIS Web Server

5.9.25 oblixCoreidServerDown has the Same Description as oblixCoreidServerFailure

The Oracle Access Manager Identity and Common Administration Guide chapter on SNMP Monitoring, provides the same description for both OBLIXCOREIDSERVERDOWN and OBLIXCOREIDSERVERFAILURE.

Incorrect

oblixCoreidServerDown

A trap generated when the SNMP Agent detects that the Identity Server is (potentially) Down. This trap contains the server ID, host name, and port.

oblixCoreidServerFailure

This trap is generated when the SNMP Agent detects that the Identity Server has failed. This trap contains the server ID, host name, and port.

Correct

oblixCoreidServerDown

A trap generated when the SNMP Agent detects that the Identity Server is (potentially) Down. This trap contains the server ID, host name, and port.

oblixCoreidServerFailure

This trap is generated when the SNMP Agent detects that the Identity Server has failed. This trap contains the server ID, host name, and port.

5.9.26 Syntax Correction in Oracle Access Manager Customization Guide

A syntax error has been corrected in Step 2 of the procedure "To import an Identity System XML file to work with its respective XSL stylesheet" in the *Oracle Access Manager Customization Guide*. `$format=xmlnoxsy` now reads `&format=xmlnoxsl`.

This information appears in the latest version of the book.

5.9.27 Clarification of `unique_value_attrs` in ldapreferentialintegrityparams.xml

The following additional information should appear in the description of `unique_value_attrs` in the table that describes ldapreferentialintegrityparams.xml in the*Oracle Access Manager Customization Guide*.

Note: Oracle Access Manager enforces uniqueness only for the attribute of Login semantic type. As a result, it appears that the product enforces uniqueness for uid or samaccountname attribute.

The 'unique_value_attrs' parameter is only used in the context of Oracle Access Manager performing LDAP referential integrity. In certain referential integrity cases, Oracle Access Manager might need to delete and add the same entry with the updated DN. In such cases, unique_value_attrs identifies whether delete needs to happen first.

This information appears in the latest version of the book.

5.9.28 Clarification on Reconfiguring COREid Server and WebPass

The following additional step should be included in the Oracle Access Manager Deployment Guide chapter on "Migration". This new Step 4 in the procedure "To reconfigure COREid Server and WebPass" will ensure that the COREid Server will restart after deleting entries in the directory.

4. Locate and run setup_ois from the following file system directory path:

IdentityServer_install_dir/identity/oblix/tools/
start_setup_ois
./start_setup_ois -i *IdentityServer_install_dir*/identity/

This information appears in the latest version of the book.

5.9.29 Updating Novell eDirectory Schema Details

Information on updating the Novell eDirectory schema should appear in the *Oracle COREid Access and Identity Installation Guide*. The following information appears in the latest version of the book.

Details for Novell eDirectory

By default, the Oracle schema for Novell eDirectory does not support creating the oblix node (o=oblix,<config-dn>) under a domain node (for example, dc=us,dc=oracle,dc=com) during browser-based Identity System setup. This means that you cannot use a domain node as the configuration base during the browser-based Identity System setup. A workaround is provided in the Troubleshooting chapter, under "Novell eDirectory Issues" on page E-7.

When setting the searchbase to "dc=nc" during browser-based Identity System setup with Novell eDirectory, you must define the CONTAINMENT object under which the "o=Oblix" (oblixconfig) objectclass can exist. Within the schema for eDirectory, the oblixconfig objectclass can include "domain" as a possible CONTAINMENT object.

Workaround

The following workaround will appear in the "Troubleshooting" chapter of the 10.1.4.3 *Oracle Access Manager Installation Guide*:

During Identity Server installation, you are asked if you want to extend the directory server schema. At this point, you can browse the Identity Server's installation directory and locate the NDS_oblix_schema_add.ldif file. From a file editor, you can edit the CONTAINMENT for this objectclass to include "domain" using the following steps:

1. When asked if you want to extend the directory schema during Identity Server installation, locate the NDS_oblix_schema_add.ldif file, as follows:

   ```
   IdentityServer_install_dir\identity\oblix\data.ldap\common\'NDS_oblix_schema_
   add.ldif
   ```

2. Open the NDS_oblix_schema_add.ldif in an editor and locate the 'oblixconfig' objectclass, which also defines the CONTAINMENT for this objectclass. For example:

   ```
   dn: cn=schema
   changetype: modify
   add: objectclasses
   objectclasses: ( 1.3.6.1.4.1.3831.0.1.2 NAME 'oblixconfig' SUP top
   STRUCTURAL MUST ( obpersonoc $
   obsearchbase $ organizationName )  MAY ( obsearchbasestr $ obgroupoc $
   ……..$ obver $
   obduplicateAction )  X-NDS_NAMING ( 'O' )  X-NDS_CONTAINMENT (
   'organization' 'organizationalUnit'  'country' 'locality' ) )
   ```

3. Modify this entry to specify the 'domain' as one of the CONTAINMENT classes for the 'oblixconfig' objectclass. For example:

   ```
   dn: cn=schema
   changetype: modify
   add: objectclasses
   objectclasses: ( 1.3.6.1.4.1.3831.0.1.2 NAME 'oblixconfig' SUP top
   STRUCTURAL MUST ( obpersonoc $
   obsearchbase $ organizationName )  MAY ( obsearchbasestr $ obgroupoc $
   ……..$ obver $
   obduplicateAction )  X-NDS_NAMING ( 'O' )  X-NDS_CONTAINMENT ( 'domain'
   'organization' 'organizationalUnit'  'country' 'locality' ) )
   ```

4. Save the modified schema file and continue with installation and browser-based setup.

5.9.30 Clarification in WebLogic Chapter of *Oracle Access Manager Integration Guide*

The following note is missing from the "Integration Architecture" section of the WebLogic chapter in the *Oracle Access Manager Integration Guide*.

Form-based authentication gives SSO between Oracle Access Manager and WebLogic applications. However, Basic Over LDAP authentication does not provide SSO.

The previous paragraph appears in the latest version of the book.

5.9.31 Policy Manager API Support Should Read Access Management Service

Oracle Access Manager manuals provide a table of product name changes in the "What's New" chapter. However, the chapter incorrectly states that the Access System Service (named AM Service State in Access System Console pages) was renamed to "Policy Manager API Support Mode". "Access System Service" was actually renamed as "Access Management Service". The latest Oracle Access Manager manuals contain the following correction in the "What's New" chapter.

Table 5–5 Product Name Changes

Item	Was	Is
Access System Service	AM Service State Policy Manager API Support Mode	Access Management Service

The correction has also been made in the *Oracle Access Manager Access Administration Guide*, "Configuring WebGates and Access Servers" chapter as follows:

- Access Server Configuration Parameters table
- AccessGate Configuration Parameters table

See Also: Section 5.5.10, "Policy Manager API Support Used Incorrectly in Help and Access System Console"

5.9.32 Invalid URL Patterns in Policy

A URL pattern is an Access System-supported mechanism for identifying different resources of a certain type that are protected by a single policy. Patterns with the following attributes are invalid:

- A '[' without a closing ']'
- A '{' without a closing '}'
- Unescaped '{' inside {}
- Unescaped '/' inside [ ]

The following information has been added to the topic on "Invalid URL Patterns" in the chapter on protecting resources with policy domains in the *Oracle Access Manager Access Administration Guide*.

The following URL pattern is not recognized when it is included within {}:

```
{pattern_1, pattern_2, /.../cleanup.asp}
```

The URL pattern will only be recognized if it is used without {}:

```
/.../cleanup.asp
```

URL patterns within {} are designed for simple expressions such as the following:

```
a{ab,bc}b matches aabb and abcb
a{x*y,y?x}b matches axyb, axabayb, ayaxb, etc
```

URL patterns within [] should not contain complex sub-expressions such as those starting with "/". For example:

```
[/.../cleanup.asp   OR    /c*/webservice/webservice.asp]
```

Instead, consider creating three separate policies:

```
??/admin/*
/c*/webservice/webservice.asp
/.../cleanup.asp
```

5.9.33 Update for Apache v2 for WebGate on UNIX with the mpm_worker_module

The troubleshooting chapter of the *Oracle Access Manager Installation Guide* provides instructions to compile Apache v2.0 for WebGate on UNIX with the mpm_worker_ module. This should be done only for the Apache 2.0 WebGate. During the update, you will modify the thread.c file from the Apache source for the UNIX environment.

The following note should be added.

Note: Apache v2.1 on Linux does not support the ThreadStackSize directive.

See Also: "Apache v2 on UNIX with the mpm_worker_module for WebGate" in the troubleshooting chapter of the latest *Oracle Access Manager Installation Guide*

6

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"
- Section 6.3, "Documentation Errata"

In addition to these release notes, please also see Patch Notes 10*g* (10.1.4.3.0) and Note 743141.1 Oracle Identity Management 10*g* (10.1.4.3) Patch Set Notes Addendum for information about Oracle Application Server Single Sign-On.

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 10*g* 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 6.2.2, "Deleting and Recreating a User Causes an Error When Accessing an External Application"
- Section 6.2.3, "You Must Change the Value for the ORCLDASURLBASE Attribute in Oracle Internet Directory After Enabling SSL"
- Section 6.2.4, "Clarification Needed for Implementing the IPASAuthInterface.java Package"
- Section 6.2.5, "Multiple Single Sign-On Servers Cannot Share a Global User Inactivity Timeout"
- Section 6.2.6, "A "Host Unavailable" Entry Appears on Non-English Monitoring Pages"
- Section 6.2.7, "Dynamic Global Logout Directives Must Pass the String "Oracle SSO""

- Section 6.2.8, "Multilevel Authentication Configuration May or May Not Require a Port Number"

6.2.1 Oracle Directory Manager Is no Longer Supported

Appendix B, "Obtaining the Single Sign-On Schema Password" in the *Oracle Application Server Single Sign-On Administrator's Guide* states that you can find the password using either the command-line tool `ldapsearch` or Oracle Directory Manager. However, Oracle Directory Manager is no longer supported.

Use the command-line tool `ldapsearch` to find the single sign-on schema password.

6.2.2 Deleting and Recreating a User Causes an Error When Accessing an External Application

If an administrator drops, then re-creates a user's entry in the Oracle Portal, the user can receive an error when accessing an external application. Dropping and re-creating the user causes the ORASSO.WWSEC_PERSON$ table to have a different value for the user's GUID than the GUID that is returned by an OracleAS Single Sign-On login to Oracle Internet Directory.

The error is as follows:

```
There is a conflict with your assigned user name. There is a user entry with this
name, but with a different globally unique identifier,
which must be resolved before you can log on with this name. Please inform your
administrator. (WWC-41742).
```

The following is a workaround for this issue:

1. Log in to SQLPLUS as an ORASSO user.

   See Appendix B, "Obtaining the Single Sign-On Schema Password" in the *Oracle Application Server Single Sign-On Administrator's Guide* for information on using the command-line tool `ldapsearch`. Note that Oracle Directory Manager is no longer supported.

2. Enter the following:

   ```
   update orasso.wwsec_person$ set guid = null ;
   commit;
   ```

To test this workaround, log in as the user who was deleted and re-created.

6.2.3 You Must Change the Value for the ORCLDASURLBASE Attribute in Oracle Internet Directory After Enabling SSL

After you enable single sign-on for HTTPS, you also must change the value for the ORCLDASURLBASE attribute in Oracle Internet Directory. You can find this attribute in the following location:

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

Set the value for this attribute to the following:

`https://`*`servername`*`:/`*`SSO_HTTPS_PORT`*

If the default 443 port is used, set the value as follows:

`https://`*`servername`*

6.2.4 Clarification Needed for Implementing the IPASAuthInterface.java Package

In the section on "Integrating with Third-Party Access Management Systems Using Integration APIs" in the *Oracle Application Server Single Sign-On Administrator's Guide*, there is information on the `IPASAuthInterface.java` package. This section needed to mention that the p2store token needs to be sent back from the single sign-on server. The redirection URL must be appended to the URL in the `getUserCredentialPage()` function.

The following note will be added to the next version of this manual:

"To implement this interface, you must modify your code to redirect the user to the OracleAS Single Sign-On login URL. This is the URL that the third-party application is protecting. You must also append the URL in `getUserCredentialPage()` to include the site2pstoretoken."

6.2.5 Multiple Single Sign-On Servers Cannot Share a Global User Inactivity Timeout

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

However, this timeout value can cause problems in a cookie domain that contains other applications that are protected by a different single sign-on server. For example, if the timeout is configured for the cookie domain ".com", a user who accesses myapplication1.mycompany1.com and myapplication2.mycompany2.com may be unable to access either application.

6.2.6 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.

6.2.7 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.

6.2.8 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
```

6.3 Documentation Errata

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

- Section 6.3.1, "Incomplete Information in "Developing Applications for Single Sign-On" Chapter of Oracle Identity Management Application Developer's Guide"

6.3.1 Incomplete Information in "Developing Applications for Single Sign-On" Chapter of Oracle Identity Management Application Developer's Guide

Table 9-1, User Attributes Passed to Partner Applications, mentions that the `Remote-User` header is recommended for pre-9.0.4 applications only. It does not explain why. The reason is that the `Remote-User` header is unique only within a domain. In release 9.0.4 and later, OracleAS Single Sign-On supports multiple domains, so you should use a header that is unique across domains, such as `Osso-User-Guid`.

7

Oracle Identity Federation

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

In addition to these release notes, please also see Patch Notes 10*g* (10.1.4.3.0) and Note 743141.1 Oracle Identity Management 10*g* (10.1.4.3) Patch Set Notes Addendum for information about Oracle Identity Federation.

7.1 Installation and Upgrade Issues

This section describes installation and upgrade issues. It includes the following topic:

7.1.1 Oracle Identity Federation Configuration Assistant Fails in SSL Mode

Problem

During Oracle Identity Federation installation, the configuration assistant fails if you specify an SSL-enabled port to use in upgrading the LDAP schema for the Oracle Identity Federation data store.

The problem is seen under these conditions:

1. You are performing the installation on one of these platforms:
   - AIX 5L-based Systems (64-Bit),
   - IBM zSeries-based Linux, or
   - Linux on Power
2. On the "Select Configuration Options" page of the installer, you check the "Federation Data in LDAP Server" box, to specify that the LDAP schema should be upgraded during installation.
3. On the "Specify Federation Data Store" page of the installer, you check the box labeled "Select if this Port is an SSL Port", directing the installer to use the LDAP SSL port for the connection when doing the LDAP schema upgrade.

The Oracle Identity Federation Configuration Assistant fails at this stage of the installation. The failure is manifested in the `install*Actions*.log` as well as the `$ORACLE_HOME/fed/log/federation-install.log`.

The `install*Actions*.log` shows an error like this:

```
Opening connection to the LDAP server
Error while interacting with the LDAP server: javax.naming.NamingException:
Cannot connect to any LDAP Servers
The Federation Configuration Assistant failed
A log of the Federation Configuration Assistant is available at
/project/as10/qa
/fed_ssl/fed/log/federation-install.log
java -jar install.jar <params> where params are:
    -oh ORACLE_HOME              The ORACLE_HOME directory. Required
    -transient type              The type of transient data store (rdbms or
                                 memory). Required
    -dbtnsname tnsname           The RDBMS TNS name. Required if rdbms used for
                                 transient data store
    -dbusername username         The RDBMS username. Required if rdbms used for
                                 transient data store
    -dbpwd password              The RDBMS password. Required if rdbms used for
                                 transient data store
    -uselocalconfig <true|false> Indicates whether or not RDMBS config data will
                                 be overwritten
```

The `$ORACLE_HOME/fed/log/federation-install.log` shows an error related to an unsupported cipher suite:

```
07/10/25 14:09:47: ERROR
oracle.security.fed.model.util.ldap.LDAPConnectionManager    -
javax.naming.CommunicationException: strsun03.us.oracle.com:636
[Root exception is java.lang.IllegalArgumentException: Unsupported ciphersuite
TLS_RSA_WITH_AES_128_CBC_SHA]
```

The problem is caused when the Oracle Identity Federation Configuration Assistant attempts to use some ciphersuites that are not supported by the JDK shipped on these platforms.

Solution

Oracle has issued a one-off patch set to fix the problem. With this fix, the installer first executes a query to get the supported ciphersuites, so that the Oracle Identity Federation Configuration Assistant attempts to use only that set of ciphersuites.

To apply this OracleAS 10.1.4.0.1 Oracle Identity Federation installation one-off patchset, download the zip file for the patch set. Follow the instructions in the README file included in the patchset.

The fix can be applied in either a corrective or a preventive mode:

- If you encounter the Oracle Identity Federation Configuration Assistant failure described above, apply the one-off patchset and re-try the configuration assistant.
- To avoid the Oracle Identity Federation Configuration Assistant failure altogether, apply the patchset immediately after the `root.sh` popup window appears during installation.

After applying the patchset, run `root.sh` as usual, then continue on with your installation. Your configuration assistants will then be executed, and the Oracle Identity Federation Configuration Assistant should run without any errors.

7.2 General Issues and Workarounds

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

7.2.1 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.

7.2.2 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.

7.2.3 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
```

7.2.4 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).

7.2.5 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.

7.2.6 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.

7.2.7 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 singing 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.

7.2.8 Encrypting Network Connections

By default, JDBC does not encrypt network connections between Oracle Identity Federation and the Oracle9*i* 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.

7.2.9 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.

7.2.10 Forced Reauthentication Not Supported with OracleAS Single Sign-On

Oracle Identity Federation does not support the ability to force re-challenging the user for credentials when integrated with OracleAS Single Sign-On. This means that Oracle Identity Federation cannot support use cases where reauthentication must be forced.

For example, if an SP sends an AuthnRequest with `ForceAuthn="true"` to an Oracle Identity Federation IdP, and Oracle Identity Federation is integrated with OracleAS Single Sign-On, the `ForceAuthn` flag is ignored.

7.3 Configuration Issues and Workarounds

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

7.3.1 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 10*g* 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.

7.3.2 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.

7.3.3 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.

7.3.4 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.

7.3.5 Some Peer Providers Are Not Displayed in Administration Console

n 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.

7.3.6 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.

7.3.7 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.

7.3.8 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.

7.4 Documentation Errata

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

7.4.1 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.

7.4.2 Enhanced Description of Provider Configuration

In the *Oracle Identity Federation Administrator's Guide*, the sections titled "Identity Provider - Global Settings" and "Service Provider - Global Settings" provide instructions on how to configure an identity provider (IdP) or a service provider (SP) for the IdP Discovery Profile using common domain cookies.

In the 10.1.4.0.1 release document (Part Number B25355-01), the section numbers are:

- 5.3.3.1 "Identity Provider - Global Settings" and
- 5.3.3.4 "Service Provider - Global Settings"

These instructions are insufficient for provider configuration; replace them with the following text:

5.3.3.1 Identity Provider - Global Settings

...

Common Domain URL

When the providers in a Circle of Trust have agreed upon a common domain for the IdP introduction cookie, each participating Identity Provider must have a cookie writing service hosted in the common domain.

An Oracle Identity Federation IdP runs the service on the /fed/idp/intro path; the HTTP server must be configured to listen for a host:port in the common domain. Once this is done, the common domain URL can be constructed.

For example, if the agreed-upon common domain is .cdc.example.org, and the Oracle Identity Federation IdP is hosted on idp.mycorp.com, then the IdP's HTTP server could be configured to listen on mycorpidp.cdc.example.org:7778. Then the Common Domain URL for the IdP's cookie-writing service would be:

```
http://mycorpidp.cdc.example.org:7778/fed/idp/intro
```

Set this value only if you checked Common Domain Enabled.

5.3.3.4 Service Provider - Global Settings

...

Common Domain Enabled

When an identity federation network contains multiple identity providers, a service provider needs to have a way to determine the identity provider(s) in use by a principal. This can be achieved by having all the IdPs and SPs in the federation network agree on a cookie domain, and sending to the user's browser a cookie written in this domain; the cookie lists all the IdPs where the user has logged in. Such a domain is known as a common domain, and the cookie identifying the IdPs is called a common domain cookie or IdP introduction cookie.

Check Common Domain Enabled to specify that this SP should read the introduction cookie to discover the IdP to use for authentication.

Common Domain URL

When the providers in a Circle of Trust have agreed upon a common domain for the IdP introduction cookie, each participating Service Provider must have a cookie reading service hosted in the common domain.

An Oracle Identity Federation SP runs the service on the /fed/sp/introsso path; the HTTP server must be configured to listen for a host:port in the common domain. Once this is done, the Common Domain URL can be constructed.

For example, if the agreed-upon common domain is .cdc.example.org, and the Oracle Identity Federation SP is hosted on sp.mycorp.com, then the SP's HTTP server could be configured to listen on mycorpsp.cdc.example.org:7778. Then the Common Domain URL for the SP's cookie-reading service would be:

```
http://mycorpsp.cdc.example.org:7778/fed/sp/introsso
```

Set this value only if you checked Common Domain Enabled.

7.4.3 Update to Section 4.2.6.2 Creating a Custom Authentication Engine

In Section 4.2.6.2, Creating a Custom Authentication Engine, of the *Oracle Identity Federation Administrator's Guide* for 10*g* (10.1.4.0.1), part number B25355-02, after following the instructions you are unable to complete login. The browser gives you the error message:

```
"500 Internal Server Error"
```

The Oracle Identity Federation `federation.log` file and the `federation-error.log` file show the following error:

```
ERROR - LOCAL LOGIN: ERROR: No JSESSIONID cookie in a POST request.
```

The steps in Section 4.2.6.2 of the guide are incomplete. To resolve the issue:

1. Apply the steps listed in Knowledge Base Note 345167.1.

> **Note:** The patch mentioned in the note is already included in version 10*g* (10.1.4), so if you are running version 10*g* (10.1.4) or higher, you only need to set the -Doracle.useSessionIDFromCookie=true flag as shown in the document.

2. Restart the Oracle Identity Federation instance

To access Knowledge Base Note 345167.1

1. Go to My Oracle Support and login as usual:

   https://support.oracle.com

2. Click **Knowledge** (upper-left corner).
3. In the Search Knowledge Base field (upper right corner), enter **`345167.1`**. Click the magnifying glass icon.
4. Click the title on the results page that states "HTTP Session Info lost between two web applications when common "cookie-path" (e.g. "/") for JSESSIONID [ID 345167.1]" to read the note.

8

Oracle Security Developer Tools

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

8.1 General Issues and Workarounds

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

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.

9 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"

In addition to these release notes, please also see Patch Notes 10*g* (10.1.4.3.0) and Note 743141.1 Oracle Identity Management 10*g* (10.1.4.3) Patch Set Notes Addendum for information about Oracle Internet Directory.

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"
- Section 9.1.4, "Data Manipulation at Database Level is Not Supported"

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 10*g* (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 10*g* (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`.

9.1.4 Data Manipulation at Database Level is Not Supported

Use only the documented tools, such as command-line tools, Oracle Directory Manager, and Oracle Enterprise Manager 10*g* Application Server Control to modify data in Oracle Internet Directory. Do not attempt to change Oracle Internet Directory data directly in the Oracle Database.

9.2 Configuration Issues and Workarounds

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

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:

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 `creatUser()` 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=user`**`s`**`,cn=hr,c=us`.

9.3.10 Bad ldifwrite Parameter in Backup Chapter

On the first page of the chapter entitled "Backup and Restoration of a Directory" in *Oracle Internet Directory Administrator's Guide*, the command line in Step 1 is:

```
ldifwrite connect="connect_string"  basedn="naming_context" file="backup.ldif"
```

It should be:

```
ldifwrite connect="connect_string"  basedn="naming_context" ldiffile="backup.ldif"
```

9.3.11 Error in Sample Code for Java Plug-ins

In the "Java Server Plug-ins" chapter of *Oracle Identity Management Application Developer's Guide*, in "Example 2: External Authentication Plug-in for Active Directory," please change:

```
// Retrieve the Base DN, Attribute and Attribute Value
     String bdn = opObj.getBaseDN().substring(0,
      opObj.getBaseDN().lastIndexOf("cn=users,dc=us,dc=oracle,dc=com")-1)
       +",cn=users,dc=dlin,dc=net";
```

to:

```
// Retrieve the Base DN, Attribute and Attribute Value
     LdapBaseEntry baseEntry = plgObj.getLdapBaseEntry();
```

```
String bdn = baseEntry.getDN().substring(0,
  baseEntry.getDN().lastIndexOf("cn=users,dc=us,dc=oracle,dc=com")-1)
  +",cn=users,dc=dlin,dc=net";
```

9.3.12 Obsolete Step in SSL Configuration Procedure

In the "Secure Sockets Layer (SSL) and the Directory" chapter of *Oracle Internet Directory Administrator's Guide*, in the section "Configure Oracle Internet Directory for SSL," please delete the following content from Step 13:

- On Windows systems, you must perform an extra configuration step. You must change the login account of the Oracle Directory Service from a local system account to the account of the user who owns the wallet. This user must be member of `Administrator Group`. Change the account as follows:

  a. On Windows, choose **Start**, then **Settings**, then **Control Panel**, then **Administrative Tools**, then **Services**.

  b. Click **PROPERTIES/LOGON**.

  c. Change from **Local System Account** to the account you logged in as when you created the Wallet. Stop and restart the service.

9.3.13 Errors in Oracle Directory Manager Help and in Appendix A of the Oracle Internet Directory Administrator's Guide

Some attribute definitions listed in the online help for Oracle Directory Manager and in Appendix A of *Oracle Internet Directory Administrator's Guide* are incorrect. Please refer to *Oracle Identity Management User Reference* and earlier sections of *Oracle Internet Directory Administrator's Guide* for attribute definitions and defaults. The following errors have been reported:

Table 9–2 Errors in Oracle Directory Manager Help and Appendix A

Attribute	Correct Definition	Incorrect Definition in Help and Appendix A
Purge Start (`orclpurgestart`)	The time when the garbage collector starts to run. The format is yyyymmddhhmmss. Default value is 12:00 a.m. of the day Oracle Internet Directory is installed.	Time, in seconds, when the Garbage collector runs for the first time. The format is YYYYMMDDHH24MISS. This attribute is optional. The default value is 0, which means that the garbage collector is enabled immediately.
Password Expiry Time (`pwdMaxAge`)	The maximum time, in seconds, that a password can be valid. Upon reaching this age, the password is considered to have expired. The default is 10368000 seconds (120 days).	The number of seconds that a given password is valid. If this attribute is not present, or if the value is 0, then the password does not expire. By default, user passwords never expire.
Password Expiration Warning (`pwdExpireWarning`)	The maximum number of seconds before a password is due to expire that expiration warning messages will be returned to an authenticating user. The default value is 604800 seconds (seven days).	The number of seconds before password expiration that the directory server sends the user a warning. If password expiration is enabled, then, by default, the directory server sends the user a warning three days before the password expires.

9.3.14 No Maximum Value Documented for pwdGraceLoginLimit

No maximum value is specified for `pwdGraceLoginLimit` in Oracle Internet Directory Administrator's Guide. The maximum value is 250.

9.3.15 Setting orcldataprivacymode to 1 Prevents OC4J_SECURITY from Starting

Chapter 16 of the Oracle Internet Directory Administrator's Guide, "Privacy of Retrieved Sensitive Attribute," states that you should enable privacy mode by changing the value of `orcldataprivacymode` from 0 to 1. Doing so, however, prevents OC4J_SECURITY from starting. You should not change the value to 1 if you are using OC4J_SECURITY or Oracle Application Server Single Sign-On.

9.3.16 External Authentication Scripts Have .pls Extension

The "Debugging the External Authentication Plug-in" section of Chapter 34, "Setting Up the Customized External Authentication Plug-in" in *Oracle Internet Directory Administrator's Guide* refers to the following files under *ORACLE_HOME*`/ldap/admin/`:

```
oidspdsu.sql
oidspdon.sql
oidspdof.sql
oidspdsh.sql
oidspdde.sql
```

These filenames are incorrect. The files are actually named:

```
oidspdsu.pls
oidspdon.pls
oidspdof.pls
oidspdsh.pls
oidspdde.pls
```

9.3.17 Patch Notes 10g (10.1.4.3.0) Contains Incorrect Instruction to Apply a Patch

There is an error in Section 4.4, "Issues Related to Applying this Patch," in the subsection entitled "To upgrade a Single Sign-On or Oracle Delegated Administration Services cluster"

Step 4 says: "Patch the instance installed in step 1". This step is incorrect and should be ignored.

10

Oracle Virtual Directory

This chapter describes issues associated with Oracle Virtual Directory 10.1.4.3.0 and is an ***addition*** to the information contained in the *Oracle Virtual Directory 10.1.4.3.0 Patch Notes*, part number E12282-01. You can access the *Oracle Virtual Directory 10.1.4.3.0 Patch Notes* on the Oracle Technology Network (OTN) Web site at the following URL:

`http://www.oracle.com/technology/documentation/oim1014.html`

This chapter includes the following topics:

10.1 General Issues and Workarounds

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

10.1.1 Creating oraInst.loc File During Installation of Oracle Virtual Directory 10*g* (10.1.4.3.0) on AIX

The readme.txt file included in Oracle Virtual Directory 10*g* (10.1.4.3.0) for AIX contains incorrect steps for creating the oraInst.loc file during installation. The following are the *correct* steps:

1. Check if there are any existing Oracle products installed on the machine. Also, check if the /etc/oraInst.loc file exists. If /etc/oraInst.loc does not exist, perform the following steps:
   a. Log in as root.
   b. Go to the /etc/ directory.
   c. Create a file named oraInst.loc in the /etc/ directory.
   d. Add the following to the /etc/oraInst.loc file you just created:

```
inventory_loc=<path>/oraInventory
inst_group=<group id>
```

   e. Save the /etc/oraInst.loc file.

10.2 Documentation Errata

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

10.2.1 Correction for Access Control Rules Documentation

In the "Access Control Rules" section of the *Oracle Virtual Directory Product Manuals* for Releases 10*g* (10.1.4.x), the documentation for "Entry Permissions," specifically, the descriptions for the BrowseDN and ReturnDN permissions, is misleading.

To clarify, both the BrowseDN and ReturnDN permissions must be set to Grant for browse or retrieve operations on source repository entries to be processed. Contrary to the 10.1.4.x documentation, browse or retrieve operations will not be processed if either the BrowseDN or ReturnDN permissions are set to Deny.

11

Oracle Application Server Certificate Authority

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

- Section 11.1, "Documentation Errata"

In addition to these release notes, please also see Patch Notes 10*g* (10.1.4.3.0) and Note 743141.1 Oracle Identity Management 10*g* (10.1.4.3) Patch Set Notes Addendum for information about Oracle Application Server Certificate Authority.

11.1 Documentation Errata

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

- Section 11.1.1, "Java Classes for Custom Policy Plug-in Must Use JDK 1.4.2"
- Section 11.1.2, "Incorrect Class Name in Custom Policy Example"

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

The *Oracle Application Server Certificate Authority Administrator's Guide*, 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."

11.1.2 Incorrect Class Name in Custom Policy Example

The *Oracle Application Server Certificate Authority Administrator's Guide*, 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;
```

12

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 12.1, "General Issues and Workarounds"
- Section 12.2, "Administration Issues and Workarounds"
- Section 12.3, "Online Help Issues and Workarounds"
- Section 12.4, "Documentation Issues"

In addition to these release notes, please also see Patch Notes 10*g* (10.1.4.3.0) and Note 743141.1 Oracle Identity Management 10*g* (10.1.4.3) Patch Set Notes Addendum for information about Oracle Delegated Administration Services.

12.1 General Issues and Workarounds

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

- Section 12.1.1, "Installation Process Does Not Enable SSL for Oracle Delegated Administration Services"
- Section 12.1.2, "Using Single Wildcard Characters to Search for Entries Fails to Return Results"
- Section 12.1.3, "Oracle Internet Directory Self-Service Console Link Does Not Work in Oracle Identity Manager Grid Control Plug-in"
- Section 12.1.4, "Attributes Set to "Searchable" Always Appear on the Search Result Page"

12.1.1 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*.

12.1.2 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.

12.1.3 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 10*g* 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.

12.1.4 Attributes Set to "Searchable" Always Appear on the Search Result Page

When configuring a user entry, you can define a particular attribute as searchable (or not). When configuring Search Table Columns, you can define whether a selected attribute is displayed in the Search Results. Search results work in combination with two Configure User Entry fields:

- **Searchable** check box for an attribute

  `mail` in this example

- **Selected Attributes** in "Configure Search Table Columns"

  `Selected Attributes:No` in this example

Result: You can search using the Searchable attribute `mail`, and the email address appears as a column in the Search Result despite specifying `Selected Attributes:No` in "Configure Search Table Columns".

You can search using any of the attributes that are configured for searches in the user entry. The value of searchable attributes appears in the Search Results. Otherwise, further filtering is not possible.

12.2 Administration Issues and Workarounds

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

- Section 12.2.1, "Disabling Password Change and Reset Functionality"
- Section 12.2.2, "Resetting Oracle Application Server Single Sign-On Passwords Redirects Users to Oracle Delegated Administration Services Home Page"

12.2.1 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 Forgot 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 Forgot 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.

12.2.2 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=value* 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
```

12.3 Online Help Issues and Workarounds

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

- Section 12.3.1, "No Help Topic When Managing Applications"
- Section 12.3.2, "The ou Attribute is Not Allowed In User Entries"

12.3.1 No Help Topic When Managing Applications

From the Provisioning Console, no help topic appears when you click the Directory tab, Applications sub tab, Manage Settings button, then Help.

The information on the Manage Settings function is currently missing from the manual and cannot be accessed. The book will be updated to include the missing information for the next product release.

Content for Manage Settings

This topic explains how to manage application settings and properties for provisioning-integrated applications. These settings include the Default Provisioning Policy (required or not required) and Event Propagation Interval.

Note: The available provisioning-enabled applications will vary, depending on your environment. In Oracle Application Server 10*g* (10.1.4.0.1), only components that are part of Oracle Collaboration Suite can be provisioned with the Provisioning Console.

To manage application settings and properties

1. Click the **Directory** tab, then click **Applications**.
2. On the Manage Settings: Select Installed Application page, click the option beside the application to manage.
3. Choose **Edit**.
4. In the Manage Settings: Edit Application Properties page:
   - Select the Default Provisioning Policy for your environment
   - Enter the Event Propagation Interval
5. Click **OK**.

12.3.2 The `ou` Attribute is Not Allowed In User Entries

The *Oracle Identity Management Guide to Delegated Administration*, chapter on managing users and groups with the Oracle Internet Directory Self-Service Console discusses the organizational unit (`ou`) attribute in the context of setting up parent DNs in an Identity Management realm. However, the online help does not make clear that this attribute cannot be configured like other attributes in the user entry configuration.

A future release of the manual will include the following description in the chapter on troubleshooting. This will be included in the online help with the next release of the product.

In Oracle Delegated Administration Services (and Oracle Internet Directory Self-Service Console), the predefined list for the organizational unit (`ou`) attribute is reserved for specifying parent DN's.

The `ou` attribute values must be mapped according to the guidelines for configuring the parent DN for entries in an Identity Management realm. For more information, see the procedure on configuring the parent DN for entries in a realm.

The `ou` attribute cannot be configured like other attributes in the user entry configuration. The organizational unit (`ou`) attribute cannot have simple text values. You cannot add the organizational unit (`ou`) attribute as a searchable and self-editable field for creating new users.

12.4 Documentation Issues

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

- Section 12.4.1, "Session Context is Not Clearly Documented"
- Section 12.4.2, "Special Characters for User ID Needs Updating"
- Section 12.4.3, "Clarification: Old_password Not Being Passed to Custom Pre_modify Password Policy Plug-in"

12.4.1 Session Context is Not Clearly Documented

Problem

With Oracle Delegated Administration Services running in two browser windows during the same session, certain combinations of events might produce unexpected results from the user's perspective. For example:

- Attempting to update a group in one browser window and a user in a different window might produce an error
- Attempting to update 2 different users in separate browser windows during the same session will result in one of two things depending on the exact sequence of operations. For example, if User1 is changed in window 1 and User2 is changed in window 2:
  - When `User1` changes are submitted last, the entry for `User2` is replaced with User1 details and User1 changes are lost.
  - If User1 changes are submitted first, and then User2 changes are submitted, User1 changes are lost and User2 is updated as expected.

Cause

Oracle Delegated Administration Services maintains only one context per browser session. There is no way for Oracle Delegated Administration Services to be aware that a single browser session is using multiple windows.

Oracle Delegated Administration Services allows only one selected user per session. Any changes occur to the current user entry in the session. Each browser window caches the values that it has displayed and sends these back as updates. Changing the current entry in one browser window and updating it with values cached in a second browser window, could produce unexpected results.

Action

A future release of the manual will include this information in the chapter on troubleshooting.

Oracle recommends that you use only a single browser window per session.

12.4.2 Special Characters for User ID Needs Updating

The *Oracle Identity Management Guide to Delegated Administration*, chapter on managing users and groups with the Oracle Internet Directory Self-Service Console discusses creating user entries. In this topic, there is a list of the special characters that cannot be used in a user ID when creating a new user. However, this list contains several characters that are considered legal for a user ID.

Incorrect

The User ID field cannot contain spaces or any of the following characters:

( ) * + , ; < > \ ~ & ' % ? / = ^ | ~

Correct

Alpha and numeric characters, and the following special characters are allowed within the User ID field:

/ & % space ? = ^ |

However, the User ID field cannot contain any of the following characters:

" ( ) + , ; < > \ ~

12.4.3 Clarification: Old_password Not Being Passed to Custom Pre_modify Password Policy Plug-in

The following information will appear in the next release of the *Oracle Identity Management Guide to Delegated Administration*. See the chapter on troubleshooting.

Problem

When users enter a value in the old_password field, Oracle Delegated Administration Services is not passing the old password value to the Oracle Internet Directory pre_modify plugin.

Cause

Oracle Delegated Administration Services and Oracle Internet Directory are working as designed. You cannot use a custom password policy pre_mod plugin for something that the standard product does not support.

Oracle Delegated Administration Services uses ldapcompare to check the password and a proxy bind as the user. With a proxy bind, there is no reason to send a user's old password to Oracle Internet Directory. Oracle Internet Directory is providing the old password to the plug-in, but in this case it does not have the password.

In contrast, Oracle Application Server SSO binds as the user and then changes the password. The same pre_modify plugin receives a value using the SSO password.jsp. However, password.jsp only appears if a user's password is about to expire.

See Also: Knowledge Base Note 601469.1.

To locate the Knowledge Base note 601469.1

1. Go to My Oracle Support and login as usual:

   `https://support.oracle.com`

2. Click **Knowledge** (upper-left corner).
3. In the Search Knowledge Base field (upper right corner), enter **`601469.1`**.
4. Click the title on the results page: `OIDDAS Not Passing The Old_password To Custom Pre_modify Password Policy Plugin...`
5. Review the article.

13

Oracle Directory Integration Platform

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

- Section 13.1, "Configuration Issues and Workarounds"
- Section 13.2, "Administration Issues and Workarounds"

In addition to these release notes, please also see Patch Notes 10*g* (10.1.4.3.0) and Note 743141.1 Oracle Identity Management 10*g* (10.1.4.3) Patch Set Notes Addendum for information about Oracle Directory Integration Platform.

13.1 Configuration Issues and Workarounds

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

- Section 13.1.1, "Configuration Requirements for Synchronizations with Domain-Level Mappings"
- Section 13.1.2, "Directory Integration Assistant Throws "LDAP: error code 2 - Decoding Error" When Uploading an Additional Configuration Information File"
- Section 13.1.3, "Reconfiguring the Oracle Password Filter for Microsoft Active Directory Generates Errors"
- Section 13.1.4, "In a High Availability Environment Using Multimaster Replication, Provisioning Events May not Be Propagated or May Be Duplicated"
- Section 13.1.5, "Manual Step Required After Configuring Oracle Directory Integration Platform from Oracle Enterprise Manager"
- Section 13.1.6, "Securing the Windows Registry Before Installing the Oracle Password Filter for Microsoft Active Directory"
- Section 13.1.7, "DIP_GEN_CREATECHG_EXCEPTION Raised When Source Directory Contains More than 10 Attributes to be Synchronized"
- Section 13.1.8, "Deletions Not Synchronized if a Domain Editing Rule Exists"
- Section 13.1.9, "Synchronizing modrdn from Sun Java System Directory Throws a Stack Trace"
- Section 13.1.10, "The SearchDeltaSize Parameter is Ignored During Synchronization"
- Section 13.1.11, "Add Operations Not Synchronized and Synchronization Fails with an "objcls is NULL" Message in the Trace File"

13.1.1 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)
```

13.1.2 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.

13.1.3 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.

13.1.4 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.

13.1.5 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/admint/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.

13.1.6 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.

13.1.7 DIP_GEN_CREATECHG_EXCEPTION Raised When Source Directory Contains More than 10 Attributes to be Synchronized

If the number of attributes to be synchronized in the source directory contains more than 10 attributes, the synchronization fails with the exception DIP_GEN_CREATECHG_EXCEPTION. To resolve this issue, apply Patch 5710021.

13.1.8 Deletions Not Synchronized if a Domain Editing Rule Exists

If a domain editing rule exists, deletions are not synchronized unless all the attributes required in the domain construct rule are specified as required in the mapping file. In

case where the required attributes are specified, the 'dn' value is not constructed because the required attributes are not being retrieved from the source directory. To resolve this issue, apply Patch 6263156.

13.1.9 Synchronizing modrdn from Sun Java System Directory Throws a Stack Trace

If you specify `modrdn` as the change type when synchronizing between Oracle Internet Directory and Sun Java System Directory, an exception is raised in the Sun Java System Directory stack trace file. To resolve this issue, apply Patch 6263156.

13.1.10 The SearchDeltaSize Parameter is Ignored During Synchronization

When synchronizing with Active Directory, eDirectory, or OpenLDAP, the `SearchDeltaSize` parameter is ignored. To resolve this issue, apply Patch 5913124.

13.1.11 Add Operations Not Synchronized and Synchronization Fails with an "objcls is NULL" Message in the Trace File

In some cases, add operations are not synchronized and synchronization fails with an "objcls is NULL" message in the trace file. To resolve this issue, apply Patch 6319399.

13.2 Administration Issues and Workarounds

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

- Section 13.2.1, "Default Mapping Rule Can Be Simplified in Single-Domain Microsoft Active Directory Deployments"
- Section 13.2.2, "Oracle Directory Integration Platform Not Sending Provisioning Events Due to Purged Change Log Entries"
- Section 13.2.3, "Oracle Internet Directory Field Unavailable in Oracle Identity Manager Grid Control Plug-in"
- Section 13.2.4, "Synchronizion from Novell eDirectory or OpenLDAP Fails When the Oracle Internet Directory Container is Within the Default Realm"

13.2.1 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(truncl(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
```

13.2.2 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
```

13.2.3 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.

13.2.4 Synchronizion 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 **reconacls.ldif**.
4. Run the following command to upload the reconacls.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 reconacls.ldif
```

41

Oracle Adaptive Access Manager

This chapter includes detailed Oracle Adaptive Access Manager component upgrade instructions and documentation updates. For information on resolved issues and database changes, refer to the most current Readme available.

14.1 Full Installation Packages

From Oracle Adaptive Access Manager, Release 10.1.4.5.bp3 onwards, a complete deployment package to set up the Oracle Adaptive Access Manager application and the database schema is no longer available as part of the bundle patches.

In order to perform a complete deployment Oracle Adaptive Access Manager at the most current revision, you will need to download the base 10.1.4.5 deployment package from OTN and then apply the latest bundle patch and the database patches.

14.2 Bundle Patch Contents

A bundle patch is an official Oracle patch for Oracle Access Manager components on baseline platforms. Bundle patches are released on a regular basis, *after* one product release and *before* the next.

Starting with Oracle Adaptive Access Manager, Release 10.1.4.5.bp4, each bundle patch includes:

- component patches that incorporate all the changes distributed in any patch release since 10.1.4.5.0
- incremental databases patches that contain changes for each bundle patch release, starting from 10.1.4.5.0 up to the most recent version

14.3 General Upgrade Instructions

General upgrade instructions are provided below.

To upgrade the components that pertain to your 10.1.4.5 installation, you must follow the detailed instructions in Section 14.4, "Component and Database Upgrade Procedures."

Determine Current Patch Level

To determine your current patch level, follow these instructions:

1. Log in to Adaptive Risk Manager.
2. Click HELP.

3. Select ONLINE HELP.
4. Select ABOUT.

The About panel should indicate the version you are running with "Welcome to Oracle Adaptive Access Manager version - 10.1.4.5.xxxxxxx"

Database Upgrade

All the database changes are included as part of the bundle patch. The database patches are incremental.

Each database patch performs an incremental upgrade in which the database is only updated with the data that has changed since the previous release.

It is highly recommended that you take a full backup of the database, and then apply all incremental updates, in sequential order, to upgrade your current database to the most recent version.

Application Upgrade

To upgrade the Oracle Adaptive Access Manager application:

1. Back up the application.
2. Follow the upgrade instructions for the components that pertain to your 10.1.4.5 application installation.

14.4 Component and Database Upgrade Procedures

Procedures to upgrade Oracle Adaptive Access Manager components and the database are provided in this section.

14.4.1 Upgrading Command Line Interface

To upgrade the Command Line Interface:

1. Back up all customized properties, .xml and keystore files.

   Some commonly customized files are: bharosa_server.properties, bharosa_client.properties, bharosa_common.properties, bharosauio_client.properties, sessions.xml, log4j.xml and keystore files.

   The files will be used later in the upgrade process.
2. It is highly recommended for you to take a backup of the entire install directory should you need to use it to revert back the patch.
3. Unzip patch_oaam_cli.zip.
4. Copy the contents of patch_oaam_cli.zip into the current Command Line Interface installation.
5. Restore your customized files to the updated Command Line Interface installation.

14.4.2 Upgrading the Database

Note: Before you start the upgrade process, it is strongly recommended that you perform a full database backup.

Follow the instructions from the most current bundle patch Readmes, which contains complete directions for the application of the database changes.

For example, if you were at 10.1.4.5.bp4 and want to upgrade to 10.1.4.5.bp12, and there were database changes in 10.1.4.5.bp5 and 10.1.4.5.bp8, the 10.1.4.5.bp12 Readme will contain directions about what needs to be applied for the 10.1.4.5.bp5 and 10.1.4.5.bp8 database changes and 10.1.4.5.bp12 software. The 10.1.4.5.bp12 bundle patch will contain separate directories with the individual database patches.

Instructions for updates from 10.1.4.5.bp1 to 10.1.4.5.bp6 are also included in this chapter.

Note that if you want to set up purging routines, you will have to perform additional steps, which are documented in the Readme.

Note: The database must be upgraded before you upgrade the application.

14.4.3 Upgrading the Location Loader

To upgrade the Location Loader:

1. Back up all customized properties, .xml and keystore files.

   Some commonly customized files are: bharosa_server.properties, bharosa_client.properties, bharosa_common.properties, bharosauio_client.properties, sessions.xml, log4j.xml, and keystore files.

   The files will be used later in the upgrade process.

2. It is highly recommended for you to take a backup of the entire install directory should you need to use it to revert back the patch.
3. Unzip patch_oaam_location_etl.zip.
4. Copy the contents of patch_oaam_location_etl.zip into the current Location Loader installation.
5. Restore your customized files to the updated application.
6. Verify that all the files have been copied into the directories

14.4.4 Applying the Patch for Native Integration

To apply the patch for native integration (soap):

1. Back up all customized properties, .xml and keystore files.

   Some commonly customized files are: bharosa_server.properties, bharosa_client.properties, bharosa_common.properties, bharosauio_client.properties, sessions.xml, log4j.xml and keystore files.

2. It is highly recommended for you to take a backup of the entire install directory should you need to use it to revert back the patch.

Note: Many of the steps below are for replacing the files in the web application directory.

3. Unzip the patch_oaam_native_soap.zip file, which is located in the oaam_native directory, into the same folder.

4. Copy all the files from conf and its subfolders to your web application's WEB-INF/classes directory.
5. Copy all the jar files from the lib directory to your web application's WEB-INF/lib directory.
6. Copy all the files from bharosa_web and its subfolder to your web application directory.
7. Copy the jars from the thirdparty directory to the web application's WEB-INF/lib directory. Make sure all the jars are copied into the lib directory.

To apply the patch for native integration inproc, perform the same steps as above, but take the patch from the oaam_native_inproc.zip file.

14.4.5 Upgrading the Oracle Adaptive Access Manager-Oracle Access Manager Integration

If SOAP was used to communicate within Adaptive Strong Authenticator and Adaptive Risk Manager, replace the content of the previous installation with the oasa directory.

If Static-Linking was used, replace the content of the previous installation with the oasa_static directory.

14.4.6 Upgrading the Oracle Adaptive Access Manager BIP Reports

To upgrade the BIP Reports:

1. Back up all customized report templates (.rtf files) files.

   The files will be used later in the upgrade process.
2. Unzip patch_oaam_bipreports_oradb.zip.
3. Copy the contents of patch_oaam_bipreports_oradb.zip into the current BIP reports installation.
4. Restore your customized files to their directories in the updated application.
5. Verify that all the files have been copied into the directories

14.4.7 Upgrading Adaptive Risk Manager Offline

In order to upgrade the Oracle Adaptive Access Manager Offline application, follow the steps documented in this section.

14.4.7.1 Pre-requisites

Before applying the patch:

1. Ensure that you have access to the webapps directory of the Adaptive Risk Manager Offline application.
2. Shut down the Adaptive Risk Manager Offline application.
3. Shut down the Oracle Adaptive Access Manager database instance.
4. Back up all customized properties, .xml and keystore files.

   Some commonly customized files are: bharosa_server.properties, bharosa_client.properties, bharosa_common.properties, bharosauio_client.properties, sessions.xml, log4j.xml, and keystore files.

The files will be used later in the upgrade process.

5. It is highly recommended for you to take a backup of the entire install directory should you need to use it to revert back the patch.

14.4.7.2 Steps

To upgrade Adaptive Risk Manager Offline:

1. Unzip patch_oarm_offline_war.zip.
2. Copy the contents of patch_oarm_offline_war.zip into the existing webapps directory.
3. Restore your customized files to their directories in the updated application.
4. Verify that all the files have been copied into the directories

14.4.8 Upgrading Adaptive Risk Manager Online

In order to upgrade the Oracle Adaptive Access Manager Online application, follow the steps documented in this section.

14.4.8.1 Pre-requisites

Before applying the patch:

1. Shut down the Adaptive Risk Manager application.
2. Shut down the Oracle Adaptive Access Manager database instance.
3. Back up all customized properties, .xml and keystore files.

   Some commonly customized files are: bharosa_server.properties, bharosa_client.properties, bharosa_common.properties, bharosauio_client.properties, sessions.xml, log4j.xml, and keystore files.

   The files will be used later in the upgrade process.
4. It is highly recommended for you to take a backup of the entire install directory should you need to use it to revert back the patch.
5. Ensure that you have access to the webapps directory of the Adaptive Risk Manager Online application.
6. Ensure that you have applied the database patch.

14.4.8.2 Steps

To upgrade Adaptive Risk Manager Online:

1. Unzip patch_oarm_online_war.zip.
2. Copy the contents of patch_oarm_online_war.zip into the existing webapps directory.
3. Restore your customized files to their directories in the updated application.
4. Verify that all the files have been copied into the directories.

14.4.9 Upgrading Rule Conditions

In order to upgrade the rule conditions, follow the steps documented in this section.

14.4.9.1 Pre-requisites

Before applying the patch:

1. Ensure that you have applied the Adaptive Risk Manager Online/Offline patches.
2. Ensure that the updated applications are running.

14.4.9.2 Steps

To import patch_oaam_rule_conditions.zip:

1. On the Admin menu, point to Rule Templates, point to Conditions, then click Import Conditions.
2. Click Browse and locate patch_oaam_rule_conditions.zip.
3. Click Import.

All the conditions in the zip are imported into the server.

Note: If models are using the conditions, the conditions will be upgraded.

14.4.10 Upgrading Adaptive Strong Authenticator

To upgrade Adaptive Strong Authenticator

1. Ensure that you have access to the webapps directory.
2. Shut down the Adaptive Strong Authenticator application.
3. Back up all customized properties, .xml and keystore files.

   Some commonly customized files are: bharosa_server.properties, bharosa_client.properties, bharosa_common.properties, bharosauio_client.properties, sessions.xml, log4j.xml, and keystore files.

   The files will be used later in the upgrade process.
4. It is highly recommended for you to take a backup of the entire install directory should you need to use it to revert back the patch.
5. Unzip patch_oasa_static_war.zip or patch_oasa_war.zip.
6. Copy the contents of the patch into the current installation.
7. Restore your customized files to their directories in the updated application.
8. Verify that all the files have been copied into the directories.

14.4.11 Upgrading the Oracle Adaptive Access Manager Proxy for Apache

The Oracle Adaptive Access Manager patch contains updates for the Oracle Adaptive Access Manager Proxy for Apache for Microsoft Windows and Linux (rhel4). Follow the instructions in the *Oracle Adaptive Access Manager Developer's Guide* to replace the mod_uio.so and related .dlls (on MS Windows) and .so (on Linux) libraries with those released as part of this patch release.

14.4.11.1 Oracle Adaptive Access Manager Proxy for Apache Patch Installation Instructions

Installation of a patch is similar to installing the Oracle Adaptive Access Manager Proxy package using the instructions in the *Oracle Adaptive Access Manager Developer's Guide*. A patch will contain only the modified files. It is good practice to back up all your existing files since the patch will overwrite some or all of the files.

General instructions are given below. A patch contains only the modified files; so if a file is not available in the patch, skip that step. The steps are to be performed manually by the patch installer.

For both MS Windows and Linux:

1. Shut down the instance of Apache that you are updating

Note: Ensure that you are using Apache httpd, version 2.2.8 with mod_ssl.

2. Back up existing files: binary, .rng and .xml files
3. Copy the binary files from the patch (additionally on Linux, you need to set soft-links to .so files appropriately)
4. Copy UIO_Settings.rng and UIO_Config.rng files from the patch
5. Compare your existing UIO_Settings.xml and UIO_log4j.xml files with those given in the patch and verify that you have got the correct settings. Refer to the sections that apply to this patch in the *Oracle Adaptive Access Manager Developer's Guide* to ensure that you have the correct settings. The same also applies to your configuration XML files.
6. Start Apache and run your sanity tests
   - For Windows,
     - The binary files are: mod_uio.so, log4cxx.dll, libxml2.dll, apr_memcache.dll (apr_memcache.dll was introduced in 10.1.4.5.bp1)
     - The configuration files are: UIO_Settings.rng, UIO_Config.rng, UIO_Settings.xml, UIO_log4j.xml and application configuration XML files
   - For Linux,
     - The binary files are: mod_uio.so, liblog4cxx.so.0.10.0.0, libxml2.so.2.6.32, libapr_memcache.so.0.0.1
     - The binary configuration files are: UIO_Settings.rng, UIO_Config.rng, UIO_Settings.xml, UIO_log4j.xml and application configuration XML files

14.4.11.2 Oracle Adaptive Access Manager Proxy for Apache Patch Backout Instructions

Restore the files that you had backed up before you installed the patch.

14.4.12 Upgrading the Oracle Adaptive Access Manager Proxy for Microsoft ISA

To upgrade the Oracle Adaptive Access Manager Proxy for Microsoft ISA:

1. Stop the Microsoft ISA server with the following command:

```
net stop fwsrv
```

2. Back up the current Oracle Adaptive Access Manager Proxy for Microsoft ISA DLL. The DLL should usually be at: %ProgramFiles%\Microsoft ISA Server\BharosaProxy.dll.
3. Overwrite the existing DLL with the one from the patch.
4. Start Microsoft ISA server with the following command:

```
net start fwsrv
```

14.4.13 Upgrading .NET API

To apply the upgrade the .NET API, follow the instructions below.

14.4.13.1 Overview

The oaam_native\oaam_native_dot_net\bin directory contains the Oracle OAAM 10.1.4.5.bp2 .NET DLLs with the fix for the timestamp issue described in SR 7702452.994.

14.4.13.2 Applying the Fix

To apply the fix, replace the following two OAAM 10.1.4.5.bp2 DLLs that are currently in use with the files included in this fix. Please note that the fix includes Oracle OAAM .NET DLLs for .NET versions 1.1 and 2.0. Please use the version suitable for your environment.

```
Bharosa.VCrypy.Common.dll
Bharosa.VCrypy.Client.dll
```

Oracle strongly advises you to back up the existing files before applying the fix.

14.4.13.3 Fix Details

The previous version added the timestamp text to the authenticators by default, that is, the timestamp was added even if the "AuthentiPad.TimeStampText" property was not explicitly set by the API user.

The fix is to add the timestamp text only if the "AuthentiPad.TimeStampText" property was set by the API user.

14.4.14 Upgrading the Keystore Util Package

If you have already created your keystore, regenerating or applying this patch is not required.

To upgrade the keystore install package:

1. Back up all customized properties, .xml and keystore files.

   Some commonly customized files are: bharosa_server.properties, bharosa_client.properties, bharosa_common.properties, bharosauio_client.properties, sessions.xml, log4j.xml, and keystore files.

   The files will be used later in the upgrade process.

2. It is highly recommended for you to take a backup of the entire install directory should you need to use it to revert back the patch.
3. Unzip oaam_keystore_util.zip.
4. Copy the contents of oaam_keystore_util.zip into the keystore_util directory of the current installation.
5. Restore your customized files to their directories in the updated application.
6. Verify that all the files have been copied into the directories

14.5 Creating a Database for an Oracle Database with the Partition Option

Information about creating an OAAM database in Oracle databases with the partition option.

- Creating a Oracle Adaptive Access Manager Database Schema for an Oracle Database with the Partition Option
- Partition Reference

Patches after 10.1.4.5.bp1 contain the oracle_partition_rm_database_setup.zip file with the scripts to create the Oracle Adaptive Access Manager database schema for an Oracle database with the partition option.

After applying the update, it will be possible to create the Oracle Adaptive Access Manager database schema with partitions in the Oracle database.

14.5.1 Creating a Oracle Adaptive Access Manager Database Schema for an Oracle Database with the Partition Option

To create the Oracle Adaptive Access Manager database schema for an Oracle database with the partition option, follow the steps below:

1. Replace the oracle_partition_rm_database_setup.zip file in the 10.1.4.5.bp1 with the file included in this patch.
2. Then, follow the database schema creation instructions to create an Oracle Adaptive Access Manager database schema in the Oracle database.

   Please refer to Chapter 3, "Creating an Oracle Database Schema," in the *Oracle Adaptive Access Manager Installation and Configuration Guide*.

   Instructions for an Oracle database with the partition option are the same as those for one without the option.

   For information on the partition tables and scripts to maintain the partition, refer to Chapter 3, "Creating an Oracle Database Schema," in the *Oracle Adaptive Access Manager Installation and Configuration Guide*.

14.5.2 Partition Reference

Database tables in the Oracle Adaptive Access Manager database are divided into three different categories. The composite partition (RANGE,HASH) is in all the tables. The Range partition is created using CREATE_TIME while the HASH key is defined as per application logic.

14.5.2.1 Tables

Details about partitioned and non-partitioned tables are provided below.

14.5.2.1.1 Static Partition Tables

Frequency: Monthly

Tables:

- V_USER_QA
- V_USER_QA_HIST

14.5.2.1.2 Transactional Partition Tables

Frequency: Monthly

Tables:

- VCRYPT_TRACKER_NODE_HISTORY
- VCRYPT_TRACKER_USERNODE_LOGS
- VCRYPT_TRACKER_NODE
- VT_USER_DEVICE_MAP
- V_MONITOR_DATA
- VT_SESSION_ACTION_MAP
- VT_ENTITY_ONE
- VT_ENTITY_ONE_PROFILE
- VT_USER_ENTITY1_MAP
- VT_ENT_TRX_MAP
- VT_TRX_DATA
- VT_TRX_LOGS

Frequency: Weekly

Tables:

- VR_POLICYSET_LOGS
- VR_POLICY_LOGS
- VR_RULE_LOGS
- VR_MODEL_LOGS

Other than the tables mentioned above, all other tables are non-partitioned.

14.5.2.2 Partition Maintenance Scripts

After the initial Oracle Adaptive Access Manager Repository setup, use the following scripts to maintain the partition.

14.5.2.2.1 Add_Monthly_Partition_tables.sql This script should be used to add partitions for tables with the Monthly frequency.

The script should be run at the end of each month to create partitions for the following month. To add partitions for subsequent months at the same time, run this script multiple times; when you run the script multiple times, partitions are added based on their previous month's partition.

If you fail to run the script to create monthly partitions (if your monthly partition is missing), the database errors, "ORA-14400 and ORA-14401," are encountered, forcing the Oracle Adaptive Access Manager application to stop.

To avoid errors, it is recommend that you schedule this script as an automated job.

14.5.2.2.2 Add_Weekly_Partition_tables.sql This script should be used to add partitions for tables with the Weekly frequency.

The script should be run at the end of each month to create partitions for the following week. To add partitions for subsequent weeks at the same time, run this script multiple times; when you run the script multiple times, partitions are added based on their previous week's partition.

If you fail to run the script to create weekly partitions (if your weekly partition is missing), the database errors, "ORA-14400 and ORA-14401," are encountered, forcing the Oracle Adaptive Access Manager application to stop.

To avoid errors, it is recommend that you schedule this script as an automated job.

14.5.2.2.3 Drop_Monthly_Partition_tables.sql Use this script to drop partitions for tables with the monthly frequency. Run this script at the end of each month to drop partitions that are older than sixth months as per the Oracle Adaptive Access Manager application requirement. Eventually, these tables will have six partitions at any point.

14.5.2.2.4 Drop_Weekly_Partition_tables.sql Use this script to drop partitions for tables with the weekly frequency. Run this script at the end of every two weeks, starting from your database creation date, to drop partitions older than two weeks as per the Oracle Adaptive Access Manager application requirement.

14.6 Upgrading the Database from 10.1.4.5.0 to 10.1.4.5.bp1

This section provides instructions for upgrading the database from 10.1.4.5.0 to 10.1.4.5.bp1.

Note: Before you start the upgrade process, it is strongly recommended that you perform a full database backup.

14.6.1 Database Patch Requirement

The database patch should be installed on systems where the base 10.1.4.5 Oracle Adaptive Access Manager database schema is created.

14.6.2 Database Patch Details

This incremental upgrade will perform the following tasks for database performance:

- Create additional indexes for performance
- Remove foreign keys from Transactional tables
- Change VCRYPT_TRACKER_USERNODE_LOGS to modify the column TRACKER_NODE_HISTORY_ID to null

For more information on the indexes created and the foreign keys that are removed, refer to Section 14.7, "10.1.4.5.bp1 Database Patch Details."

14.6.3 Database Patch Installation Instructions

Before applying the database patch:

1. Unzip oaam_bundle_patch_10_1_4_5_bp5.zip.
2. Copy the database script (for Oracle database or Microsoft SQL Server) from the oaam_db/db_patches/bp01 directory to your database server.
3. Bring down your system.

For Oracle

To install the database patch for an Oracle Adaptive Access Manager database on an Oracle server:

1. Create a patch directory, oaam_db_patch_oracle_10.1.4.5_01.
2. Move oaam_db_patch_oracle_10_1_4_5_01.sql to your patch directory.
3. Login to the database using the Oracle Adaptive Access Manager schema username and password.

   ```
   sqlplus <OAAM>/<PASSWORD>
   ```

4. Run the oaam_db_patch_oracle_10_1_4_5_01.sql script.

   For example:

   ```
   SQL > @oaam_db_patch_oracle_10_1_4_5_01.sql
   ```

5. Check the oaam_db_patch_oracle_10_1_4_5_01.log for any error. Please contact Oracle Support if you experience any ORA- errors in the log.

For Microsoft SQL Server

To install the database patch for an Oracle Adaptive Access Manager database on a Microsoft SQL Server:

1. Create a patch directory, oaam_db_patch_mssql_10.1.4.5_01.
2. Move oaam_db_patch_mssql_10_1_4_5_01.sql to your patch directory.
3. Login to OAAM database using Microsoft SQL Server Management Studio.
4. Open the patch file: from the File menu, point to Open, click File. Then, navigate to the patch directory, oaam_db_patch_mssql_10.1.4.5_01, and select oaam_db_patch_mssql_10_1_4_5_01.sql.
5. In the Query Window, please change following lines:

   ```
   USE [DATABASE_NAME]
   ```

   to

   ```
   USE <your OAAM Database>
   ```

6. Execute the script.
7. Contact Oracle Support for any errors.

14.6.4 Database Patch Execution Time

It would take approximately 5 minutes to run the scripts. However, if the database has not been regularly purged, it may take longer time.

14.6.5 Database Patch Special Instruction

N/A

14.6.6 Best Practices

The system should be brought down before applying the database patch.

After the patch has been applied, restart the system.

14.7 10.1.4.5.bp1 Database Patch Details

Changes and additions to the database as a result of installing the database patch are listed below.

14.7.1 Create additional indexes for performance

This patch creates additional indexes for the performance of the Oracle Adaptive Access Manager system. The following indexes will be created:

- VCRYPT_TRACKER_USERNODE_LOGS("CREATE_TIME")
- VT_TRX_DATA("DATA1","ROW_ORDER")
- VT_TRX_DATA("DATA2","ROW_ORDER")
- VT_TRX_DATA("DATA3","ROW_ORDER")
- VT_ENTITY_ONE("ENTITY_KEY")
- VT_ENT_TRX_MAP("TRX_ID")
- VT_ENTITY_ONE_PROFILE (DATA3)
- VT_ENTITY_ONE_PROFILE (DATA2)
- VT_ENTITY_ONE_PROFILE (DATA1)
- VT_ENTITY_ONE_PROFILE (ROW_ORDER)
- VT_ENTITY_ONE_PROFILE (ROW_ORDER,DATA1,EXPIRE_TIME)
- VT_TRX_DATA (TRX_ID, ROW_ORDER)
- VT_TRX_DATA (NUM_DATA0)
- VT_TRX_DATA (NUM_DATA1)
- VT_TRX_DATA (NUM_DATA2)
- VT_TRX_LOGS (TRX_DEF_ID)
- VT_TRX_LOGS (CREATE_TIME)
- VT_ENT_TRX_MAP (DEF_MAP_ID)
- VT_ENT_TRX_MAP (MAP_OBJ_ID)

14.7.2 Remove foreign keys from Transactional tables

This patch will remove the following foreign keys from the Transactional tables:

- V_FP_MAP(V_FP_MAP_FK0)
- V_FPRINTS(V_FPRINTS_FK0)
- VCRYPT_TRACKER_NODE(VCRYPT_TRACKER_NODE_FK0)
- VCRYPT_TRACKER_NODE(VCRYPT_TRACKER_NODE_FK1)
- VCRYPT_TRACKER_NODE_HISTORY(VCRYPT_TRACKER_NODE_HISTORY_FK0)
- VCRYPT_TRACKER_NODE_HISTORY(VCRYPT_TRACKER_NODE_HISTORY_FK1)
- VCRYPT_TRACKER_USERNODE_LOGS(VCRYPT_TRACKER_USERNODE_LOGS_FK0

- VCRYPT_TRACKER_USERNODE_LOGS(VCRYPT_TRACKER_USERNODE_LOGS_FK1)
- VCRYPT_TRACKER_USERNODE_LOGS(VCRYPT_TRACKER_USERNODE_LOGS_FK2)
- VCRYPT_TRACKER_USERNODE_LOGS(VCRYPT_TRACKER_USERNODE_LOGS_FK3)
- VT_ENT_TRX_MAP(VT_ENT_TRX_MAP_FK0)
- VT_ENTITY_ONE(VT_ENTITY_ONE_FK0)
- VT_ENTITY_ONE_PROFILE(VT_ENTITY_ONE_PROFILE_FK0)
- VT_ENTITY_ONE_PROFILE(VT_ENTITY_ONE_PROFILE_FK1)
- VT_TRX_DATA(VT_TRX_DATA_FK0)
- VT_TRX_DATA(VT_TRX_DATA_FK1)
- VT_TRX_LOGS(VT_TRX_LOGS_FK0)
- VT_TRX_LOGS(VT_TRX_LOGS_FK1)
- VT_USER(VT_USER_FK0)
- VT_USER_DEVICE_MAP(VT_USER_DEVICE_MAP_FK0)
- VT_USER_DEVICE_MAP(VT_USER_DEVICE_MAP_FK1)
- VT_USER_DEVICE_MAP(VT_USER_DEVICE_MAP_FK2)
- VT_USER_DEVICE_MAP(VT_USER_DEVICE_MAP_FK3)
- VT_WF_DAYS(VT_WF_DAYS_FK0)
- VT_WF_DAYS(VT_WF_DAYS_FK1)
- VT_WF_HOURS(VT_WF_HOURS_FK0)
- VT_WF_HOURS(VT_WF_HOURS_FK1)
- VT_WF_MONTHS(VT_WF_MONTHS_FK0)
- VT_WF_MONTHS(VT_WF_MONTHS_FK1)
- VT_WF_YEARS(VT_WF_YEARS_FK0)
- VT_WF_YEARS(VT_WF_YEARS_FK1)

14.7.3 Change VCRYPT_TRACKER_USERNODE_LOGS

The patch will also change VCRYPT_TRACKER_USERNODE_LOGS to modify the column TRACKER_NODE_HISTORY_ID to null.

14.8 Upgrading the Database from 10.1.4.5.bp1 to 10.1.4.5.bp2

This section provides information about the setup and execution of the database patch to upgrade Oracle Adaptive Access Manager 10.1.4.5.bp1 to 10.1.4.5.bp2.

Note: Before you start the upgrade process, it is strongly recommended that you perform a full database backup.

14.8.1 Database Patch Requirement

This patch should be applied where the Oracle Adaptive Access Manager 10.1.4.5.bp2 database patch is already installed.

14.8.2 Database Pre-requisite

Ensure that the database server is not connected to the application server(s).

14.8.3 Database Patch Details

This patch introduces new tables, indexes, and columns related to the Scheduler and Auto-learning features of Oracle Adaptive Access Manager.

The list of changes is provided in Section 14.9, "10.1.4.5.bp2 Database Patch Details."

14.8.4 Database Patch Installation Instructions

Instructions to install the 10.1.4.5.bp2 database patch are provided below.

For Oracle

To install the database patch for an Oracle Adaptive Access Manager database on an Oracle server:

1. Create a patch directory, oaam_db_patch_oracle_10.1.4.5_02.
2. Copy all the scripts from the oaam_db/db_patches/bp02 directory to the patch directory.

   You will be copying the following scripts:

   - db_upgrade.sql
   - oaam_db_patch_oracle_10_1_4_5_02.sql
   - oaam_db_oracle_CreateMonitorDataRollupTask.sql
   - oaam_db_patch_oracle_10_1_4_5_02_oneoff.sql

Note: The one-off script, oaam_db_patch_oracle_10_1_4_5_02_oneoff.sql, is not required. It should only be used if there are ORA-01758 or ORA-00904 exceptions in oaam_db_patch_oracle_10_1_4_5_02.log.

---

3. Log in to the database using the Oracle Adaptive Access Manager schema username and password.

   ```
   sqlplus <OAAM>/<PASSWORD>
   ```

4. Run the db_upgrade.sql script.

   For example:

   ```
   SQL > @db_upgrade.sql
   ```

5. Check the oaam_db_patch_oracle_10_1_4_5_02.log file and create_monitor_rollup.lst spool for any errors. Please contact Oracle Support if you experience any ORA- errors in the log.

For Microsoft SQL Server

To install the database patch for an Oracle Adaptive Access Manager database on a Microsoft SQL Server:

1. Create a patch directory, oaam_db_patch_mssql_10_1_4_5_02.
2. For a non- Unicode database, copy all the scripts from the oaam_db/db_patches/bp02/msql_db_nonunicode directory to your patch directory.

   You will be copying the following scripts:

   - 01_oaam_db_patch_mssql_10_1_4_5_02.sql
   - 02_oaam_db_CreateMonitorDataRollupTask_mssql.sql
3. For a Unicode database, copy all the scripts from the oaam_db/db_patches/bp02/msql_db_unicode directory to your patch directory.

   You will be copying the following scripts:

   - 01_oaam_db_patch_mssql_unicode_10_1_4_5_02.sql
   - 02_oaam_db_CreateMonitorDataRollupTask_mssql.sql
4. Log in to the OAAM database using Microsoft SQL Server Management Studio.
5. For a non- Unicode database:
   a. Open the patch file and then navigate to the patch directory, oaam_db_patch_mssql_10_1_4_5_02.

      To open the patch file, from the File menu, point to Open, click File.

Note: In the Query Window, ensure that you change `USE <DATABASE_NAME>` to `USE <YOUR_OAAM_DATABASE_NAME>` before executing the scripts.

   b. Select 01_oaam_db_patch_mssql_10_1_4_5_02.sql and Execute.
   c. Select 02_oaam_db_CreateMonitorDataRollupTask_mssql.sql and Execute.
6. For a Unicode database:
   a. Open the patch file and then navigate to the patch directory, oaam_db_patch_mssql_10_1_4_5_02.

      To open the patch file, from the File menu, point to Open, click File.

Note: In the Query Window, ensure that you change `USE <DATABASE_NAME>` to `USE <YOUR_OAAM_DATABASE_NAME>` before executing the scripts.

   b. Select oaam_db_patch_mssql_unicode_10_1_4_5_02.sql and Execute.
   c. Select 02_oaam_db_CreateMonitorDataRollupTask_mssql.sql and Execute.
7. Contact Oracle Support for any errors.

Note: If streams replication is enabled, run the scripts only on the active master node or run the scripts on all the nodes using tag.

14.8.5 Validation

To test that the scripts executed successfully to install the database patch, follow the steps listed below.

For Oracle

To validate that the scripts are successfully executed, check the oaam_db_patch_oracle_10_1_4_5_02.log file for any error.

For the Microsoft SQL Server Database

To validate that the scripts are successfully executed, check the output of the Microsoft SQL Server Management Studio.

14.8.6 Server Restart

After the upgrade process, restart the application server.

You will not have to restart the database server.

14.9 10.1.4.5.bp2 Database Patch Details

Database patch details are listed below.

14.9.1 Objects Altered or Added

The following objects are altered or added.

14.9.1.1 Columns

The following columns are altered or added.

- VCRYPT_TRACKER_USERNODE_LOGS.CACHE
- VR_RULESET_ROW.CHAIN_POLICY
- VR_RULESET_ROW_HIST.CHAIN_POLICY
- V_ACTION_LOG_SESS.CLIENT_ID
- V_ACTION_LOG_SESS.CLIENT_SESS_ID
- V_ACTION_LOG_SESS.CLIENT_VER
- VCRYPT_ALERT.EXEC_TIME
- VT_SESSION_ACTION_MAP.EXEC_TIME_MS
- VT_IP_CLUSTER.GLOBAL_ID
- VT_IP_CLUSTER_GROUP.GLOBAL_ID
- VRA_SESS_SET_HIST.GLOBAL_ID
- VRA_SESS_SET.GLOBAL_ID
- VCRYPT_ALERT.GLOBAL_ID
- VT_IP_CLUSTER_GROUPMAP.GLOBAL_ID
- VT_DYN_ACT_EXEC_LOG.OBJECT_ID
- VT_DYN_ACT_EXEC_LOG.OBJECT_TYPE
- VR_DYN_ACTION_INST_HIST.REF_ID

- VR_DYN_ACTION_INST.REF_ID
- VR_DYN_ACTION_INST_HIST.REF_TYPE
- VR_DYN_ACTION_INST.REF_TYPE
- VT_ENTITY_ONE_PROFILE.RENEW_TIME
- VT_SESSION_ACTION_MAP.RULE_TRACE_FP_ID
- V_ACTION_LOG_SESS.SERVER_ID
- VT_DYN_ACT_EXEC_LOG.TRX_DEF_ID
- VT_DYN_ACT_EXEC_LOG.TRX_ID
- V_ACTION_LOG_SESS.USER_AGENT

14.9.1.2 Constraints

The following constraints are added or modified.

- PK_VR_DA_RT_CRIT on VR_DA_RT_CRIT
- PK_VR_DA_RT_CRIT_HIST on VR_DA_RT_CRIT_HIST
- PK_VR_POST_ACTION on VR_POST_ACTION
- PK_VR_POST_ACTION_HIST on VR_POST_ACTION_HIST
- PK_VS_GRP_EXEC_LOG on VS_GRP_EXEC_LOG
- PK_VS_GRP_EXEC_REC on VS_GRP_EXEC_REC
- PK_VS_GRP_QUEUED on VS_GRP_QUEUED
- PK_VS_TASK on VS_TASK
- PK_VS_TASK_EXEC_LOG on VS_TASK_EXEC_LOG
- PK_VS_TASK_EXEC_REC on VS_TASK_EXEC_REC
- PK_VS_TASK_GRP on VS_TASK_GRP
- PK_VS_TASK_GRP_HIST on VS_TASK_GRP_HIST
- PK_VS_TASK_HIST on VS_TASK_HIST
- PK_VS_TASK_PROP on VS_TASK_PROP
- PK_VS_TASK_PROP_HIST on VS_TASK_PROP_HIST
- PK_VT_SESS_AUTH_MAP on VT_SESS_AUTH_MAP
- PK_VT_WF on VT_WF
- PK_V_LOCK on V_LOCK
- PK_V_SESS_TRACE_LOG on V_SESS_TRACE_LOG
- VRA_SESS_SET_UK0 on VRA_SESS_SET
- VR_DA_RT_CRIT_FK0 on VR_DA_RT_CRIT
- VR_DA_RT_CRIT_FK1 on VR_DA_RT_CRIT
- VR_DA_RT_CRIT_FK2 on VR_DA_RT_CRIT
- VR_DA_RT_CRIT_FK3 on VR_DA_RT_CRIT
- VR_DA_RT_CRIT_FK4 on VR_DA_RT_CRIT
- VR_DA_RT_CRIT_HIST_FK0 on VR_DA_RT_CRIT_HIST

- VR_DA_RT_CRIT_HIST_UK0 on VR_DA_RT_CRIT_HIST
- VR_DA_RT_CRIT_UK0 on VR_DA_RT_CRIT
- VR_DYN_ACTION_INST_FK1 on VR_DYN_ACTION_INST
- VR_POST_ACTION_UK0 on VR_POST_ACTION
- VS_GRP_EXEC_LOG_FK0 on VS_GRP_EXEC_LOG
- VS_GRP_EXEC_REC_FK0 on VS_GRP_EXEC_REC
- VS_GRP_QUEUED_FK0 on VS_GRP_QUEUED
- VS_TASK_EXEC_LOG_FK0 on VS_TASK_EXEC_LOG
- VS_TASK_EXEC_REC_FK0 on VS_TASK_EXEC_REC
- VS_TASK_EXEC_REC_FK1 on VS_TASK_EXEC_REC
- VS_TASK_FK0 on VS_TASK
- VS_TASK_GRP_UK0 on VS_TASK_GRP
- VS_TASK_PROP_FK0 on VS_TASK_PROP
- VS_TASK_PROP_UK0 on VS_TASK_PROP
- VS_TASK_UK0 on VS_TASK
- V_SESS_TRACE_LOG_FK0 on V_SESS_TRACE_LOG

14.9.1.3 Indexes

The following indexes are added or modified.

- PK_VR_DA_RT_CRIT on VR_DA_RT_CRIT
- PK_VR_DA_RT_CRIT_HIST on VR_DA_RT_CRIT_HIST
- PK_VR_POST_ACTION on VR_POST_ACTION
- PK_VR_POST_ACTION_HIST on VR_POST_ACTION_HIST
- PK_VS_GRP_EXEC_LOG on VS_GRP_EXEC_LOG
- PK_VS_GRP_EXEC_REC on VS_GRP_EXEC_REC
- PK_VS_GRP_QUEUED on VS_GRP_QUEUED
- PK_VS_TASK on VS_TASK
- PK_VS_TASK_EXEC_LOG on VS_TASK_EXEC_LOG
- PK_VS_TASK_EXEC_REC on VS_TASK_EXEC_REC
- PK_VS_TASK_GRP on VS_TASK_GRP
- PK_VS_TASK_GRP_HIST on VS_TASK_GRP_HIST
- PK_VS_TASK_HIST on VS_TASK_HIST
- PK_VS_TASK_PROP on VS_TASK_PROP
- PK_VS_TASK_PROP_HIST on VS_TASK_PROP_HIST
- PK_VT_SESS_AUTH_MAP on VT_SESS_AUTH_MAP
- PK_VT_WF on VT_WF
- PK_V_LOCK on V_LOCK
- PK_V_SESS_TRACE_LOG on V_SESS_TRACE_LOG

- VRA_SESS_SET_UK0 on VRA_SESS_SET
- VR_DA_RT_CRIT_HIST_UK0 on VR_DA_RT_CRIT_HIST
- VR_DA_RT_CRIT_UK0 on VR_DA_RT_CRIT
- VR_POST_ACTION_UK0 on VR_POST_ACTION
- VS_GRP_EXEC_LOG_IDX0 on VS_GRP_EXEC_LOG
- VS_GRP_EXEC_REC_IDX0 on VS_GRP_EXEC_REC
- VS_GRP_EXEC_REC_IDX1 on VS_GRP_EXEC_REC
- VS_GRP_QUEUED_IDX0 on VS_GRP_QUEUED
- VS_TASK_EXEC_LOG_IDX0 on VS_TASK_EXEC_LOG
- VS_TASK_EXEC_REC_IDX0 on VS_TASK_EXEC_REC
- VS_TASK_EXEC_REC_IDX1 on VS_TASK_EXEC_REC
- VS_TASK_GRP_IDX0 on VS_TASK_GRP
- VS_TASK_GRP_IDX1 on VS_TASK_GRP
- VS_TASK_GRP_IDX2 on VS_TASK_GRP
- VS_TASK_GRP_UK0 on VS_TASK_GRP
- VS_TASK_IDX0 on VS_TASK
- VS_TASK_IDX1 on VS_TASK
- VS_TASK_IDX2 on VS_TASK
- VS_TASK_PROP_IDX0 on VS_TASK_PROP
- VS_TASK_PROP_UK0 on VS_TASK_PROP
- VS_TASK_UK0 on VS_TASK
- VT_SESS_AUTH_MAP_IDX1 on VT_SESS_AUTH_MAP
- VT_WF_IDX0 on VT_WF
- V_ALERT_IDX2 on VCRYPT_ALERT
- V_ALERT_IDX3 on VCRYPT_ALERT
- V_LOCK_IDX0 on V_LOCK
- V_SESS_TRACE_LOG_IDX0 on V_SESS_TRACE_LOG

14.9.1.4 Sequences

The following sequences are added or modified.

- VR_DA_RT_CRIT_HIST_SEQ
- VR_DA_RT_CRIT_SEQ
- VR_POST_ACTION_HIST_SEQ
- VR_POST_ACTION_SEQ
- VS_GRP_EXEC_LOG_SEQ
- VS_GRP_EXEC_REC_SEQ
- VS_GRP_QUEUED_SEQ
- VS_TASK_EXEC_LOG_SEQ

- VS_TASK_EXEC_REC_SEQ
- VS_TASK_GRP_HIST_SEQ
- VS_TASK_GRP_SEQ
- VS_TASK_HIST_SEQ
- VS_TASK_PROP_HIST_SEQ
- VS_TASK_PROP_SEQ
- VS_TASK_SEQ
- VT_SESS_AUTH_MAP_SEQ
- VT_WF_SEQ
- V_LOCK_SEQ
- V_SESS_TRACE_LOG_SEQ

14.9.1.5 Tables

The following tables are added or modified.

- VR_DA_RT_CRIT
- VR_DA_RT_CRIT_HIST
- VR_POST_ACTION
- VR_POST_ACTION_HIST
- VS_GRP_EXEC_LOG
- VS_GRP_EXEC_REC
- VS_GRP_QUEUED
- VS_TASK
- VS_TASK_EXEC_LOG
- VS_TASK_EXEC_REC
- VS_TASK_GRP
- VS_TASK_GRP_HIST
- VS_TASK_HIST
- VS_TASK_PROP
- VS_TASK_PROP_HIST
- VT_SESS_AUTH_MAP
- VT_WF
- V_LOCK
- V_SESS_TRACE_LOG

14.9.2 Seed Data

The database upgrade patch will also insert seed data into Scheduler-related tables.

14.10 Setting Up Database Archive and Purge Routines (10.1.4.5.bp3)

Archive and purge scripts were added as part of 10.1.4.5.bp3.

If you want to set up purging routines, you will have to perform additional steps, which are documented in the Readme. Otherwise, skip this section and go on to Section 14.12, "Upgrading the Database from 10.1.4.5.bp2 to 10.1.4.5.bp5."

The files are located in the oaam_db\db_patches\bp03\purge_scripts directory

---

Note: Before you start the upgrade process, it is strongly recommended that you perform a full database backup.

Please refer to Section 14.10, "Setting Up Database Archive and Purge Routines (10.1.4.5.bp3)" for instructions.

Note: You must be running a 10.1.4.5.bp2 Oracle Adaptive Access Manager database before you can set up the archive and purging routines.

Information about setting up purging routines are additions or corrections to Appendix E, "Archive and Purge," in the *Oracle Adaptive Access Manager Installation and Configuration Guide*.

This section presents the concepts, prerequisites, policy, and post-process procedures in archiving and purging the Oracle Adaptive Access Manager database. A DBA or system administrator, who performs routine maintenance and the archiving and purging of the Oracle Adaptive Access Manager database, should follow the instructions in this chapter.

Note: Users can run the purging scripts online in the Enterprise version of MS SQL server 2005.

14.10.1 Purge Process

Purging is the process of freeing up space in the database or of deleting obsolete data that is not required by the system. The purge process can be based on the age of the data or the type of data.

14.10.2 Archive Process

Archiving is the process of backing up the obsolete data that will be deleted during the purge process. During the archive process, data will be moved from the main transactional tables to the backup tables. By default the Oracle Adaptive Access Manager purge scripts will archive data that will be deleted during the purge process.

14.10.3 Archive and Purge Data Classification

Oracle Adaptive Access Manager has different sets of transactional tables that will be archived and purged. These sets are documented below. The tables in the transaction table sets are listed in Section 14.11.1, "List of Tables and the Corresponding Archived Tables."

14.10.3.1 Device Fingerprinting

The device fingerprinting data is archived and purged based on the following criteria:

- archive and purge the device fingerprinting logs that are older than a specified period first.
- archive and purge user device maps that are not used after the data from the device fingerprinting logs is purged.
- archive and purge the device history that is not used after the data from the device fingerprinting logs is purged.
- archive and purge the device data that is not used after the data from the device fingerprinting logs is purged.

Note: The VT_SESSION_ACTION_MAP table is not purged using the partition drop maintenance script. This table stores the device fingerprinting session information; therefore the purging of this table is performed using the manual purge stored procedure (SP_SESS_ACT_MAP_PROC) which is called by the exec_sp_purge_tracker_data.sql script.

14.10.3.2 Transaction In-Session Based Data

The in-session transaction data is archived and purged based on the following criteria:

- archive and purge the in-session transactional-based data that is older than a specified period first.
- archive and purge transaction data that is not used in the transaction data after the transactions logs are purged for a specific time period.
- archive and purge the entity, entity profile, user entity map and entity transaction map after the transactions logs are purged for a specific time period.

14.10.3.3 Auto-learning Profile Data

The Auto-learning and profile data is archived and purged based on the following criteria:

- archive and purge the Workflow tables based on a specific time period.
  - HOURS based Workflow tables will retain 3 days' worth of data.
  - DAYS based Workflow tables will retain 32 days' worth of data.
  - MONTHS based Workflow tables will retain 1 year's worth of data.
  - YEARS based Workflow tables will retain 5 years' worth of data.

  These values are hard-coded. The profile data value can be changed in the execution script for no of days.
- archive and purge fingerprinting data with fingerprint type 11, 12, and no child records in the Workflow tables

```
vcrypt.fingerprint.type.enum.autolearning.auth=11
vcrypt.fingerprint.type.enum.autolearning.transaction=12
```

  - 11 is the enum value for the Auto-learning AUTH type. Change these values in the script if another value was used during integration.

  - 12 is enum value for the Auto-learning TRANSACTION type. Change these values in the script if another value was used during integration.
- archive and purge profile related data that is 183 days old and profiles type 2 (Auto-learning Profile) from the Auto-learning profiles tables.

14.10.3.4 Rule Log Data

The rule log transaction data is archived and purged based on the following criteria:

- archive and purge the rule log data that is 30 days old

14.10.4 Archive and Purge Process

Updated procedures for the archive and purge process are provided below.

14.10.4.1 Archive and Purge Process - Special Recommendations for Schemas with Partitioned Objects

Special recommendations are listed below for schemas with partitioned objects.

14.10.4.1.1 Schema with Partitioned Objects (Oracle Databases Only) Without a Separate Reporting Database If you are using an Oracle Adaptive Access Manager schema with the partition option enabled and do not have a separate reporting and administrative environment, perform only manual purging, as described in this document. Partition drop scripts are part of the partition base package. These scripts are not shipped with the purging scripts.

Follow the steps below:

1. Set up archive and purge routines.
2. Schedule archive and purge routines.

14.10.4.1.2 Schema with Partitioned Objects (Oracle Databases Only) With a Separate Reporting Database If you are using an Oracle Adaptive Access Manager schema with the partition option enabled and have a separate reporting and administrative environment, you must perform manual purging, as described below, as well as run the partition maintenance scripts that are shipped with the Oracle Adaptive Access Manager database setup package.

Note: Please make sure replication is not enable during the archive and purge process.

Follow the steps below:

1. Set up archive and purge routines.
2. Schedule monthly/weekly partition drops. Refer to Section 14.11.4, "Drop Scripts for Partitioned Tables."
3. Schedule archive and purge routines.

14.10.4.2 Archive and Purge Process - Setting Up for Users with an Existing Process In Place

The setup scripts are one-time scripts that are required to create objects for the archive and purge process. The setup scripts will create the archived tables and store procedure required to execute during the routine archive and purge process.

If you are already using the Oracle Adaptive Access Manager Archive and Purge process, you should back up your existing archived tables (listed in Section 14.11.1, "List of Tables and the Corresponding Archived Tables") on disk before setting up a new archive and purge process. With 10.1.4.5.bp2, the structure of the old tables has changed; the setup scripts will recreate these tables.

14.10.4.3 Archive and Purge Process - Setting Up for the Oracle Database

The Create_purge_proc.sql script is required to set up the archive and purge routines for the Oracle database. For more information on this script, refer to Section 14.11.2.1, "Scripts for the Oracle Database."

14.10.4.3.1 Prerequisite

Important

You must ensure that the Oracle Adaptive Access Manager schema has the following privileges granted before the execution of the purging/archiving scripts and revoked after the execution of the purging/archiving scripts:

- Create procedure
- Execute procedure
- Create any procedure
- Create any table
- Create any index

The purging/archiving scripts need CREATE Any privilege to create and execute purge related stored procedures.

Since the purging/archiving scripts use custom rebuild index stored procedures for a given table, this stored procedure requires CREATE Any Table and Create Any index privileges granted to the OAAM schema. If these privileges are not granted, the rebuild_oaam_index stored procedure will not work.

These privileges must be granted to set up and execute the OAAM purging/archiving routines and must be revoked once purge/archiving process is completed.

14.10.4.3.2 Instructions To set up the archive and purge process for the Oracle database, follow the steps below:

1. Create the script directory, oaam_purge_script.
2. Unzip the Oracle Adaptive Access Manager purge package Oracle scripts to the script directory.
3. Log in to the database using the `system` or `sys` account.
4. Grant privileges to the Oracle Adaptive Access Manager schema:

```
GRANT create any procedure TO <schema_name>;
GRANT create any table TO <schema_name>;
GRANT create any index TO <schema name>;
GRANT create procedure TO <schema_name>;
GRANT execute any procedure TO <schema_name>;
```

5. Connect to database using the Oracle Adaptive Access Manager schema.

```
For example, sqlplus <OAAMADMIN>/<PASSWORD>
```

6. Run the create_purge_proc.sql script

```
SQL>@ create_purge_proc.sql
```

14.10.4.4 Archive and Purge Process - Setting Up for the SQL Server Database

The required scripts to setup the archive and purge routines for the SQL Server database are listed below.

If you are using Microsoft SQL Server with globalization support, please use the scripts under the msql_db_unicode directory.

If you are using Microsoft SQL Server with non-globalization support, please use the scripts under the msql_db_nonunicode directory.

The required scripts to setup the archive and purge routines for the SQL Server database are listed below. For more information on these scripts, refer to Section 14.11.2.2, "Scripts for the SQL Server Database."

- cr_vcrypt_purge_tables.sql
- cr_sp_arch_purge_tracker_data.sql
- cr_sp_arch_purge_txn_logs.sql
- cr_sp_arch_purge_workflow_data.sql
- cr_sp_arch_purge_profile_data.sql
- cr_sp_arch_purge_rules_log.sql

To setup the archive and purge process for the SQL Server database, follow the steps below:

1. Create the script directory, oaam_purge_script.
2. Unzip the Oracle Adaptive Access Manager purge package SQL Server scripts to the script directory.
3. Login to the Oracle Adaptive Access Manager database using SQL Server Management Studio.
4. Open the script files, which are listed below, using File > Open > File. Then, navigate to the script directory.
   - cr_vcrypt_purge_tables.sql
   - cr_sp_arch_purge_tracker_data.sql
   - cr_sp_arch_purge_txn_logs.sql
   - cr_sp_arch_purge_workflow_data.sql
   - cr_sp_arch_purge_profile_data.sql
   - cr_sp_arch_purge_rules_log.sql
5. In the Query window, change the following line for every script:

   ```
   USE [DATABASE_NAME] to USE < your OAAM Database>
   ```

6. Execute the scripts.
7. In the message window of SQL Server Management Studio, save the results to a file.

14.10.5 Performing Archive and Purge

The execution of the archive and purge scripts is described below. Prior to starting the archive and purge process, go through the checklist, which is documented below, to ensure that the requirements for archive and purge are met.

- Setup of the archive and purge scripts.
- Enough space is available on the database server to store the archived data, if archive is enabled for the purge.
- Archive and purge could be resource (like CPU) intensive. Oracle recommends running these during off peak load hours.

14.10.5.1 Oracle Databases

The required scripts to execute archive and purge routines for the Oracle database are listed below. For more information on these scripts, refer to Section 14.11.3, "Scripts to Execute Archive and Purge."

Archive and purge periods are set based on the business requirement specified for retention periods.

By default, the archive and purge scripts/routines have the following two parameters set:

- p_days1 =no of days for data retention
- p_archived= archived flag

To change these values per the business requirement, modify the following scripts:

- exec_sp_purge_tracker_data.sql
- exec_sp_purge_txn_log.sql
- exec_sp_purge_workflow_data.sql
- exec_sp_purge_profile_data.sql
- exec_sp_purge_rule_log.sql

14.10.5.1.1 Manual Execution To execute the scripts to archive and purge, follow the steps below:

1. Create the script directory, oaam_purge_script
2. Unzip the Oracle Adaptive Access Manager archive and purge package Oracle scripts to the script directory.
3. Login to the database using the Oracle Adaptive Access Manager schema

   For example,

   ```
   sqlplus <OAAMADMIN>/<PASSWORD>
   ```

4. Run the purging execution scripts:

   ```
   SQL>@ exec_sp_purge_tracker_data.sql
   SQL>@ exec_sp_purge_txn_log.sql
   SQL>@ exec_sp_purge_workflow_data.sql
   SQL>@ exec_sp_purge_profile_data.sql
   SQL>@ exec_sp_purge_rule_log.sql
   ```

14.10.5.1.2 Automatic Scheduling Archive and purge jobs should be part of a routine schedule. These jobs can be scheduled using database jobs or OS-based scheduling utilities (crontab, at) or scheduler software (autosys, appworx).

It is recommended that these scripts are scheduled to run on regular intervals and only during off-peak hours.

14.10.5.2 SQL Server Database

The required scripts to execute archive and purge routines are listed below. For more information about these scripts, refer to Section 14.11.3, "Scripts to Execute Archive and Purge."

Archive and purge periods are set based on the business requirement specified for retention periods.

By default, the required scripts for archive and purge routines have the following two parameters set:

- p_days1 =no of days for data retention
- p_archived= Archived flag

To change these values per the business requirement, modify the following scripts:

- exec_sp_purge_tracker_data.sql
- exec_sp_purge_txn_log.sql
- exec_sp_purge_workflow_data.sql
- exec_sp_purge_profile_data.sql
- exec_sp_purge_rule_log.sql

14.10.5.2.1 Manual Execution To execute the scripts to archive and purge, follow the steps below:

1. Create the script directory, oaam_purge_script.
2. Unzip the Oracle Adaptive Access Manager archive and purge package SQL Server scripts to the script directory.
3. Login to the Oracle Adaptive Access Manager database using SQL Server Management Studio.
4. Open the script files listed below using File > Open > File. Then, navigate to the script directory.

```
exec_sp_purge_tracker_data.sql
exec_sp_purge_txn_log.sql
exec_sp_purge_workflow_data.sql
exec_sp_purge_profile_data.sql
exec_sp_purge_rule_log.sql
```

5. In the Query window, change the following line for every script:

```
USE [DATABASE_NAME] to USE < your OAAM Database>
```

6. Execute the scripts.
7. In the message window of the SQL Server Management Studio, save the results to a file.

14.10.5.2.2 Automatic Scheduling Archive and purge jobs should be part of a routine schedule. These jobs can be scheduled using database jobs or OS-based scheduling utilities (crontab, at) or scheduler software (autosys, appworx).

It is recommended that these scripts are scheduled to run on regular intervals and only during off-peak hours.

14.10.6 Validating Archive and Purge

To determine if the archive and purge was successful, check the log files (for example scheduler log, script output log, and others) for any errors. When the archive and purge process has completed, users can also query the transactional log and its related purged tables to validate that the data was archived and purged.

14.10.7 Restoring Archived Data

As recommended, users should take an export backup of archived tables after the archive process has completed in case they should need to perform troubleshooting in the future.

When performing a restoration, the user should restore the desired date's data to a temporary table using Oracle's database Import feature.

Please contact Oracle Support if any data restoration is required.

14.11 10.1.4.5.bp3 Archive and Purge Details

This section contains information about the tables and their corresponding archived tables and details on the setup scripts.

14.11.1 List of Tables and the Corresponding Archived Tables

Device fingerprint, Auto-learning transactional, transaction, and rule log tables and their corresponding tables are listed below.

14.11.1.1 Device Fingerprint Tables and Corresponding Archived Tables

Device Fingerprint Transaction Tables	Corresponding Archived Tables
VCRYPT_TRACKER_NODE	VCRYPT_TRACKER_NODE_PURGE
VCRYPT_TRACKER_NODE_HISTORY	VCRYPT_TRACKER_NODE_HISTORY_PURGE
VCRYPT_TRACKER_USERNODE_LOGS	VCRYPT_TRACKER_USERNODE_LOGS_PURGE
VT_DYN_ACT_EXEC_LOG	VT_DYN_ACT_EXEC_LOG_PURGE
VT_SESSION_ACTION_MAP	VT_SESSION_ACTION_MAP_PURGE
VT_USER_DEVICE_MAP	VT_USER_DEVICE_MAP_PURGE

14.11.1.2 Auto-learning Transactional Tables and Corresponding Archive Tables

Auto-learning Transactional Tables	Corresponding Archived Tables
VT_WF_DAYS	VT_WF_DAYS_PURGE
VT_WF_HOURS	VT_WF_HOURS_PURGE
VT_WF_MONTHS	VT_WF_MONTHS_PURGE

Auto-learning Transactional Tables	Corresponding Archived Tables
VT_WF_YEARS	VT_WF_YEARS_PURGE
V_FPRINTS	V_FPRINTS_PURGE
V_FP_MAP	V_FP_MAP_PURGE
VT_USER_PROFILE	VT_USER_PROFILE_PURGE
VT_DEVICE_PROFILE	VT_DEVICE_PROFILE_PURGE
VT_BASE_IP_PROFILE	VT_BASE_IP_PROFILE_PURGE
VT_IP_PROFILE	VT_IP_PROFILE_PURGE
VT_STATE_PROFILE	VT_STATE_PROFILE_PURGE
VT_CITY_PROFILE	VT_CITY_PROFILE_PURGE
VT_COUNTRY_PROFILE	VT_COUNTRY_PROFILE_PURGE

14.11.1.3 Transaction Tables and Corresponding Archived Tables

Transaction Tables	Corresponding Archived Tables
VT_ENTITY_ONE	VT_ENTITY_ONE_PURGE
VT_ENTITY_ONE_PROFILE	VT_ENTITY_ONE_PROFILE_PURGE
VT_USER_ENTITY1_MAP	VT_USER_ENTITY1_MAP_PURGE
VT_ENT_TRX_MAP	VT_ENT_TRX_MAP_PURGE
VT_TRX_DATA	VT_TRX_DATA_PURGE
VT_TRX_LOGS	VT_TRX_LOGS_PURGE

14.11.1.4 Rule Logs Tables and Corresponding Archived Tables

Rule Log Tables	Corresponding Archived Tables
VR_POLICYSET_LOGS	VR_POLICYSET_LOGS_PURGE
VR_RULE_LOGS	VR_RULE_LOGS_PURGE
VR_MODEL_LOGS	VR_MODEL_LOGS_PURGE
VR_POLICY_LOGS	VR_POLICY_LOGS_PURGE

14.11.2 Scripts to Set Up Archive and Purge

Archive and purge setup scripts for the Oracle and SQL server databases are listed below.

14.11.2.1 Scripts for the Oracle Database

The archive and purge setup scripts for the Oracle database are presented below.

14.11.2.1.1 create_purge_proc.sql The create_purge_proc.sql script creates the tables (Listed in Section 14.11.1, "List of Tables and the Corresponding Archived Tables") and the following stored procedures to archive and purge data from the transaction tables:

- SP_RULE_ PROC
- SP_MODEL_ PROC

- SP_POLICYSET_ PROC
- SP_POLICY_ PROC
- SP_NODE_HISTORY_ PROC
- SP_NODE_PROC
- SP_USER_NODE_PROC
- SP_USER_DVC_PROC
- SP_SESS_ACT_MAP_PROC
- SP_WF_YEARS_PROC
- SP_WF_MONTHS_PROC
- SP_WF_DAYS_PROC
- SP_WF_HOURS_PROC
- SP_V_FPRINTS_PROC
- SP_V_FP_MAP_PROC
- SP_VT_DY_ACT_EX_LOG_PRO
- SP_VT_TRX_LOGS_PROC
- SP_VT_TRX_DATA_PROC
- SP_VT_ENT_TRX_MAP_PROC
- SP_VT_ENT_ONE_PRF_PROC
- SP_VT_ENT_ONE_PROC
- SP_VT_ENT_ONE_MAP_PROC
- SP_VT_USER_PRF_PROC
- SP_VT_DEVICE_PRF_PROC
- SP_VT_IP_PRF_PROC
- SP_VT_BASE_IP_PRF_PROC
- SP_VT_CITY_PRF_PROC
- SP_VT_COUNTRY_PRF_PROC
- SP_VT_STATE_PRF_PROC

14.11.2.2 Scripts for the SQL Server Database

The archive and purge setup scripts for the SQL server database are presented below.

14.11.2.2.1 cr_vcrypt_purge_tables.sql The cr_vcrypt_purge_tables.sql script creates the tables (Section 14.11.1, "List of Tables and the Corresponding Archived Tables") to archive and purge data from the transaction tables.

14.11.2.2.2 cr_sp_arch_purge_tracker_data.sql The cr_vcrypt_purge_tables.sql script creates the stored procedure sp_archive_purge_tracker_data to archive and purge data from device fingerprinting transaction tables.

14.11.2.2.3 cr_sp_arch_purge_txn_logs.sql The cr_vcrypt_purge_tables.sql script creates the stored procedure sp_archive_purge_txn_logs_data to archive and purge data from in-session transaction tables.

14.11.2.2.4 cr_sp_arch_purge_workflow_data.sql The cr_vcrypt_purge_tables.sql script creates the stored procedure sp_archive_purge_wf_data to archive and purge data from work flow transaction tables.

14.11.2.2.5 cr_sp_arch_purge_profile_data.sql The cr_vcrypt_purge_tables.sql script stored procedure sp_archive_purge_profile_data to archive and purge data from Auto-learning profile transaction tables.

14.11.2.2.6 cr_sp_arch_purge_rules_log.sql The cr_vcrypt_purge_tables.sql script creates the stored procedure sp_archive_purge_rule_log to archive and purge data from rule logs transaction tables.

14.11.3 Scripts to Execute Archive and Purge

The scripts to execute the archive and purge process are documented below.

14.11.3.1 exec_sp_purge_tracker_data.sql

This script calls stored procedures to archive and purge data from device fingerprinting tables. By running this script, the following tables will be archived and purged:

- VCRYPT_TRACKER_NODE
- VCRYPT_TRACKER_NODE_HISTORY
- VCRYPT_TRACKER_USERNODE_LOGS
- VT_USER_DEVICE_MAP
- VT_DYN_ACT_EXEC_LOG
- VT_SESSION_ACTION_MAP

Note: The VT_SESSION_ACTION_MAP table is not purged using the partition drop maintenance script. This table stores the device fingerprinting session information; therefore the purging of this table is performed using the manual purge stored procedure (SP_SESS_ACT_MAP_PROC) which is called by the exec_sp_purge_tracker_data.sql script.

14.11.3.2 exec_sp_purge_txn_log.sql

This script calls stored procedures to archive and purge data from in-session transaction tables. By running this script, the following tables will be archived and purged:

- VT_ENTITY_ONE
- VT_ENTITY_ONE_PROFILE
- VT_ENT_TRX_MAP
- VT_TRX_DATA
- VT_TRX_LOGS
- VT_USER_ENTITY1_MAP

14.11.3.3 exec_sp_purge_workflow_data.sql

This script calls stored procedures to archive and purge data from the Workflow Auto-learning tables. By running this script, the following tables will be archived and purged:

- VT_WF_DAYS
- VT_WF_HOURS
- VT_WF_MONTHS
- VT_WF_YEARS
- V_FPRINTS
- V_FP_MAP

14.11.3.4 exec_sp_purge_profile_data.sql

This script calls stored procedures to archive and purge data from the Auto-learning profile tables. By running this script, the following tables will be archived and purged:

- VT_BASE_IP_PROFILE
- VT _IP_PROFILE
- VT_DEVICE_PROFILE
- VT_COUNTRY_PROFILE
- VT_CITY_PROFILE
- VT_STATE_PROFILE
- VT_USER_PROFILE

14.11.3.5 exec_sp_purge_rule_log.sql

This script calls stored procedures to archive and purge data from the Rules Engine logging tables. By running this script, the following tables will be archived and purged:

- VR_POLICYSET_LOGS
- VR_RULE_LOGS
- VR_MODEL_LOGS
- VR_POLICY_LOGS

14.11.4 Drop Scripts for Partitioned Tables

Two scripts to drop partitions are listed below.

14.11.4.1 Drop_Monthly_Partition_tables.sql

Use this script to drop partitions for tables with the monthly frequency. Run this script at the end of each month to drop partitions that are older than sixth months as per the Oracle Adaptive Access Manager application requirement. Eventually, these tables will have six partitions at any point.

14.11.4.2 Drop_Weekly_Partition_tables.sql

Use this script to drop partitions for tables with the weekly frequency. Run this script at the end of every two weeks, starting from your database creation date, to drop

partitions older than two weeks as per the Oracle Adaptive Access Manager application requirement.

14.12 Upgrading the Database from 10.1.4.5.bp2 to 10.1.4.5.bp5

This section provides information about the setup and execution of the database patch to reduce the column size in the OAAM database.

Note: Before you start the upgrade process, it is strongly recommended that you perform a full database backup.

14.12.1 Database Pre-requisite

The prerequisites for applying the database patch are:

1. This patch should be applied where the Oracle Adaptive Access Manager 10.1.4.5.bp2 database patch is already installed.
2. Ensure that the database server is not connected to the application server(s).

14.12.2 Database Patch Details

Patch details are listed below for the Oracle Database and MS SQL Server.

The list of objects impacted is provided in 10.1.4.5.bp5 Database Patch Details.

14.12.2.1 Oracle

This patch includes the oaam_db_patch_oracle_10_1_4_5_05.sql script for the Oracle database that will drop the not null constraint for the REF_ID, REF_TYPE from the VR_DYN_ACTION_INST_HIST, VR_DYN_ACTION_INST tables.

14.12.2.2 Microsoft SQL Server

This patch includes two scripts for the Microsoft SQL Server to reduce column size. They are listed below. These scripts will create and run the stored procedure, sp_oaam_changecolumnsize, to change the column size for the OAAM tables to fix the "index data length exceeding 900 byte" exception.

- cr_sp_OAAM_ChangeColumnsize.sql
- exec_sp_OAAM_ChangeColumnsize.sql

14.12.3 Database Patch Installation Instructions

Installation instructions for Oracle and the MS SQL Server are listed below.

For Oracle

To apply the OAAM database patch:

1. Create the patch directory, oaam_db_patch_oracle_10.1.4.5_05.
2. Copy oaam_db_patch_oracle_10_1_4_5_05.sql from the oaam_db\db_patches\bp05\oracle-script directory to your patch directory.
3. Log in to the database using the Oracle Adaptive Access Manager schema username and password.

   For example:

```
sqlplus <OAAM>/<PASSWORD>
```

4. Run oaam_db_patch_oracle_10_1_4_5_05.sql.

   For example:

   ```
   SQL > @ oaam_db_patch_oracle_10_1_4_5_05.sql
   ```

5. Check oaam_db_patch_oracle_10_1_4_5_05.sql.log for any error. Please contact Oracle Support if you experience any ORA- errors in the log.

Note: Ignore the ORA-01451, ORA-01418, and ORA-01408 errors.

For Microsoft SQL Server

To apply the database patch for an Oracle Adaptive Access Manager database on a Microsoft SQL Server:

1. Create a patch directory, oaam_db_patch_mssql_10.1.4.5_bp05.
2. Copy all the scripts from the extracted zip to your patch directory.

   For non-Unicode, the scripts are in the oaam_db\db_patches\bp05\msql_db_nonunicode directory.

   For unicode, the scripts are in the oaam_db\db_patches\bp05\msql_db_unicode directory.
3. Log in to the OAAM database using Microsoft SQL Server Management Studio.
4. For a non- Unicode database:
   a. For a non-Unicode database, open the patch file from the msql_db_nonunicode directory using File > Open >File, and then navigate to the patch directory.
   b. In the Query window, please follow these instructions:

      Change USE [DATABASE_NAME] to USE < your OAAM Database>.

      Select cr_sp_OAAM_ChangeColumnsize.sql and Execute.

      Select exec_sp_OAAM_ChangeColumnsize.sql and Execute.
5. For a Unicode database:
   a. For a Unicode database, open the patch file from the msql_db_Unicode directory using File > Open > File, and then navigate to the patch directory.
   b. In the Query window, please follow these instructions:

      Change USE [DATABASE_NAME] to USE < your OAAM Database>.

      Select cr_sp_OAAM_ChangeColumnsize.sql and Execute.

      Select exec_sp_OAAM_ChangeColumnsize.sql and Execute.

14.12.4 Validation

To validate that the scripts are successfully executed, please check the output from SQL Server Management Studio.

14.12.5 Server Restart

After the upgrade process, restart the application server.

You will not have to restart the database server.

14.13 10.1.4.5.bp5 Database Patch Details

The Oracle and MS SQL Server objects that will be altered are listed below.

14.13.1 Oracle

The Oracle objects that will be altered are:

- VR_DYN_ACTION_INST_HIST.REF_TYPE
- VR_DYN_ACTION_INST_HIST.REF_ID
- VR_DYN_ACTION_INST.REF_TYPE
- VR_DYN_ACTION_INST.REF_ID

14.13.2 MS SQL Server

The MS SQL Server objects that will be altered are:

- §V_B_ENUM, PROP_NAME
- §V_B_ENUM_ELMNT, PROP_NAME
- §V_FPRINTS, HASH_VALUE
- §V_LOCK, LOCK_NAME
- §V_PAT_ENT_OPER, LABEL
- §V_PATTERN, LABEL
- §VCRYPT_ACCOUNTS, ACCT_NAME
- §VCRYPT_ISP, ISP_NAME
- §VCRYPT_PROFILE, PROFILE_NAME
- §VCRYPT_RULE, RULE_NAME
- §VCRYPT_STRING_VALUE_ELEMENT, ELEMENT_VALUE
- §VCRYPT_TRACKER_USERNODE_LOGS, EXT_SESSION_ID
- §VCRYPT_USER_GROUPS, GROUP_NAME
- §VCRYPT_USER_ROLES, ROLE_NAME
- §VCRYPT_VALUE_LIST, LIST_NAME
- §VR_DYN_ACTION, ACTION_NAME
- §VR_OVERRIDE, OBJECT_VALUE
- §VR_RULE_CONDN, CONDN_NAME
- §VS_TASK, TASK_NAME
- §VS_TASK_GRP, GRP_NAME
- §VT_ENTITY_DEF, LABEL
- §VT_ENTITY_ONE, ENTITY_KEY
- §VT_IP_CLUSTER, LABEL
- §VT_IP_CLUSTER_GROUP, LABEL

- §VT_TRX_DATA, DATA1
- §VT_TRX_DATA, DATA2
- §VT_TRX_DATA, DATA3
- §VT_TRX_DEF, LABEL
- §VT_TRX_DEF, TRX_DEF_KEY
- §VT_TRX_INPUT_DEF, LABEL
- §VT_TRX_INPUT_DEF, TRX_DEF_KEY
- §VT_USER_SESS, EXT_SESSION_ID
- §V_B_ENUM_HIST, LABEL
- §V_B_ENUM_HIST, PROP_NAME
- §V_B_ENUM_ELMNT_HIST, PROP_NAME
- §V_PAT_ENT_OPER_HIST, LABEL
- §V_PATTERN_HIST, LABEL
- §VCRYPT_ACCOUNTS_HIST, ACCT_NAME
- §VCRYPT_ISP_HIST, ISP_NAME
- §VCRYPT_PROFILE_HIST, PROFILE_NAME
- §VCRYPT_RULE_HIST, RULE_NAME
- §VCRYPT_USER_GROUPS_HIST, GROUP_NAME
- §VCRYPT_USER_ROLES_HIST, ROLE_NAME
- §VCRYPT_VALUE_LIST_HIST, LIST_NAME
- §VR_DYN_ACTION_HIST, ACTION_NAME
- §VR_OVERRIDE_HIST, OBJECT_VALUE
- §VR_RULE_CONDN_HIST, CONDN_NAME
- §VS_TASK_HIST, TASK_NAME
- §VS_TASK_GRP_HIST, GRP_NAME
- §VT_ENTITY_DEF_HIST, LABEL
- §VT_TRX_DEF_HIST, LABEL
- §VT_TRX_DEF_HIST, TRX_DEF_KEY
- §VT_TRX_INPUT_DEF_HIST, LABEL
- §VT_TRX_INPUT_DEF_HIST, TRX_DEF_KEY

14.14 Upgrading the Database from 10.1.4.5.bp5 to 10.1.4.5.bp6

This section provides information about the setup and execution of the database patch to create additional indexes to improve system performance.

Note: Before you start the upgrade process, it is strongly recommended that you perform a full database backup.

14.14.1 Database Pre-requisite

The prerequisites for applying the database patch are:

1. This patch must be applied where the Oracle Adaptive Access Manager 10.1.4.5.bp02 and higher is already installed.
2. The database server is not connected to the application server(s).

14.14.2 Database Patch Details

Patch details are listed below for the Oracle Database and MS SQL Server.

This patch includes a script that will create a few additional indexes for system performance. This patch will also remove unique key constraint from the V_B_ENUM table.

14.14.3 Objects Impacted

The following objects will be altered when the patch is applied.

Index Created

- VT_TRACKER_USERNODE_LOGS_IDX14 ON VCRYPT_TRACKER_ USERNODE_LOGS("USER_LOGIN_ID")
- V_CASE_HIST_IDX1 ON V_CASE_HIST("CASE_ID","TO_TIME")
- V_CASE_IDX2 ON V_CASE("CASE_TYPE")

14.14.4 Database Patch Installation Instructions

Installation instructions for Oracle and the MS SQL Server are listed below.

For Oracle

To apply the OAAM database patch:

1. Create the patch directory, oaam_db_patch_oracle_10.1.4.5_06.
2. Copy oaam_db_patch_oracle_10_1_4_5_06.sql from the extracted zip to your patch directory.
3. Log in to the database using the Oracle Adaptive Access Manager schema username and password.

   For example:

   ```
   sqlplus <OAAM>/<PASSWORD>
   ```

4. Run oaam_db_patch_oracle_10_1_4_5_06.sql.

   For example:

   ```
   SQL > @ oaam_db_patch_oracle_10_1_4_5_06.sql
   ```

5. Check oaam_db_patch_oracle_10_1_4_5_06.sql.log for any error. Please contact Oracle Support if you experience any ORA- errors in the log.

Note: Ignore the ORA-01451, ORA-01418, and ORA-01408 errors.

For Microsoft SQL Server

To apply the database patch for an Oracle Adaptive Access Manager database on a Microsoft SQL Server:

1. Create a patch directory, oaam_db_patch_mssql_10.1.4.5_bp06.
2. Copy all the scripts from the extracted zip to your patch directory.
3. Log in to the OAAM database using Microsoft SQL Server Management Studio.
4. Open the patch file from the Microsoft SQL directory using File > Open >File, and then navigate to the patch directory.
5. In the Query window, please follow these instructions:
   a. Change USE [DATABASE_NAME] to USE < your OAAM Database>.
   b. Select oaam_db_patch_mssql_10_1_4_5_06.sql and execute.

14.14.5 Validation

To validate that the scripts are successfully executed, please check the output from SQL Server Management Studio.

14.14.6 Server Restart

After the upgrade process, restart the application server.

You will not have to restart the database server.

14.15 Documentation Corrections

This section contains last minute information not included in the Oracle Adaptive Access Manager Release 10g (10.1.4.5) documentation library:

14.15.1 Configuration to Log Rule Executions Based on Total Rule Processing Time Taken

Rule execution logs are not configurable and therefore may affect Adaptive Risk Manager performance. Users who experience large numbers of log ins per day will have many rows of data written in the logs.

Configurable parameters are provided to address this issue. Users can now configure "n," a numeric property for time, so that logging is performed only if the total time taken for the Runtime is greater than "n" milliseconds. The parameter can be configured globally or for a specific runtime.

For example, the properties, as set below, logs for all Runtime process rules, only if the total time taken is more than 1000 ms.

```
vcrypt.tracker.rules.trace.policySet=false
vcrypt.tracker.rules.trace.policySet.min.ms=1000
```

14.15.2 Pattern Member Condition Does Not Take into Account the Bucket

When an Entity: Pattern Membership rule condition is evaluated, it does not take into account the current bucket that the pattern authentication operation belongs to.

To resolve this issue, the "ENTITY: Entity is member of bucket N times in a given time period" condition has been created.

Condition	ENTITY: Entity is member of bucket N times in a given time period
Description	Condition to check if this Entity is a member of the bucket a number of times in a given time period. This condition can be used to check the current behavior against the pattern. Please note that this is a count-based condition. So, if you configure to trigger it, for example, for a count less than three, it will trigger on the first login that matches the fingerprint.
Pre-Requisites	Ensure that the following pre-requisites are met: ■ 10.1.4.5.bp2 or later must be installed. ■ Entities and patterns must be defined before adding this condition to rules/ policys.
Assumptions	Auto-Learning is enabled.
Available since version	10.1.4.5.bp2
Checkpoints	All checkpoints see the note for pre-auth though.

14.15.3 Randomize KBA Questions

The oaam.kba.questions.randomorder property has been added for presenting KBA questions in random order instead of sequentially. Randomization will be performed Online only (Adaptive Strong Authenticator) if the oaam.kba.questions.randomorder property is missing or is set to true. For the CSR Get Challenge Question flow, question access will always be sequential.

14.15.4 No Rule Logs Shown in Offline Application

The following properties in tracker.properties can be used to enable the rule log using fingerprint:

```
# Int property determining finger print logging or detailed logging. Detailed
logging if exceeds this. Inclusive
vcrypt.tracker.rulelog.exectime.maxlimit=-1
# Boolean property to do both fingerprint and detailed logging. Overrides
vcrypt.tracker.rulelog.exectime.maxlimit.
vcrypt.tracker.rulelog.logBoth=false
```

14.15.5 Slider in OAAM 10.1.4.5 bpX

The slider is now available for 10.1.4.5.bp6. Users will have to look at the reference/sample class BharosaHelper and use the new methods.

Note: The names of the new methods in the reference class, BharosaHelper.java, are listed as follows:

- public int validateSlider(BharosaSession bharosaSession, HttpServletRequest request)
- public void sliderOptIn(BharosaSession bharosaSession, String newPin)
- public void sliderOptOut(BharosaSession bharosaSession)
- public String getSliderHTML(BharosaSession bharosaSession)
- public static String getSliderTutorialHTML()
- public String getUserPinStatus(BharosaSession bharosaSession)

- public boolean isPinEnabled(BharosaSession bharosaSession)
- public void registerDevice(BharosaSession bharosaSession, String regDeviceStr)

14.15.6 Session: Time Unit Condition

The "Session: Time Unit" condition is described below.

Condition	Day of the Week
Description	The condition determines if a particular time unit (in the current time) is in a particular position in the time unit. This condition uses the request date if available to evaluate the date function requested with the use of parameters. If the request date is not available, then the current server date time will be used.
Example	This condition can determine if the day of the week is equal to (or not equal to or other comparison operators) Monday or Tuesday and so on. It can also determine if the day of the month matches a certain criterion of the day of the month. It can also try to match the same criterion if the month of the year is <value> or not <value> or in or not in <value>.

Parameters

Parameters	Description	Possible Values
Time Unit	Enum What is the time unit you are looking for? The default value is Day of the Week	Possible values are: ■ Day of the Week ■ Day of the Month ■ Day of the Year ■ Month of the Year ■ Hour of the Day ■ Week of the Month ■ Week of the Year ■ Year
Comparison operator	Enum What comparison you want to make with the time unit. The default value = Equal To	Possible values are: ■ Equal To ■ Not Equal To ■ Less Than ■ More Than ■ Less than Equal to ■ More than Equal to ■ IN ■ not IN

Parameters	Description	Possible Values
Comparison value	String The default value = "" (empty string), that represents integer or string that represents comma separated integers. Example: "1" or "1,2,3,4". The user can use comma-separated values when using the IN or NOT in operator. If comma-separated values are used for any other operators, it will be determined as an error and the value of the #5 parameter below will be returned. If the string does not represent a number (or a list of comma separated numbers) then it is determined as an error and a value of parameter #5 will be returned.	Correct values of this parameter for different time units. ■ Day of the Week: 1 through 7 (1 = Monday). ■ Day of the Month: 1 through 31 ■ Day of the Year: 1 through 366 ■ Month of the Year: 0 through 11 (0 = January) ■ Hour of the Day: 0 through 23 ■ Week of the Month: 0 through 6 ■ Week of the Year 1 through 53 ■ Year: positive integer
IS Condition True	Boolean Default value = true This will the return a value if the comparison is true.	
Error Return value	Boolean Default value = false If the user has configured the value of the comparison value (#3) above incorrectly, or if there is any other error determining the date or <some value> then this value will be returned. Example: To configure the day of the week as a weekday, we will use the following values: Time Unit = Day of the Week Comparison Operator = "IN" Comparison Value = "1,2,3,4,5" Is Condition True = "true" Error Return value = "false"	

14.15.7 Using Time Extraction Scheme for Time Portion

This section describes how to check transaction aggregate/count that includes filter criteria involving the time portion of date.

14.15.7.1 Use Cases that require using "Time Extraction"

It is recommended to use the "Time Extraction" mapping scheme if the following kind of rules have to be specified:

- Check if there are "n" or more number of transactions by the same user between 9am and 5am regardless of the date
- Check if there are "n" or more number of transactions and the sum of the amount of those greater than "x" amount that happened between 2am and 5am regardless of the date

14.15.7.2 During Transaction Definition Phase

The Transaction Definition Phrase is described below.

- If time portion of **transaction timestamp** has to be considered in the filter criteria, then add a **source field** in the transaction definition with the **internal Id** as **oaam.transaction.datetime**. Make sure internal Id is exactly the same without any spaces. The name and description of that source field can be, for example, like "Transaction Timestamp". In this case the client application does not need to populate this source field, it will be implicitly available.
  - If time has to be extracted from some other source field other than the transaction timestamp, make sure the source field is a date time field and the client application sends a valid date time value in the format: **yyyy-MM-dd'T'HH:mm:ss.SSSz**
- Add a numeric field to either "Transaction Data" or "Entity" that can store the time value. The time value is stored in the precision of milliseconds. The formula used to derive the time value is:
  - Timevalue = hour * 10000000 + minute * 100000 + seconds * 1000 + milliSeconds;
- Now both the source field and destination field are set up. Go to 'Data Mapping' or 'Entity Mapping' based on whether the destination field is "Transaction Data" or "Entity Data". There, select the destination field as the time field and map it to the source date-time field using the "Extract Time" mapping scheme available in the list of mappings.
- Once the transaction definition is completed and activated, the time value will be populated in the time field column whenever transaction data is created. You can verify the value of the time field using the formula specified in the previous step.

14.15.7.3 Using the time field in transaction rules

The time field usage in transaction rules is described below.

- The time field can be used like a numeric field in the transaction rules. You can specify filter conditions that use operators like "greater than", "less than", and others.
- You can specify the value to be compared in any of the following formats:
  - HH24:MM:SS:MS (Most recommended if milliseconds precision is required)
  - HH24:MM:SS
  - HH24:MM
- Apart from specifying the value in the above format there are no special steps for using it in the transaction rules

14.15.7.4 Limitations of time extraction and usage in transaction rules

Limitations of time extraction and usage in transaction rules are listed as follows:

- Time value is stored in a 24-hour format and is not stored along with date. Because of this, filter expressions that involve time spread across different dates can be specified. For example, a filter expression like "greater than 23:00:00:000 and less than 5:00:00:000" is not valid.
- Since time value is stored at the precision of milli-seconds, it is recommended not to use a time field with "equals" and "not-equals" operators in the filter expression of the transaction rules. If it is absolutely necessary, be aware that the application

will check for the "exact" time value (including milliseconds), so make sure the proper value is specified in the filter expression.

- Currently the user interface will display the numeric value of the time field without any formatting while displaying the transaction details.

15

Oracle Role Manager

This chapter introduces Oracle Role Manager Release Notes, 10g (10.1.4.2). It includes the following topics:

15.1 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/`

15.2 What's New in Oracle Role Manager

The following sections discuss what's new in Oracle Role Manager release 10.1.4.2:

15.2.1 New Component Support

This section discusses the following new certifications:

Note: For a complete list of certified components, visit the official platform certification Web site at:

http://www.oracle.com/wocportal/page/wocprod/ver-DRAFT/ocom/technology/software/products/ias/files/idm_certification_101401.html

15.2.1.1 Operating System Requirements

Oracle Role Manager is now certified to run on the following operating systems:

- Oracle Enterprise Linux 4 (64-bit)
- Oracle Enterprise Linux 5 (64-bit)
- Microsoft Windows 2008 (64-bit)
- Microsoft Windows 2008 (32-bit and 64-bit)
- Red Hat Enterprise Linux AS Release 4 (64-bit)
- Red Hat Enterprise Linux AS Release 5 (64-bit)
- SUSE 10 (32 bit)
- Solaris 10 (64 bit)

15.2.1.2 Application Servers

Oracle Role Manager and Oracle Role Manager Integration Library are now certified to run in clustered environments with JBoss and IBM WebSphere.

15.2.1.3 Oracle Role Manager Integration Library Certification

Oracle Role Manager Integration Library is supported only with Oracle Identity Manager 9.1.0.2. For more information, see *Oracle Role Manager Integration Guide.*

15.2.2 New Features and Enhancements

This section discusses the following new features and enhancements:

- Usability
- Installation
- Integration Library
- Upgrade

15.2.2.1 Usability

This release includes many usability enhancements to the Oracle Role Manager user interface for an improved end-user experience. These include the following:

- Audit history details now display workflow events as well as dynamic role membership audit events.
- The Outbox now displays workflow events.
- The system now detects whether the Integration Library is installed and the user experience is affected as follows:

- Entitlement data from Oracle Identity Manager now displays if the Integration Library is installed. If the Integration Library is not installed, no entitlement data from Oracle Identity Manager is displayed.
- Person fields and entitlement fields display as read-only if the Integration Library is installed, so that Oracle Identity Manager remains the system of record for person and entitlement data. If the Integration Library is not installed, person fields and entitlement fields are editable fields.

15.2.2.2 Installation

The Oracle Role Manager installation now includes the Oracle Role Manager Integration Library software for easier deployments. In addition, for deployments of the Integration Library on Oracle WebLogic Server, a new tool is provided in this release for facilitate easier configuration.

15.2.2.3 Integration Library

The Integration Library has been enhanced with new functionality supporting role grant approval workflow and reconciliation of entitlements and IT Roles (as access policies in Oracle Identity Manager). Additionally, there are now new scheduled tasks for one-time import of entitlements, user groups, and access policies. See *Oracle Role Manager Integration Guide* for details.

15.2.2.4 Upgrade

This release now supports upgrade from Oracle Role Manager 10.1.4.1 and Oracle Role Manager 10.1.4.1.1.

15.2.3 Application Data Model Changes

This release contains changes to the application data model as described in the following table.

Table 15–1 Application Data Model Changes

Model	Description of Change
primordial.xml	The `auditStatus` domain definition has three new enum constraint values: `submitted`, `approved`, and `rejected`.
	The `approverType` domain definition has been added and is an attribute in the `businessRole` structural type definition.
	The `email` domain definition has been moved from `abstractIdentity` to `person` in the standard model.
	The word "privilege" in all titles and messages, when referring to IT privileges, has been changed to "entitlement."
standard.xml	The `email` definition is now an attribute on the `person` type and the `pattern` constraint has been removed.
	The `oimEntitlementId` domain definition has been added and is an attribute in the `itPrivilege` structural type definition.
	The `resourceName` domain definition has been added and is an attribute in the `itPrivilege` structural type definition.

Table 15–1 (Cont.) Application Data Model Changes

Model	Description of Change
	A new reference attribute (relationship path) that relates approver to approver business roles has been added to the `businessRole` structural type definition.
oim_integration.xml	The `oimUserGroupId` domain definition integer scale value has changed from 10 to 19 and has been added as an attribute to `itRole` and `businessRole` structural type definitions with a uniqueness constraint. The `oimAccessPolicyId` domain definition integer scale value has changed from 10 to 19. The `oimManagerKey` domain definition has been removed. A uniqueness constraint has been added to the `oimAccessPolicyId` attribute in the `itRole` structural type definition.

15.2.4 Java API Changes

This section discusses the following changes to the Oracle Role Manager Java API related to the new features and enhancements for this release:

- Classes
- Methods

15.2.4.1 Classes

No public classes have been added in this release.

15.2.4.2 Methods

The methods listed in this section have been added to the classes specified below. See *Oracle Role Manager Java API Reference* for full descriptions of each method.

Table 15–2 New Methods

Containing Class	Method
oracle.iam.rm.client.BusinessTransactionOperation	invoke
oracle.iam.rm.inherent.role.RoleManager	findMappedITPrivileges
oracle.iam.rm.server_api.Server	hasHierarchyChildren
oracle.iam.rm.server_api.ServerOperation	isApprovalRequired

15.3 Certified Components

This section identifies components certified with Oracle Role Manager release 10.1.4.2 and contains the following topics:

- Operating Systems
- Application Servers
- Databases
- Certified JDKs
- Supported Configurations

- Certified Single Sign-On Components
- Languages
- Web Browsers

15.3.1 Operating Systems

Oracle Role Manager release 10.1.4.2 is certified for the following operating systems:

- Microsoft Windows Server 2003 Standard Edition with SP1 (32-bit and 64-bit)
- Microsoft Windows 2008 (32-bit and 64-bit)
- Oracle Enterprise Linux 4 (32-bit and 64-bit)
- Oracle Enterprise Linux 5 (32-bit and 64-bit)
- Red Hat Enterprise Linux AS Release 4 (32-bit and 64-bit)
- Red Hat Enterprise Linux AS Release 5 (32-bit and 64-bit)
- SUSE 10 (32 bit)
- Solaris 10 (64 bit)

15.3.2 Application Servers

Oracle Role Manager release 10.1.4.2 is certified for the following application servers:

- WebLogic Server 10.3 (on clustered and nonclustered environments)
- IBM WebSphere Application Server 6.1.0.21 (on clustered and nonclustered environments)
- JBoss Application Server 4.2.3 (on clustered and nonclustered environments)

15.3.3 Databases

Oracle Role Manager release 10.1.4.2 is certified for the following databases:

- Oracle Database Deployment
  - Oracle Database 10*g* Enterprise Edition release 10.2.0.4 to 10.2.*x*
  - Oracle Database 10*g* Standard Edition release 10.2.0.4 to 10.2.*x*
  - Oracle Database 11*g* Standard Edition release 11.1.0.6 to 11.1.0.*x*
  - Oracle Database 11*g* Enterprise Edition release 11.1.0.6 to 11.1.0.*x*
- Oracle RAC Deployment (general purpose operation)
  - Oracle Database 10*g* Enterprise Edition release 10.2.0.4 to 10.2.*x*
  - Oracle Database 11*g* Enterprise Edition release 11.1.0.6 to 11.1.0.*x*

15.3.4 Certified JDKs

For each certified application server, Oracle Role Manager release 10.1.4.2 is certified for the JDKs listed in Table 15–3.

Table 15–3 Certified JDKs

Application Server	Certified JDK
Oracle WebLogic Server	Oracle JRockit 6.0 (R27.6.0-50) **Note:** For 64-bit systems, the JDK must be the 64-bit version of JRockit, not the version that is installed with WebLogic Server. For information about installing the 64-bit JDK, refer to *WebLogic Server 10.3 Installation Guide*.
IBM WebSphere Application Server	IBM JDK 1.5
JBoss Application Server	Sun Java 2 JDK 1.6

15.3.5 Supported Configurations

Oracle Role Manager release 10.1.4.2 supports the configurations listed in Table 15–4.

Table 15–4 Supported Configurations

Operating System	Hardware	Application Server	Database
Oracle Enterprise Linux 4 and 5 (32-bit)	Intel x86	WebLogic 10.3	Oracle Database (see Section 15.3.3)
		JBoss 4.2.3	Oracle Database (see Section 15.3.3)
		WebSphere 6.1.0.21	Oracle Database (see Section 15.3.3)
Oracle Enterprise Linux 4 and 5 (64-bit)	Intel EM64T or AMD64	WebLogic 10.3	Oracle Database (see Section 15.3.3)
		JBoss 4.2.3	Oracle Database (see Section 15.3.3)
		WebSphere 6.1.0.21	Oracle Database (see Section 15.3.3)
RedHat AS ES4 and ES5 (32-bit)	Intel x86	WebLogic 10.3	Oracle Database (see Section 15.3.3)
		JBoss 4.2.3	Oracle Database (see Section 15.3.3)
		WebSphere 6.1.0.21	Oracle Database (see Section 15.3.3)
RedHat AS ES4 and ES5 (64-bit)	Intel EM64T or AMD64	WebLogic 10.3	Oracle Database (see Section 15.3.3)
		JBoss 4.2.3	Oracle Database (see Section 15.3.3)
		WebSphere 6.1.0.21	Oracle Database (see Section 15.3.3)
Windows Server 2003 SP1 or Windows 2008 (32-bit)	Intel x86	WebLogic 10.3	Oracle Database (see Section 15.3.3)
		JBoss 4.2.3	Oracle Database (see Section 15.3.3)

Table 15–4 (Cont.) Supported Configurations

Operating System	Hardware	Application Server	Database
		WebSphere 6.1.0.21	Oracle Database (see Section 15.3.3)
Windows Server 2003 SP1 or Windows 2008 (64-bit)	Intel EM64T or AMD64	WebLogic 10.3	Oracle Database (see Section 15.3.3)
		JBoss 4.2.3	Oracle Database (see Section 15.3.3)
		WebSphere 6.1.0.21	Oracle Database (see Section 15.3.3)
Windows XP Professional SP2 (32-bit development environments only)	Intel x86	WebLogic 10.3	Oracle Database (see Section 15.3.3)
		JBoss 4.2.3	Oracle Database (see Section 15.3.3)
		WebSphere 6.1.0.21	Oracle Database (see Section 15.3.3)

15.3.6 Certified Single Sign-On Components

Oracle Role Manager release 10.1.4.2 is certified for Single Sign-On with the following component:

- Oracle Access Manager 10.1.4.0.1 (formerly known as Oracle COREid) using both ASCII and non-ASCII character logins.

> **Note:** Single Sign-On with Oracle Access Manager 10.1.4.0.1 for non-ASCII character logins requires an Oracle Access Manager patch.

15.3.7 Languages

Oracle Role Manager release 10.1.4.2 is certified for the following language:

- English (en_US locale only)

15.3.8 Web Browsers

Oracle Role Manager release 10.1.4.2 is certified for the following Web browsers:

- Microsoft Internet Explorer 6.0 (SP2)
- Microsoft Internet Explorer 7.0

15.4 Fixes in This Release

Oracle Role Manager release 10.1.4.2 resolves the known bugs from previous releases listed in the following table.

Table 15–5 Bugs Resolved by 10.1.4.2

Bug #	Description
6949154	Auditing: Dynamic membership updates are not audited. Changes to a user's memberships based on dynamic roles (resolved by membership rules or grant policies) are not stored with audit data.
6949255	System Messages: System should provide useful warning for syntactically incorrect XML rule. The system does not issue a user-friendly message if a syntactically incorrect membership rule is given in the role grant policy or membership rule. Instead, a generic "setMembershipRule failed" error displays.
7043245	Integration Library: Exception in Oracle Identity Manager server console when creating user. The message can be ignored. User creation is successful, both in Oracle Identity Manager and in Oracle Role Manager
7529678	Search: SELECT query returns deleted objects. A SELECT query run on the database using the Oracle Role Manager tjdbc driver returns deleted objects. This can affect reports but has no affect on the Oracle Role Manager user interface.
7718897	Server: CSV file parsing errors during data load. The strings defined as field delimiters in the load script for different object types are inconsistent. All objects types use the carat (^) as a delimiter except `organization` object types, which are set to use the single quote (’). This can result in CSV file parsing errors.
8226900	Integration Library: Exception "ERROR [ACCOUNTMANAGEMENT] Class/Method: Authenticate/connect encounter some problems" intermittently displays in Oracle Identity Manager application server console on JBoss. This message is harmless and can be ignored.
8235658	Integration Library: Deploying on UNIX-based systems requires renaming of directory to ensure successful role reconciliation. Role reconciliation fails on case-sensitive UNIX-based systems because the message from Integration Library is looking for the pluginConfigDir directory instead of the pluginConfigdir directory (note the lowercase *d*).

15.5 Known Problems

This section describes known problems for Oracle Role Manager release 10.1.4.*x*. If a suitable workaround exists for a known problem, it is listed with the description of the bug to provide a temporary solution.

This section contains the following topics:

15.5.1 Auditing

This section describes known bugs related to the auditing component and contains the following topics:

15.5.1.1 Some audit messages unclear or inaccurate

Some audit and validation messages displayed to the end user are unclear or contain incorrect references.

15.5.1.2 System displays misleading information for create transactions

System displays the transaction as an update action in the Outbox even when the user has performed a create transaction.

15.5.1.3 Duplicate audit messages are displayed in the transaction details

If a user updates any attribute and navigates to any other tab before clicking the Submit button, duplicate entries are displayed in the transaction details in the Outbox.

15.5.2 General Usability

This section describes general user interface bugs and contains the following topics.

15.5.2.1 User has no indication why the Delete option is disabled for organizations with child entities

The relationship between organization type objects and their child entities (other organization types, roles, and people) is restrictive, which means if the organization has active relationships with child entities, the organization cannot be deleted. Therefore, the Delete option on the context menu is disabled but the user is given no indication about why it is disabled.

15.5.2.2 Wrapping of data fails

System fails to wrap data with a large number of characters in multiple places in the application.

15.5.2.3 Context menu continues to display when a user selects another transaction

System displays the context menu in left hand pane even when the user has selected to perform another transaction, until the user either clicks another primary or secondary menu item or refreshes the context menu.

15.5.2.4 Unnecessary scroll bar on tabbed pages

In resolution 1600 x 1200 or smaller, the horizontal scroll bar always appears for all the tabs at the bottom content frame (Attributes, Members, Privileges, Mappings and History).

15.5.2.5 Hierarchy bread crumbs update only on submit and reload of the page

When a person's location in any of the hierarchies changes, the hierarchy path bread crumb does not change unless submit and reload actions are performed.

15.5.2.6 Tree view requires refresh to reflect recent updates

The user must refresh the tree after performing a transaction that creates or updates tree members to reflect those changes in the tree view. This is only an issue if a node is created directly under the root node or for operations performed in other user sessions.

15.5.2.7 Timestamp value does not always match user's locale in role mapping details

When viewing role mapping details, the user may see local time in some and GMT in others. The timestamp format should always match the user's locale.

15.5.2.8 Submit button appears functional to users without appropriate sphere of control to edit role

When a user is granted a system role with system privilege, "All for System Role Objects," where the role grant sphere of control is set to *ORG_A*, but that system role is defined with sphere of control set to *ORG_B*, if the user navigates to roles in *ORG_B*, edits appear to be allowed. However, when the user clicks the Submit button and then returns to the "edited" role, no changes have been made.

15.5.2.9 Cannot change sphere of control while creating a new role if user switches tab focus

While creating a system role, if the user navigates to another tab in the application, when returning to the Attributes tab and sets sphere of control, the error "Cannot change the SOC hierarchy type of a role" displays. The workaround is to cancel the operation and start over, setting sphere of control before navigating to another tab.

15.5.3 Installation

This section describes known bugs related to installation and contains the following topics.

15.5.3.1 Configuration Assistant fails on retry after database connection

System fails to roll back the previous configuration and displays an exception on retrying the configuration. The workaround is to exit and restart the installer and uninstall the recent installation home, drop and re-create the users/schemas for Oracle Role Manager, then run the installer to install and configure Oracle Role Manager.

15.5.3.2 Installer intermittently skips screens when the user goes back to previous screen

If this occurs, the workaround is to navigate all the way back to the File Location Page, which forces the installer to restart the interview phase and display all screens.

15.5.3.3 System displays the file copy progress as 92% on completion instead of 100% while running the silent installer

While running the installer in silent mode, the file copy progress is displayed as 92% instead of 100%.

15.5.3.4 In clustered environments, managed server fails to start after configuring WebLogic using the provided template

When attempting to start the managed server for Oracle Role Manager, the following exception message displays in the application server console:

```
SEVERE: Failure disabling delivery of messages to BtFinisherMessageEJB
weblogic.management.NoAccessRuntimeException:
Access not allowed for subject: principals=[ormserver, Deployers], on
ResourceType: MessageDrivenEJBRuntime
```

This occurs because a permission is missing from the template file used to configure WebLogic for Oracle Role Manager in clustered environments. The workaround is to assign the ormserver user to the Administrators group using the WebLogic Administrative Console, and then restart all servers.

15.5.3.5 Oracle Role Manager runInstaller fails to install on SUSE 10

To install Oracle Role Manager successfully on SUSE 10, run the installer with the option to ignore pre-reqs:

```
./runInstaller -ignoreSysPrereqs
```

15.5.4 Integration Library

This section describes known bugs of the Oracle Role Manager Integration Library with Oracle Identity Manager and contains the following topic:

- Sequence in which records are reconciled from Oracle Identity Manager affects creation of relationships between person records
- Exception in Oracle Identity Manager application server console while running RoleManagerUserGroupsCleanup scheduled task
- Static business roles with the same name not created properly in Oracle Identity Manager
- OIM-setup.sh and ORM-setup.sh scripts does not run on SUSE 10 machine

15.5.4.1 Sequence in which records are reconciled from Oracle Identity Manager affects creation of relationships between person records

Suppose the person records of a user and the user's manager are created in Oracle Role Manager during reconciliation with Oracle Identity Manager. You then delete the manager's person record through the Oracle Role Manager user interface. During the scheduled user reconciliation (Quick or Full) after the manager's person record is deleted, although the manager's person record is re-created in Oracle Role Manager, the manager's person record might not be associated with the user's person record. By the end of the next scheduled user reconciliation (Quick or Full), the manager's person record is associated with the user's reconciliation run.

15.5.4.2 Exception in Oracle Identity Manager application server console while running RoleManagerUserGroupsCleanup scheduled task

The following error might display on the application server console for Oracle Identity Manager when the RoleManagerUserGroupsCleanup scheduled task is run:

```
ERROR,19 Apr 2009 00:28:17,080,[XELLERATE.SERVER],Class/Method: QuartzWrapper/run
encounter some problems: Exhausted Resultset
java.sql.SQLException: Exhausted Resultset
```

The recommended workaround is to use the Resource Management component of the Oracle Administrative and User Console to create and then run a scheduled task with a task name of RoleManagerUserGroupsCleanup1 and class name of oracle.iam.rm.imframework.scheduledTasks.ScheduledUserGroupsCleanup.

15.5.4.3 Static business roles with the same name not created properly in Oracle Identity Manager

If more than one static business role share the same name and are sent to Oracle Identity Manager during in the same run of the BusinessRolePublishing process, the Integration Library creates the first user group of that name, but fails to create the others. In this case, the Integration Library throws the error "duplication user group" in the Oracle Identity Manager application server console.

The workaround is to run the BusinessRolePublishing process again to create the second user group of that name (ORM_BR_*name*~1), and again for the third (ORM_BR_*name*~2), and so forth.

15.5.4.4 OIM-setup.sh and ORM-setup.sh scripts does not run on SUSE 10 machine

To execute OIM-setup.sh successfully, you must ensure that the following prerequisites are met:

For Oracle Identity Manager:

Remove ^M character in:

ORMINT_HOME/tools/WebLogic_Automation/oim-setup.sh

and

ORMINT_HOME/tools/WebLogicAutomation/properties/OIMConfig.properties.

This is done by executing either dos2unix, for example, dos2unix oim-setup.sh or the following shell commands:

1. sed 's/^M//g' oim-setup.sh > oim-setup-temp.sh
2. mv oim-setup-temp.sh oim-setup.sh

Note:

- Character '^M' is entered as 'ctl-V' and 'ctl-M'.
- Execute Step 1 and Step 2 for OIMConfig.properties file.

For Oracle Role Manager:

Remove ^M character in:

ORMINT_HOME/tools/WebLogic_Automation/orm-setup.sh

and

ORMINT_HOME/tools/WebLogicAutomation/properties/ORMConfig.properties.

This is done by executing either dos2unix, for example, dos2unix oim-setup.sh or the following shell commands:

1. sed 's/^M//g' oim-setup.sh > orm-setup-temp.sh
2. mv orm-setup-temp.sh orm-setup.sh

Note:

- Characters '^M' is entered as 'ctl-V' and 'ctl-M'.
- Execute Step 1and Step 2 for ORMConfig.properties file.

15.5.5 Search

This section describes known bugs around the search functionality and behavior and contains the following topics:

- Sorting of items in search results are case sensitive
- Search results fail to refresh in pop-up windows

15.5.5.1 Sorting of items in search results are case sensitive

Sorting of search results should not be case sensitive throughout the application.

15.5.5.2 Search results fail to refresh in pop-up windows

System fails to refresh the search results and displays the previous search results in the pop-up window.

15.5.5.3 Searchable attributes/operators should be sorted alphabetically

Search attributes and operators appear to be sorted in random order in the search menu on search pages. Sort order should be alphabetical and non-case-insensitive.

15.5.5.4 Search operator should be retained when selecting a different search attribute.

When the user searches by first name using the *begins with* operator and later searches by a different attribute, the operator refreshes to contains, the default operator.

15.5.5.5 Misleading message when user attempts empty wildcard search

When the user searches on a blank value, the message "Full wildcard search is not supported" displays, which is a misleading statement. Full wildcard searches can be performed by entering the percent symbol (%) in the field to search.

15.5.6 Server

This section describes known server bugs and contains the following topics:

- JMSContainerInvoker exception displays in console on clustered JBoss environments

15.5.6.1 Data load fails when data contains the specified field delimiter

When the specified field delimiter character is present in the data to be loaded, the data loader fails. There is not currently a means by which an escape character can be provided to allow the special character to be treated as "loadable" data.

The recommendation is to make sure the field delimiter for all object types is a character that is not contained in your data set. The delimiter is set in the file parsing scripts. For information about the file parsing scripts see *Oracle Role Manager Administrator's Guide*.

15.5.6.2 System allows the System Administrator system role to be deleted or made inactive

Important grants are allowed to be removed. The recommended workaround is to use the procedures described in the *Oracle Role Manager Administrator's Guide* to restore the System Administrator system user.

15.5.6.3 J2EE EJB method invocation may time out and roll back if batch role resolution takes longer than specified time

EJB method invocation has a timeout associated with it so that no matter how many retries might take place, the batch role membership does not complete.

For JBoss, in the jboss.xml file, add configuration of the following to the TimerCommandEJB configuration:

```
<method-attributes>
   <method>
      <method-name>execute</method-name>
                  <transaction-timeout>3600</transaction-timeout><!-- Maximum 1
hour per batch
resolution process -->
   </method>
</method-attributes>
```

For WebSphere, in the server.jar file, add a META-INF/ibm-ejb-jar-ext.xmi file with the following contents:

```
<?xml version="1.0" encoding="UTF-8"?>
<ejbext:EJBJarExtension xmi:version="2.0" xmlns:xmi="http://www.omg.org/XMI"
xmlns:ejbext="ejbext.xmi" xmlns:ejb="ejb.xmi" xmi:id="ejb-jar_ID_Ext">
<ejbExtensions xmi:type="ejbext:SessionExtension" xmi:id="SessionExtension_1"
timeout="3600">
   <enterpriseBean xmi:type="ejb:Session" href="META-INF/ejb-jar.xml#Session_
1183672362012"/>
</ejbExtensions>
<ejbJar href="META-INF/ejb-jar.xml#EJBJar_1183672362010"/>
</ejbext:EJBJarExtension>
```

15.5.6.4 Oracle RAC support lacks certification for high availability scenarios

The Oracle Role Manager supports Oracle RAC database environments for general purpose operation only. High-availability scenarios, such as load balancing and failover, are not officially supported.

15.5.6.5 Bulk loading of large data set with Sun JDK throws errors

When deploying large data sets on Oracle Role Manager configured with the Sun JDK, the error "java.lang.OutOfMemoryError: Java heap space" might display. This is caused by either not enough JVM memory set in JAVA_OPTIONS, not enough physical memory on the host, or both.

For more information about increasing the JVM memory settings, see *Oracle Role Manager Installation Guide*.

15.5.6.6 Deploy tool fails to deploy when CAR file contains unchanged XML

If a customized CAR bundle contains already deployed but unchanged versioned XML files, the CAR file cannot be deployed. One workaround is to make sure that customizations are bundled separately, for example, the CAR file to deploy contains only the changed XML files.

Another workaround is to separate the versioned files (standard.xml, standard_ permissions.xml, oim_integration.xml in oracle.iam.rm.temporal, and any XML that contains customized application data model extensions) from the component configuration XML files. This workaround allows redeploy of configuration without having to create separate CAR files. Note that redeploying the versioned files requires incrementing the version each time the CAR is changed and redeployed.

15.5.6.7 Web sessions on clustered JBoss environments may not failover where messages are waiting to display

Due to a Java Server Faces bug, there is a small chance that a user session might be lost when replicating a user session during an application server failover event. This issue only occurs when a user performs create, delete, or update actions in the Web application and a message instance inside the session is not yet visible in the user interface. In this rare situation, a JBossCacheService exception (java.io.NotSerializableException) displays in the log file and can be ignored.

15.5.6.8 Problems when the database server and the application server are set to different times

When the database server and the application server are set to different times, there can be problems deploying the Oracle Role Manager server to the application server. There can also be problems related to setting transaction time for operations submitted from the Oracle Role Manager Web application.

15.5.6.9 JMSContainerInvoker exception displays in console on clustered JBoss environments

When starting the primary node on JBoss, some WARN exceptions display in the application server console. This is because JBoss happens to load the

finalization-server.ear before its dependencies, such as the JMS resources and the server.ear EJBs. These error conditions recover when the dependencies are subsequently loaded, so the exception messages can be ignored.

15.5.7 System Messages

This section describes bugs relating to messages generated by the system that display to the end user. This section contains the following topics:

- System fails to display a warning dialog when canceling or navigating away from a create process
- No warning message when delegating a Business Role twice to the same person

15.5.7.1 System fails to display a warning dialog when canceling or navigating away from a create process

The system does not display a dialog with a meaningful message and successfully allows the user to navigate away from the create page. The user is not warned that he may lose data already entered.

15.5.7.2 No warning message when delegating a Business Role twice to the same person

When delegating a Business Role twice to the same person, the system successfully prevents repeat delegation, but no message displays to inform the user that the person already has been delegated that role.

15.6 Certification Information

The latest certification information for Oracle Role Manager 10g (10.1.4.2) is available at:

`http://www.oracle.com/technology/software/products/ias/files/idm_certification_101401.html`

16

Oracle Identity Manager

The Oracle Identity Manager release 9.1.0.2 patch set enables you to upgrade to Oracle Identity Manager release 9.1.0.2 from the following releases:

- Oracle Identity Manager release 9.1.0.1
- Oracle Identity Manager release 9.1.0 (running on Oracle Application Server) on which the patch set for Arabic language support has been installed

You can upgrade to release 9.1.0.2 if any one of the following conditions is true:

- You are running Oracle Identity Manager release 9.1.0 on Oracle Application Server and the patch set for Arabic language support has been installed.

  Note: Contact Oracle Support for information about the patch set for Arabic language support.

- You are running Oracle Identity Manager release 9.1.0.1 on any application server.

The following sections of this chapter contain release notes information and installation instructions for the patch set:

16.1 What's New in Oracle Identity Manager Release 9.1.0.2?

The following sections discuss new features introduced in Oracle Identity Manager release 9.1.0.2:

16.1.1 Support for Segregation of Duties (SoD)

In the Oracle Identity Manager implementation of SoD, IT privilege (entitlement) requests submitted by a user are checked and approved by an SoD engine and other users. Multiple levels of system and human checks can be introduced to ensure that even changes to the original request are vetted before they are cleared. This preventive simulation approach helps identify and correct potentially conflicting assignment of entitlements to a user, before the requested entitlements are granted to the user.

> **See Also:** "Segregation of Duties (SoD) in Oracle Identity Manager" in *Oracle Identity Manager Tools Reference* for more information

16.1.2 Support for Offline Provisioning

In online provisioning, multiple provisioning operations that constitute a provisioning request are performed in sequence. In addition, the provisioning request is treated as a single transaction. This approach could cause performance issues. In addition, there is a higher probability of transaction timeout and, therefore, the entire transaction being rolled back.

In offline provisioning, provisioning operations within a request are converted into JMS messages. There is one JMS message submitted for each resource provisioned to each user. Processing of each JMS message is treated as a single transaction, and it is asynchronous and independent of other JMS messages. Processing of the other messages continues even if one transaction times out. This approach offers better performance and a lower probability of transaction timeout.

The Failed Off-line Provisioning Messages report provides details of failed messages.

The Remove Failed Off-line Messages scheduled task has been introduced to remove failed messages from the database table in which these messages are stored.

See the "Enabling Offline Provisioning" chapter in *Oracle Identity Manager Best Practices Guide* for more information.

16.1.3 Support for Capture and Use of Entitlement Data

From this release onward, you can mark a child process form field as an entitlement and then enable the capture of data related to the entitlement. By enabling this feature for all resource objects defined in your Oracle Identity Manager installation, you can generate reports related to entitlements that are available for provisioning and entitlements that have been assigned to users.

See the "Using Entitlement Data" chapter in *Oracle Identity Manager Tools Reference* for more information.

16.1.4 Introduction of the Bulk Load Utility

The Bulk Load utility is aimed at automating the process of loading large volumes of user and account data into Oracle Identity Manager. It helps reduce the downtime involved in loading data. You can use this utility either immediately after you install Oracle Identity Manager or at any time during the production lifetime of Oracle Identity Manager.

See the "Bulk Load Utility" chapter in *Oracle Identity Manager Tools Reference* for more information.

16.1.5 Support for Future-Dated Reconciliation Events

Some target systems allow future-dating (effective-dating) of certain user lifecycle events. For example, an administrator on the target system can specify that a user's account must be enabled on 17-April-2009 by setting the Effective End Date to that date for the account. You can configure the Process Deferred Recon Events scheduled task to correctly respond to these future-dated reconciliation events. This scheduled task is described in Section 16.1.10, "New Scheduled Tasks." The scheduled task is used in conjunction with the createReconciliationEvent API. This API is listed in Section 16.1.12, "New APIs."

16.1.6 Support for Connection Pooling

Oracle Identity Manager supports connection pooling from this release onward. A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Manager connectors can use these connections to communicate with target systems. At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

See Oracle Identity Manager connector documentation for information about using this feature.

16.1.7 Support for the Arabic Language

Arabic language support has been included in release 9.1.0.2 for Oracle Identity Manager installed on Oracle Application Server. See Section 16.3.9, "Applying the Patch for Arabic Language Support" for information about applying this patch set.

16.1.8 Enhanced Support for Integration Between Oracle Role Manager and Oracle Identity Manager

This section lists the UI changes introduced in release 9.1.0.2.

Features Disabled in Oracle Identity Manager Administrative and User Console

The following features are *disabled* in the Administrative and User Console when the property `XL.OIM-ORM.Integration.Deployed` is set to `true`. These features are disabled when you integrate Oracle Identity Manager with Oracle Role Manager.

However, if you do not integrate Oracle Identity Manager and Oracle Role Manager, then those features will still be seen in Oracle Identity Manager.

> **Note:** The disabled features are now available through the Oracle Role Manager Console. See *Oracle Role Manager User's Guide* for more information.

- **User Details**

  Editing group membership details

- **Organizations**

  Creating administrative groups for organizations

- **User Groups**
  - Creating user groups
  - Editing or deleting group details of user groups
  - Creating administrative user groups
  - Assigning users or sub groups to user groups
  - Removing members from user groups
  - Assigning and removing access policies to user groups

- **Access Policies**

  If the Access Policy is created through Oracle Role Manager Console, then you cannot edit the following values of Access Policy:

  - Resources to be provisioned by this access policy
  - Groups for this access policy

  If the Access Policy is created through Oracle Role Manager Console, then you can view only the following properties:

  - Access Policy Details
    * Name
    * Description
    * With Approval
    * Retrofit Access Policy
    * Priority
  - Resource Form Data
  - Process Form Data

  > **Note:** During reconciliation between Oracle Role Manager and Oracle Identity Manager, only entitlement data in the access policies is sent to Oracle Identity Manager.

- **Resource Management**

  Creating resource administrator groups

16.1.9 Additional Changes on the Oracle Identity Manager UIs

The following changes have been made on the Oracle Identity Manager UIs:

> **Note:** These changes are in addition to the ones described in Section 16.1.8, "Enhanced Support for Integration Between Oracle Role Manager and Oracle Identity Manager."

- A login page appears when you access the Diagnostic Dashboard home page. You can access the Diagnostic Dashboard by using a URL in the following format:

  `http://HOST:PORT/XIMDD`

  The account credentials that you use to log in are the same as your OIM User credentials.
- An error page appears when login to the Diagnostic Dashboard fails, or when a user tries to run a script in the Diagnostic Dashboard.
- A LOGOUT link is displayed if you access the Diagnostic Dashboard through the following URL:

  `http://<host>:<port>/XIMDD/SystemVerification`
- In the Oracle Identity Manager Design Console, a new field `Future Date` is added in the Reconciliation Manager form.
- A filter is introduced for the Rules in a group for Membership Rule.

16.1.10 New Scheduled Tasks

The following scheduled tasks have been introduced in this release:

- Section 16.1.10.1, "Scheduled Tasks for the SoD Feature"
- Section 16.1.10.2, "Scheduled Tasks for Working with Entitlement Data"
- Section 16.1.10.3, "Scheduled Tasks for the Offline Provisioning Feature"
- Section 16.1.10.4, "Other Scheduled Tasks"

16.1.10.1 Scheduled Tasks for the SoD Feature

The following scheduled tasks have been introduced along with the SoD feature:

Get SOD Check Results Provisioning

This scheduled task is used to fetch the SOD Check Results if the SOD Engine is asynchronous in nature. For an asynchronous SOD Engine, the SOD Check Results are not available all at the same time. So, this schedule task must be run after the SOD Check has been initiated. It is run only if SOD Check is triggered through Direct Provisioning or Form Edit.

Get SOD Check Results Approval

This scheduled task helps in getting back the SOD Check Results in case of request based provisioning (if SOD Check was initiated during Approval).

Resubmit Uninitiated Provisioning SOD Checks

During direct provisioning, if the SoD check remains in the SODCheckNotInitiated state or SODCheckCompletedWithError state, then you can run the Resubmit

Uninitiated Provisioning SOD Checks task to initiate the SoD check. When you run the scheduled task, the status of the process task is changed from SODCheckNotInitiated or SODCheckCompletedWithError to SODCheckPending. Tasks in the SODCheckPending state will be completed in the next run of the Get SOD Check Results Provisioning scheduled task.

Resubmit Uninitiated Approval SOD Checks

During request-based provisioning, if the SoD check remains in the SODCheckNotInitiated state or SODCheckCompletedWithError state, then you can run the Resubmit Uninitiated Approval SOD Checks scheduled task to initiate the SoD check. When you run the scheduled task, the status of the process task is changed from SODCheckNotInitiated or SODCheckCompletedWithError to SODCheckPending. Tasks in the SODCheckPending state will be completed in the next run of the Get SOD Check Results Approval scheduled task.

16.1.10.2 Scheduled Tasks for Working with Entitlement Data

The following scheduled tasks have been introduced for working with entitlement data:

Entitlement List

The Entitlement List scheduled task identifies the entitlement attribute from the child process form table and then copies entitlement data from the LKV table into the ENT_LIST table.

Entitlement Assignments

The Entitlement Assignments scheduled task is used for first-time copying of data about assigned entitlements into the ENT_ASSIGN table. This task identifies the entitlement attribute from the child process form table and then copies data about assigned entitlements from the child process form table into the ENT_ASSIGN table. A record created in the ENT_ASSIGN table corresponds to an entitlement assigned to a particular user on a particular target system.

Entitlement Updations

The Entitlement Updations scheduled task updates the ENT_ASSIGN table with changes to entitlement assignment data in the child process form tables. Triggers created by the Entitlement Assignments scheduled task copy changes made to entitlement assignment data into a staging table. The Entitlement Updations scheduled task processes data in the staging table and makes the required changes to data in the ENT_ASSIGN table.

16.1.10.3 Scheduled Tasks for the Offline Provisioning Feature

The following scheduled tasks have been introduced along with the offline provisioning feature:

Remove Failed Off-line Messages

This scheduled task has been introduced to remove failed messages from the database table in which these messages are stored.

16.1.10.4 Other Scheduled Tasks

The following scheduled task can be used after reconciliation of user or account data from target systems:

Configuring the Process Deferred Recon Events

Some target systems of Oracle Identity Manager allow effective-dating of certain user lifecycle events, such as hiring and designation changes. In other words, you can set a future date for such a change to a user's record, and the change will take effect on the specified day.

> **See Also:** *Oracle Identity Manager Administrative and User Console Guide* for detailed information about working with scheduled tasks.

The Process Deferred Recon Events scheduled task has been added to support reconciliation of effective-dated reconciliation events. Reconciliation scheduled tasks fetch all modified records into Oracle Identity Manager. The following sequence of steps describes how future-dated events are processed:

> **Note:** It is not mandatory to configure the Process Deferred Recon Events scheduled task.

1. When the Reconciliation Manager encounters a future-dated reconciliation event, it sets the status of the event to `Event Deferred`, if the date value of `Future Date` passed to the API is greater than the `Current System Date` and the `Future Date` column in the database is set to `date passed`.
2. When the Process Deferred Recon Events scheduled task is run, it checks if the date value stored in the database is less than or equal to the `Current System Date`. If yes, then it processes the Recon Event as the existing recon flow and changes the status of the Recon Event accordingly. If not, then it does not perform any action.

16.1.11 New Reports

The following reports have been introduced in release 9.1.0.2:

> **Note:** These reports are available as part of BI Publisher based reports on Oracle Technology Network. To download the reports bundle:
>
> 1. Visit the Oracle Technology Network Web site at `http://www.oracle.com/technology/products/id_mgmt/oxp/index.html`
> 2. Under the Technical Information section, click **Oracle Identity Manager 9.1.0.2 - BI Publisher Reports.**

Off-line Resource Provisioning Messages

The Off-line Resource Provisioning Messages report provides details of failed messages. This report has been introduced along with the offline provisioning feature.

Entitlement Access List

The Entitlement Access List report lists users who are currently assigned the entitlements that you specify while generating the report. The report provides basic information about the entitlements and the list of users to whom the entitlements are assigned.

Entitlement Access List History

The Entitlement Access List History report lists users who had been assigned the entitlements that you specify while generating the report. The report provides basic information about the entitlements and the list of users to whom the entitlements were assigned.

User Resource Entitlement

The User Resource Entitlement report lists the current entitlements of users whom you specify while generating the report. The report displays basic user information and entitlement details.

User Resource Entitlement History

The User Resource Entitlement History report lists details of past entitlements assigned to users whom you specify while generating the report. The report displays basic user information and entitlement details.

16.1.12 New APIs

Table 16–1 lists the new application programming interfaces (APIs) that are added in release 9.1.0.2.

Table 16–1 New APIs in Release 9.1.0.2

Interface	API Method	Description
`tcAccessPolicyOperationsIntf`	`public void updateEntitlementToAccessPolicy (long policyKey, long[] entitlementKey) throws tcPolicyNotFoundException, tcAPIException,tcEntitlementNotFoundException`	Updates a set of entitlements mapped to an Access Policy. The entitlement data provided should be final as it overrides the existing data.
`tcAccessPolicyOperationsIntf`	`public Thor.API.tcResultSet getMappedEntitlements( longpolicyKey) throws tcPolicyNotFoundException, tcAPIException`	The returned attributes contain the following columns: Entitlements.Resource ID Entitlements.Key Entitlements.Entitlement Entitlements.Entitlement Code Entitlements.Entitlement Valid Flag
`tcAccessPolicyOperationsIntf`	`public void unAssignObjects(long policyKey, long[] objectKeys, boolean removeFormData) throws tcPolicyNotFoundException, tcAPIException, tcBulkException`	Cleans up the existing associated form data for objects of an Access Policy.

Table 16–1 (Cont.) New APIs in Release 9.1.0.2

Interface	API Method	Description
tcRulesOperationsIntf	tcResultSet findRuleElements(long rulekey)throws tcRuleNotFoundException, tcAPIException	The returned attributes contain the following columns: Rule Designer.Rule Element.Attribute Rule Designer.Rule Element.Attribute Source Rule Designer.Rule Element.Attribute Value Rule Designer.Rule Element.Child Key Rule Designer.Rule Element.Key Rule Designer.Rule Element.Operation Rule Designer.Rule Element.Sequence Rule Designer.Rule Element.User-Defined Form
tcLookupOperationsIntf	public tcResultSet getLookupCodesForDecoded(String psLookupCode, String decodedValues) throws tcAPIException, tcInvalidLookupException	Returns, in the form of a tcResultSet, a list of lookup encoded values with associated decoded values.
tcReconciliationOperationsIntf	public long createReconciliationEvent(String psObjectName, Map poData, boolean pbFinishEvent, java.sql.Date futureDate) throws tcAPIException, tcObjectNotFoundException;	Returns the key for future-dated reconciliation events created for the specified object. The status of these events is Event Deferred.
tcReconciliationOperationsIntf	public long createReconciliationEvent(String psObjectName, Map poData, boolean pbFinishEvent, String psDateFormat, java.sql.Date futureDate) throws tcAPIException, tcObjectNotFoundException;	Returns the key for future-dated reconciliation events created for the specified object. The status of these events is Event Deferred.

Table 16–1 (Cont.) New APIs in Release 9.1.0.2

Interface	API Method	Description
`tcReconciliationOperationsIntf`	`public void updateReconEvent(long rceKey,java.util.Map attributes) throws Thor.API.Exceptions.tcAPIException, Thor.API.Exceptions.tcReconEventNotFoundException, tcAPIException`	Updates any attribute of the recon event.
`tcGroupOperationsIntf`	`public Thor.API.tcResultSet findAssignedMembershipRules(java.util.Map searchCriteria) throws Thor.API.Exceptions.tcAPIException, tcAPIException`	Returns, in the form of a tcResultSet, a list of assigned membership rules of the group. The tcResultSet contains the following column names: ■ Groups.Key ■ Groups.Group Name ■ Rule Designer.Key ■ Rule Designer.Name
`tcGroupOperationsIntf`	`public Thor.API.tcResultSet findUnassignedMembershipRules(java.util.Map searchCriterias) throws Thor.API.Exceptions.tcAPIException, tcAPIException`	Returns, in the form of a tcResultSet, a list of unassigned membership rules of the group. The tcResultSet contains the following column names: ■ Groups.Key ■ Groups.Group Name ■ Rule Designer.Key ■ Rule Designer.Name ■ Rule Designer.Type
`tcEntitlementsOperationsBean`	`public tcResultSet findEntitlements(Map attributeList)`	Returns, in the form of a tcResultSet, a list of entitlements.
`tcProvisioningOperationsIntf`	`public tcResultSet findAllOpenProvisioningTasks(Map attributeList , String[] statuses) throws tcAPIException`	This method returns a list of all provisioning tasks (and their details) assigned to any user. For displaying the open pending and rejected tasks, the statuses argument filter can be used. The returned object will be a result set with each row having detailed information about each task.

Table 16–1 (Cont.) New APIs in Release 9.1.0.2

Interface	API Method	Description
tcFormInstanceOperationsIntf	public void executeSODCheck(long plProcessInstanceKey) throws tcProcessNotFoundException, tcFormNotFoundException, tcRequiredDataMissingException, tcInvalidValueException, tcNotAtomicProcessException, tcAPIException	This method initiates the SOD Check by creating SODChecker Task Instance for the process whose instance key is passed as argument.
tcFormInstanceOperationsIntf	public long addProcessFormChildData(long plChildFormDefinitionKey, long plProcessInstanceKey, Map phAttributeList, boolean createHolder, boolean createSODChecker)throws tcProcessNotFoundException, tcFormNotFoundException, tcRequiredDataMissingException, tcInvalidValueException, tcNotAtomicProcessException, tcAPIException	Adds process data to the child form that is associated with an instance of a process in the system. It takes 2 flags for creation of Holder and SODChecker Tasks. Holder Task is used to hold the entitlement task until SODCheck is performed and SODChecker task instantiates the SOD Check (by running the InitiateSODCheck Adapter that must be attached to it).

16.1.13 New System Properties

The following client-side system properties have been introduced in release 9.1.0.2:

- XL.OIM-ORM.Integration.Deployed

  This property is used to determine whether the ORM-OIM integration library is deployed or not. The Oracle Role Manager (ORM) Console governs certain Oracle Identity Manager features, such as creating a group and modifying an access policy.

  The default value for this property is `False`.

- XL.SoDCheckRequired

  This property is used to enable or disable SOD Check.

  The default value for this property is `False`.

- XL.SIL.Home.Dir

  The property must be set to the full path and name of the *SIL_HOME* directory.

  The default value for this property is `C:/SIL_HOME`.

- XL.SoD.Offlined.Sync

If the SoD check remains in the SODCheckNotInitiated state or SODCheckCompletedWithError state, then you can run one of the following scheduled tasks to initiate the SoD check:

- Resubmit Uninitiated Provisioning SOD Checks
- Resubmit Uninitiated Approval SOD Checks

To enable these scheduled tasks to run automatically at this stage of the process, set the XL.SoD.Offlined.Sync to `true`. Otherwise, set this system property to `false`. The default value is `true`.

16.1.14 New Adapters

`InitiateSODCheck`

This adapter initiates the SOD Check. It must be attached to an SODChecker Task (that is, any Task whose name is prefixed by 'SODChecker').

16.2 Certified Components

For information about certified application servers and languages, refer to the following sections:

- Section 16.2.1, "Certified Application Servers"
- Section 16.2.2, "Certified Languages"

For information about other certified components, refer to the certification matrix on the following page:

`http://www.oracle.com/technology/software/products/ias/files/idm_certification_101401.html`

16.2.1 Certified Application Servers

Note: There is no change in application server certification from release 9.1.0.1 to release 9.1.0.2.

Oracle Identity Manager release 9.1.0.2 is certified for the following application servers:

- IBM WebSphere Application Server 6.1.0.21 and later fix packs (that is, 6.1.0.21 and later)

  Note: Stop the IBM WebSphere Application Server. Upgrade IBM WebSphere Application Server and Application client to 6.1.0.21. Restart IBM WebSphere Application Server 6.1.0.21.

- JBoss Application Server 4.2.3 GA
- Oracle Application Server 10.1.3.3 (Upgrade patch 10.1.3.3 applied on top of the base package bundled in Oracle SOA Suite 10g release 10.1.3.1)

Note:

- To update Oracle Application Server JDKs for DST 2007 compliance, you must use the appropriate time zone update utility from your JDK vendor. For information about using JDK vendor time zone update utilities, refer to Note 414153.1 on the My Oracle Support Web site.

  You can access the My Oracle Support Web site at

  http://metalink.oracle.com/

- For the production deployment of Oracle Identity Manager running on Oracle Application Server, you must configure Oracle AQ as the JMS provider. Oracle AQ-based JMS cannot be configured on Microsoft Vista at this time. Microsoft Vista is, therefore, supported for only nonclustered development environments with file-based JMS. To update Oracle Application Server JDKs for DST 2007 compliance, you must use the appropriate time zone update utility from your JDK vendor. For information about using JDK vendor time zone update utilities, refer to Note 414153.1 on the My Oracle Support Web site.

- Oracle WebLogic Server 10.3, 10.3.1, and 10.3.2

16.2.2 Certified Languages

Oracle Identity Manager release 9.1.0.2 is certified for the following languages:

- Arabic

  Note: The Arabic language is supported only on an Oracle Identity Manager installation running on Oracle Application Server.

- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)

  The combination of the Portuguese (Brazilian) locale and IBM WebSphere Application Server is not supported. For more information, refer to APAR IZ01077 on the IBM WebSphere Application Server Web site.

- Spanish

See Also: *Oracle Identity Manager Globalization Guide* for detailed information about Oracle Identity Manager globalization support

16.3 Upgrading to Oracle Identity Manager Release 9.1.0.2

To upgrade from Oracle Identity Manager release 9.1.0.1 to release 9.1.0.2, perform the following procedures:

Note:

- Before you begin the upgrade, extract the contents of the Oracle Identity Manager release 9.1.0.2 patch set to a temporary directory on the computer on which Oracle Identity Manager is installed. This temporary directory is referred to as *PATCH* in this document.
- You can skip any section that does not apply to your operating environment.

16.3.1 Addressing Prerequisites for the Upgrade

Before you begin the upgrade procedure, ensure that the following prerequisites are addressed:

- Create backups of the Oracle Identity Manager and application server installation directories.
- Create a backup of the Oracle Identity Manager database.
- Ensure that there are no pending JMS messages to be consumed.

16.3.2 Upgrading the Oracle Identity Manager Database

The procedure to upgrade Oracle Identity Manager database depends on the database product you are using. The following sections describe the procedure to upgrade Oracle Identity Manager database on Microsoft SQL Server and Oracle Database:

- Section 16.3.2.3, "Loading Metadata into the Database"
- Section 16.3.2.4, "Loading E-Mail Templates"
- Section 16.3.2.5, "Using the Oracle Identity Manager Database Validator"

16.3.2.1 Upgrading Oracle Identity Manager Database on Microsoft SQL Server

To upgrade Oracle Identity Manager database on Microsoft SQL Server 2005:

1. Create a backup of the database.
2. Open a command prompt from the Microsoft SQL Server computer, and then run the following script:

   ```
   PATCH\db\SQLServer\Scripts\oim_db_upg_9101_to_9102.bat SERVER_NAME[\INSTANCE_
   NAME]
   DB_NAME DB_USER_NAME DB_USER_PASSWORD PATCH\db\SQLServer\Scripts\
   ```

3. Compile the stored procedures as follows:
   a. In a text editor, open the following BAT file:

      ```
      PATCH\db\SQLServer\StoredProcedures\compile_all_XL_SP.bat
      ```

   b. For every stored procedure listed in the Sequential Lists section of the compile_all_XL_SP.bat file, replace the string `@sysuser` with the database user name. This must be done because Microsoft SQL Server requires functions invoked from a stored procedure to be qualified by the database user name (owner).

      Note: Ensure that you replace the entire @sysuser string, including the at sign (@).

   c. Run the following script:

      ```
      PATCH\db\SQLServer\StoredProcedures\compile_all_XL_SP.bat SERVER_
      NAME[\INSTANCE_NAME]
      DB_NAME DB_USER_NAME DB_USER_PASSWORD PATCH\db\SQLServer\StoredProcedures\
      ```

4. If you are not using the Audit and Compliance Module and if you want to enable it for release 9.1.0.2, then run the following script:

   ```
   PATCH\db\SQLServer\Scripts\SQLServer_Enable_XACM.bat SERVER_NAME[\INSTANCE_
   NAME]
   DB_NAME DB_USER_NAME DB_USER_PASSWORD PATCH\db\SQLServer\Scripts\
   ```

5. Load the metadata into the Oracle Identity Manager database. See 16.3.2.3 , "Loading Metadata into the Database" for more information about loading the metadata into the database.
6. Enable XA transactions for MSDTC as follows:
   a. On the computer on which Microsoft SQL Server 2005 is running, click **Start**, **Administrative Tools**, and **Component Services**.
   b. Expand the Component Service tree to locate the computer, right-click the computer name, and then select **Properties**.
   c. On the MSDTC tab, click **Security Configuration**.
   d. Under Security Settings, select **Enable XA Transactions**.

e. Click **OK**, and then save the changes.

16.3.2.2 Upgrading Oracle Identity Manager Database on Oracle Database

To upgrade Oracle Identity Manager database on Oracle Database:

1. Back up the existing database.

   Use the export/backup utility provided with the database to perform a complete backup of the database.

   A production database backup includes, but is not limited to, complete export or backup of the Oracle Identity Manager release 9.1.0 or 9.1.0.1 database instance to ensure that, if required, the database can be restored to its original state.

2. If you are using Oracle Database 11*g* release 11.1.0.7, then apply the following patches:

   - 7628358
   - 7598314
   - 7614692

3. Enable execute permissions on the scripts in the *PATCH* directory.

4. To upgrade the database schema from release 9.1.0 to release 9.1.0.2, run the oim_db_upg_910_to_9102.sh (or oim_db_upg_910_to_9102.bat) script on the system on which the release 9.1.0 database is installed.

   The command-line usage for the Oracle oim_db_upg_910_to_9102 script is as follows:

   ```
   PATCH/db/oracle/Scripts/oim_db_upg_910_to_9102.sh (or oim_db_upg_910_to_
   9102.bat)
   ORACLE_SID ORACLE_HOME DB_USER_NAME DB_USER_PASSWORD DIRECTORY_IN_WHICH_DB_
   UPGRADE_ZIP_FILE_IS_EXTRACTED
   ```

5. To upgrade the database schema from release 9.1.0.1 to release 9.1.0.2, run the oim_db_upg_9101_to_9102.sh (oim_db_upg_9101_to_9102.sh) script on the system on which the release 9.1.0.1 database is installed.

   The command-line usage for the script is as follows:

   ```
   PATCH/db/oracle/Scripts/oim_db_upg_9101_to_9102.sh (or oim_db_upg_9101_to_
   9102.bat)
   ORACLE_SID ORACLE_HOME DB_USER_NAME DB_USER_PASSWORD DIRECTORY_IN_WHICH_DB_
   UPGRADE_ZIP_FILE_IS_EXTRACTED
   ```

6. If you are not using the Audit and Compliance Module and if you want to enable it for release 9.1.0.2, perform the following steps as appropriate for your database

   a. Log in to SQL*Plus with the credentials of the Oracle Identity Manager database schema owner.

   b. Run the *PATCH*/db/oracle/Scripts/Oracle_Enable_XACM.sql script.

7. Load metadata into the Oracle Identity Manager database. See 16.3.2.3 , "Loading Metadata into the Database" for more information.

16.3.2.3 Loading Metadata into the Database

To load metadata into the database, you must first make the required changes in one of the following files:

Note: Run the script on the computer on which Oracle Identity Manager is installed.

If you are not using the Audit and Compliance Module, then copy one of the following files:

- LoadXML.bat
- LoadXML.sh

If you are using the Audit and Compliance Module, then copy one of the following files:

- LoadXML_XACM.bat
- LoadXML_XACM.sh

This file is located in the *PATCH*/db/Metadata directory.

To load metadata into the database:

Note: You must run the script on the Oracle Identity Manager host computer.

1. Open the LoadXML or LoadXML_XACM script in a text editor.

   Set the value of the JAVA_HOME variable.

2. Depending on the operating system on which Oracle Identity Manager is deployed:

   - **For Microsoft SQL Server on Microsoft Windows**

     a. In the LoadXML or LoadXML_XACM file, remove REM from the following lines:

     ```
     REM SET SQL_SERVER_DRIVER_DIR=
     ```

     b. Assign the path to the SQL Server driver directory that contains the sqljdbc.jar file:

     ```
     SET SQL_SERVER_DRIVER_DIR=PATH_TO_SQL_DRIVER
     ```

     c. In the LoadXML or LoadXML_XACM file, remove REM from the following line:

     ```
     REM SET XLHOME=
     ```

     d. Specify the full path of the Oracle Identity Manager installation directory.

     ```
     SET XLHOME=OIM_HOME/xellerate
     ```

     Specify the full path up to the xellerate directory.

   - **For Oracle Database on Microsoft Windows**

     a. In the LoadXML or LoadXML_XACM file, remove REM from the following line:

     ```
     REM SET ORACLE_DRIVER_DIR=
     ```

b. Assign the path to the Oracle driver directory containing the Oracle JDBC drivers:

```
SET ORACLE_DRIVER_DIR=PATH_TO_ORACLE_DRIVER
```

c. In the LoadXML or LoadXML_XACM file, remove REM from the following line:

```
REM SET JDBC_DRIVER_VERSION=
```

d. Specify name of the Oracle JDBC driver. For example, `SET JDBC_DRIVER_VERSION=ojdbc14.jar`.

e. In the LoadXML or LoadXML_XACM file, remove REM from the following line:

```
REM SET XLHOME=
```

f. Specify the fullpath for OIM install directory. For example, `SET XLHOME=`*PATH_TO_ORACLE_IDENTITY_MANAGER_INSTALLATION_DIRECTORY*. Specify the path up to the Xellerate directory.

- **For Oracle Database on UNIX:**

  a. In the LoadXML or LoadXML_XACM file, uncomment the following lines:

  ```
  #ORACLE_DRIVER_DIR=
  #export ORACLE_DRIVER_DIR
  ```

  b. Assign the path to the JDBC driver for Oracle, so that the line is similar to the following:

  ```
  ORACLE_DRIVER_DIR=PATH_TO_ORACLE_DRIVER
  export ORACLE_DRIVER_DIR
  ```

  c. In the LoadXML or LoadXML_XACM file, uncomment the following lines:

  ```
  #JDBC_DRIVER_VERSION=
  #export JDBC_DRIVER_VERSION
  ```

  d. Specify name of the Oracle JDBC driver. For example, `JDBC_DRIVER_VERSION=ojdbc14.jar`.

  e. In the LoadXML or LoadXML_XACM file, uncomment the following lines:

  ```
  #XLHOME=
  #export XLHOME
  ```

  f. Specify the full path for OIM install directory. For example, XLHOME=*PATH_TO_ORACLE_IDENTITY_MANAGER_INSTALLATION_DIRECTORY*. Mention the path up to the Xellerate directory.

3. Open a command prompt or console and run the LoadXML or LoadXML_XACM script. While running the script, you must enter values for the following parameters (in the given order):

   - **For Microsoft SQL Server:**

     - JDBC URL. For example: `jdbc:sqlserver://`*DB_HOST_IP*:*PORT* (replace *DB_HOST_IP* with the IP address of the database host and replace *PORT* with the port number of the database host)

     - Database name

     - Database user name

- Password

- **For Oracle Database:**

  - JDBC URL. For example: `jdbc:oracle:thin:@`*`DB_HOST_IP:PORT:SID`* (replace *DB_HOST_IP* with the IP address of the database host, *PORT* with the port number of the database host, and *SID* with the database user ID)

  - Database user name

  - Password

16.3.2.4 Loading E-Mail Templates

To load e-mail templates:

1. Open the *PATCH*/db/metadata/LoadXLIF script in a text editor.

   Set the value of the JAVA_HOME variable.

2. Depending on the operating system on which Oracle Identity Manager is deployed:

   For Microsoft SQL Server on Microsoft Windows

   a. In the LoadXLIF file, remove REM from the following line:

      ```
      REM SET SQL_SERVER_DRIVER_DIR=
      ```

   b. Assign the path to the Microsoft SQL Server driver directory that contains the sqljdbc.jar file:

      ```
      SET SQL_SERVER_DRIVER_DIR=PATH_TO_SQL_DRIVER
      ```

   c. In the LoadXLIF file, remove REM from the following line:

      ```
      REM SET XLHOME=
      ```

   d. Specify the full path of the Oracle Identity Manager installation directory.

      ```
      SET XLHOME=OIM_HOME/xellerate
      ```

      Note: Specify the full path up to the xellerate directory.

   For Oracle Database on Microsoft Windows:

   a. In the LoadXLIF file, remove REM from the following line:

      ```
      REM SET ORACLE_DRIVER_DIR=
      ```

   b. Set the path to the Oracle Database driver directory containing the Oracle JDBC drivers:

      ```
      SET ORACLE_DRIVER_DIR=PATH_TO_ORACLE_DRIVER
      ```

   c. Specify the name of the Oracle JDBC driver. For example:

      ```
      SET JDBC_DRIVER_VERSION=ojdbc14.jar.
      ```

   d. In the LoadXLIF file, remove REM from the following line:

      ```
      REM SET XLHOME=
      ```

e. Specify the full path of the Oracle Identity Manager installation directory. For example:

```
SET XLHOME=PATH_TO_ORACLE_IDENTITY_MANAGER_INSTALLATION_DIRECTORY.
```

Note: Specify the full path up to the xellerate directory.

For Oracle Database on UNIX:

a. In the LoadXLIF file, uncomment the following lines:

```
#ORACLE_DRIVER_DIR=
#export ORACLE_DRIVER_DIR
```

b. In the LoadXLIF file, uncomment the following lines:

```
#XLHOME=
#export XLHOME
```

c. Specify the full path of the Oracle Identity Manager installation directory. For example:

```
XLHOME=PATH_TO_ORACLE_IDENTITY_MANAGER_INSTALLATION_DIRECTORY
```

Note: Specify the full path up to the xellerate directory.

3. Open a command prompt or console, and run the LoadXLIF script. While running the script, you must enter values for the following parameters (in the given order):

For Microsoft SQL Server:

- JDBC URL

  For example: `jdbc:sqlserver://DB_HOST_IP:PORT`

  Replace *DB_HOST_IP* with the IP address of the database host, and replace *PORT* with the port number.
- Database name
- Database user name
- Password
- AUDITCOMPLIANCE

For Oracle Database:

- JDBC URL. For example: `jdbc:oracle:thin:@DB_HOST_IP:SID`

  Replace *DB_HOST_IP* with the IP address of the database host, *PORT* with the port number of the database host, and *SID* with the database user ID.
- Database user name
- Password
- AUDITCOMPLIANCE

16.3.2.5 Using the Oracle Identity Manager Database Validator

The Oracle Identity Manager Database Validator is a command-line interface (CLI) utility that compares objects of two databases and generates a report of the missing and mismatched objects in the destination database.

You can also use this utility to verify an upgrade that you perform.

The Oracle Identity Manager Database Validator compares objects of a standard Oracle Identity Manager schema or a customized Oracle Identity Manager database (source) with a destination database that you specify.

The utility gathers source database details in a table. This information is the standard for comparison. For Oracle Database, the information is saved in a file that is created by the database export utility.

In upgrade scenarios, you can use this utility to verify an upgrade that you perform. You can compare the upgraded Oracle Identity Manager database with the provided standard dump (as source dump). This is to verify the success of Oracle Identity Manager database upgrade after the upgrade patch is applied.

Scenario: You upgrade your Oracle Identity Manager installation from release x.x.1 to release x.x.2 by using a standard upgrade package. Oracle Identity Manager Database Validator identifies the missing and mismatched objects, if any, after the upgrade has been completed.

16.3.2.5.1 Location and Components The Oracle Identity Manager Database Validator files are at the following location:

Oracle Database

PATCH/db/oracle/Utilities/OIMDBValidator

Microsoft SQL Server

PATCH/db/SQLServer/Utilities/OIMDBValidator

All Oracle Identity Manager Database Validator files are located in the OIMDBValidator directory.

Table 16–2 provides information about the files that are part of the Oracle Identity Manager Database Validator.

Table 16–2 Files of the Oracle Identity Manager Database Validator

File	Description
oim_ddl_create_oim_src_db.sql	Creates the oim_src_db table.
oim_dml_populate_oim_src_db.sql	Populates the oim_src_db table with metadata details.
oim_dml_src_do_counts.sql	Takes the row count of Oracle Identity Manager standard tables. This file is optional and is based on your inputs.

Table 16–2 (Cont.) Files of the Oracle Identity Manager Database Validator

File	Description
If Source is a standard database, then:	If Source is a standard/vanilla database, then the standard dump files is named oim_std_src_db.dmp.
oim_std_src_db.dmp	For a successful standard vanilla installation, a standard dump accompanies the utility. This standard file for Oracle Database is available at the following location: PATCH/db/oracle/Utilities/OIMDBValidator\SrcInfo This standard file for Microsoft SQL Server is available at the following location: *PATCH*/db/SQLServer/Utilities/OIMDBValidator\SrcInfo
If Source is a customized database, then: oim_src_db.dmp	You can opt to generate the dump file on your own. This file is created when you want to create a dump file from a source Oracle Identity Manager database of your choice. It is named oim_src_db.dmp, and for Oracle Database, it is available at the following location: For Oracle Database: *PATCH*/db/oracle/Utilities/OIMDBValidator\SrcInfo For Microsoft SQL Server: *PATCH*/db/SQLServer/Utilities/OIMDBValidator\SrcInfo
oim_dml_check_oim_version.sql	Selects the version from the oim_src_db table and compares it with the version of the XSD table of the Destination Oracle Identity Manager schema.
oim_ddl_create_oim_dest_db.sql	Creates the oim_dest_db table in the destination Oracle Identity Manager database. This file is used to store the data dictionary information of Oracle Identity Manager.
oim_dml_populate_oim_dest_db.sql	Populates the oim_dest_db table with metadata details.
oim_dml_dest_do_counts.sql	Counts the number of records in the Oracle Identity Manager standard tables. This file is optional and is based on your input.
oim_db_compare.sql	This main comparison script creates a comparison report named COMPARISON_SUMMARY_*YYYY_MM_DD_HH_MI*.log that lists details of the missing or mismatched objects and the row count difference if any.
oim_ddl_drop_oim_src_dest_db.sql	Drops the tables that are created at the destination. This file is optional and is based on your input.
oim_db_validator.bat (Microsoft Windows) oim_db_validator.sh (UNIX and Linux)	Runs the utility.
oim_db_input.bat (Microsoft Windows)	The oim_db_validator.bat file calls the oim_db_input.bat file to get the user input and validate the provided information.
oim_db_input.sh (UNIX and Linux)	The oim_db_validator.sh file calls the oim_db_input.sh file to get the user input and validate the provided information.

16.3.2.5.2 Oracle Identity Manager Database Validator Functionality To use the Database Validator utility, run the following script:

- On Microsoft Windows: oim_db_validator.bat
- On UNIX: oim_db_validator.sh

After you run the script, a log file is generated with the following name:

For Microsoft Windows:

- If the utility runs without error: oim_db_validator_*YYYY_MM_DD_HH_MM*.log
- In case of error: oim_db_validator_err_*YYYY_MM_DD_HH_MM*.log

For UNIX:

- If the utility runs without error: oim_db_validator_*YYYY_MM_DD_HH_MM*.log
- In case of error: oim_db_validator_err_*YYYY_MM_DD_HH_MM*.log

Authentication

When you run the script, you are prompted to enter the following information:

- Oracle Home/SQL Server name
- Database Name
- Database User name
- Database Password

The utility permits only three connection attempts.

Functionality

The following options are available:

- **Collect Details about the Source Oracle Identity Manager Database:**

  Enter **1** to select this option.

  Select this option to collect details of a specific source.

  The utility generates a .dmp file that is named based on your input of whether or not the source is a standard Oracle Identity Manager installation.

  - **For standard Oracle Identity Manager installation:** The file is named as follows:
    - For Oracle Database: oim_std_src_db.dmp
    - For Microsoft SQL Server: oim_std_src_db.bcp

    This file is shipped along with the utility and is available in the following directory:

    - For Oracle Database:

      PATCH/db/oracle/Utilities/OIMDBValidator\SrcInfo

    - For Microsoft SQL Server:

      PATCH/db/SQLServer/Utilities/OIMDBValidator\SrcInfo

    You can use this file for comparison or upgrade verification.

  - **For nonstandard Oracle Identity Manager installation:** The file is named as follows:
    - For Oracle Database: oim_std_src_db.dmp
    - For Microsoft SQL Server: oim_std_src_db.bcp

- **Compare Source Oracle Identity Manager Database with a Destination Oracle Identity Manager Database:**

Enter **2** to select this option.

Choose either to compare against a standard dump or a user-created dump for a specific source:

– To compare against a standard dump, copy oim_std_src_db.dmp (or oim_std_src_db.bcp) from SoureMetadataDump910 to SrcInfo. If SrcInfo is not already available, then create a new directory. The oim_std_src_db.dmp (or oim_std_src_db.bcp) file is a dump of an Oracle Identity Manager release 9.1.0 vanilla installation.

Note: If the comparison with the standard dump indicates any difference, then contact Oracle support.

– To compare against a user-created dump, copy your dump file to SrcInfo. The name of the dump file must be oim_src_db.dmp or oim_src_db.bcp.

You have options for choosing the source for comparison, whether to calculate the number of rows in the destination Oracle Identity Manager database tables, or to drop the comparison tables.

- **Exit:** Enter **3** to select this option.

  Choose this option to close the utility.

16.3.2.5.3 Sample Comparison Summary Report The following is a sample summary report of the Database Validator utility:

```
################################################################################
#################       R E P O R T        ##########################
################################################################################
Start Time (hh:mi:ss:mmm) : 15:09:39:370
================================================================
======================  S U M M A R Y  ==========================
================================================================
 OIM OBJECT TYPE SOURCE     DESTINATION    COMPARE STATUS
 -------------- ----------- ----------- --------------------
-------------------
 TABLE                    6           5 1 TABLE MISSING
 COLUMN                  26          23 3 COLUMNS MISSING
 PK                       6           5 1 PKS MISSING
 PK COL                   7           6 1 PK COLS MISSING
 FK                       1           0 1 FKS MISSING
 FK COL                   1           0 1 FK COLS MISSING
 U INDEX                  2           2 SUCCESSFUL
 UIDX COL                 5           5 SUCCESSFUL
 NU INDEX                 1           1 SUCCESSFUL
 NUIDX COL                1           1 SUCCESSFUL
 VIEW                     1           1 SUCCESSFUL
 PROCEDURE                1           1 SUCCESSFUL
 FUNCTION                 1           1 SUCCESSFUL
 TRIGGER                  1           1 SUCCESSFUL

============================================================  DETAILS OF
DIFFERENCES  ==============================================================
 ######################## MISSING OBJECTS  ##########################

 MISSING OBJECT'S NAME          MISSING OBJECT'S TYPE
 ------------------------------ ------------------------------
 AAP                             TABLE
```

```
 PK_AAP                          PK
 FK_AAD_FK_AAD_AC_ACT         FK

####################MIS-MATCHEDOBJECTS  #################
**********************
MISSING TABLE COLUMNS
**********************
 OBJECT NAME        OBJECT TYPE PARENT OBJECT      PARENT OBJECT TYPE DATATYPE
COLUMN LENGTH ISNULL
 -------------------- ----------- -------------------- ------------------
--------------- ------------- -----
 AAP_KEY           COLUMN     AAP              TABLE           numeric
9 NO
 ACT_KEY           COLUMN     AAP              TABLE           numeric
9 NO
 AAP_VALUE          COLUMN     AAP               TABLE           varchar
200 YES

*****************************************************
COLUMN DETAILS OF PRIMARY KEYS, FOREIGN KEYS & INDEXES
*****************************************************
 OBJECT NAME          OBJECT TYPE PARENT OBJECT        PARENT OBJECT TYPE COLUMN
POSITION CHILD TABLE          CHILD TABLE COLUMN
 -------------------- ----------- -------------------- ------------------
--------------- -------------------- --------------------
 AAP_KEY              PK COL      PK_AAP               PK
1
 ACT_KEY             FK COL      FK_AAD_FK_AAD_AC_ACT FK
1 ACT                   ACT_KEY

============================================================  SEED METADATA
COMPARISION  ==================================================================
 NO DIFFERENCES FOUND.

End Time (hh:mi:ss:mmm) : 15:09:39:387
```

16.3.3 Upgrading Oracle Identity Manager

Note:

It is assumed that you have already upgraded the database by performing the procedure described earlier in this document.

Do not attempt to upgrade to release 9.1.0.2 from any other previous Oracle Identity Manager release.

The procedure to upgrade from release 9.1.0 or release 9.1.0.1 to release 9.1.0.2 is divided into the following sections:

- Section 16.3.3.1, "Copying Files"
- Section 16.3.3.2, "Modifying the FormMetaData.xml File"
- Section 16.3.3.3, "Upgrading Oracle Identity Manager on Oracle WebLogic Server"
- Section 16.3.3.4, "Upgrading Oracle Identity Manager on JBoss Application Server"

- Section 16.3.3.5, "Upgrading Oracle Identity Manager on IBM WebSphere Application Server"
- Section 16.3.3.6, "Upgrading Oracle Identity Manager on Oracle Application Server"

16.3.3.1 Copying Files

Perform the following steps:

1. Create a backup of the contents of the *OIM_HOME*/xellerate directory.
2. Copy the files listed in Table 16–3.

> **Note:**
>
> For a clustered installation of Oracle Identity Manager, copy all the files from the *PATCH* directory to the cluster members.
>
> If you want to enable the SoD feature introduced in this release, then you may have to copy additional files. For detailed instructions on enabling the SoD feature, see the "Segregation of Duties (SoD) in Oracle Identity Manager" chapter in *Oracle Identity Manager Tools Reference*.

Table 16–3 Files to Be Copied from the Deployment Package

Copy Files From	Copy Files To
PATCH/xellerate/lib	*OIM_HOME*/xellerate/lib
PATCH/xellerate/webapp	*OIM_HOME*/xellerate/webapp
PATCH/xellerate/DDTemplates	*OIM_HOME*/xellerate/DDTemplates
PATCH/xellerate/ext	*OIM_HOME*/xellerate/ext
PATCH/xellerate/customResources **Note:** If you have modified any of the properties files on your Oracle Identity Manager installation, then create a backup of those files before you overwrite the files with the ones from the PATCH directory. After you copy the files, make the same modifications in the newly copied files.	*OIM_HOME*/xellerate/customResources
PATCH/xellerate/GTC	*OIM_HOME*/xellerate/GTC
PATCH/xellerate/bin	*OIM_HOME*/xellerate/bin

Table 16–3 (Cont.) Files to Be Copied from the Deployment Package

Copy Files From	Copy Files To
Copy the following files from the *PATCH*/xellerate/setup directory: ▪ setup ▪ If you are upgrading from release 9.1.0 with the Arabic language patch set applied, then copy the following files: UpgradeAttestation UpgradeAttestation.sh (or UpgradeAttestation.bat) ▪ If you are using Oracle Application Server, then copy the oc4j-setup file. ▪ If you are using IBM WebSphere Application Server, then copy the following files: websphereCheckParameter WebSphereCreateDataSource.jacl websphere-setup	*OIM_HOME*/xellerate/setup
PATCH/xellerate/SPMLWS	*OIM_HOME*/xellerate/SPMLWS
PATCH/config	*OIM_HOME*/xellerate/config

3. The setup directory is in the *OIM_HOME* directory. You must ensure that the name of the setup directory is in lowercase letters, and not `Setup`.
4. If you are upgrading from release 9.1.0, then run the UpgradeAttestation script as follows:
   a. Open the following script files in a text editor:

      On Microsoft Windows:

      OIM_HOME\xellerate\setup\UpgradeAttestation.bat

      On UNIX:

      OIM_HOME/xellerate/setup/UpgradeAttestation.sh
   b. Set the path of the JAVA_HOME directory in the file.

      If there are spaces in the names of any directory in JAVA_HOME path, then enclose the directory name in double quotation marks as shown in the following example:

      JAVA_HOME=C:\"program files"\Java\jdk1.6.0_11
   c. Save and close the file.
   d. Run one of the following commands:

      On Microsoft Windows:

      OIM_HOME\xellerate\setup\UpgradeAttestation.bat *JDBC_DRIVER DB_URL OIM_DB_USERNAME OIM_DB_PASSWORD*

      On UNIX:

      OIM_HOME/xellerate/setup/UpgradeAttestation.sh *JDBC_DRIVER DB_URL OIM_DB_USERNAME OIM_DB_PASSWORD*

      In this command:

- Replace *JDBC_DRIVER* with the name of the JDBC driver.
- Replace *DB_URL* with the URL for the database.
- Replace *OIM_DB_USERNAME* with the user name for the database.
- Replace *OIM_DB_PASSWORD* with the password for the database

On Microsoft SQL Server, the semicolon (;) and equal sign (=) characters are treated as delimiters. If you are passing arguments with these characters from the command line, then enclose the arguments in double quotes. For example, when running UpgradeAttestation.bat, pass the arguments as shown in the following example:

```
UpgradeAttestation.bat com.microsoft.jdbc.sqlserver.SQLServerDriver
"jdbc:microsoft:sqlserver://localhost:1433;DatabaseName=XELL;
SelectMethod=Cursor" user password
```

5. Update the GenerateSnapShot script as follows:
   a. Create backups of the existing GenerateSnapShot files from the *OIM_HOME*/xellerate/bin directory:

      GenerateSnapshot.bat

      GenerateSnapshot.sh

      GenerateGPASnapshot.bat

      GenerateGPASnapshot.sh

   b. Copy the GenerateSnapShot files from the *PATCH*/xellerate/bin directory to the *OIM_HOME*/xellerate/bin directory.

   c. In the *OIM_HOME*/xellerate/bin directory, open the new GenerateSnapShot.sh or GenerateSnapShot.bat in a text editor.

   d. In the file, search for the lines containing the following text:

      ```
      APP_SERVER=@appserver
      APP_SERVER_HOME=@app_server_home
      JAVA_HOME=@jdk_loc
      Profile_Name=@profile_name
      ```

   e. Replace the @appserver, @appserver, @app_server_home, @jdk_loc, and @profile_name placeholders with actual values from the backup copy of the GenerateSnapShot file.

   f. If you are using Microsoft SQL Server, then search for SQL_SERVER_DRIVER_DIR in the file and replace it with the full path of the Microsoft SQL Server driver directory.

   g. Save and close the file.

6. If you are using Microsoft SQL Server, then copy the sqljdbc.jar file to the lib directory of the application server.
   - For a nonclustered installation in JBoss Application Server:

     JBOSS_HOME\server\default\lib

     For a clustered installation in JBoss Application Server:

     JBOSS_HOME\server\all\lib

   - For Oracle WebLogic Server:

DOMAIN_HOME\lib

Note: For a clustered installation of Oracle Identity Manager, copy *DOMAIN_HOME*\lib\ on all the nodes.

- For IBM WebSphere Application Server:

  WAS_HOME\profiles\<ProfileName>\lib\

Note: For a clustered installation of Oracle Identity Manager, copy *WAS_HOME*\profiles\<ProfileName>\lib\ on all the nodes.

16.3.3.2 Modifying the FormMetaData.xml File

Note: The steps described in this section are part of the procedure required to implement the offline provisioning feature. See Section 16.1.2, "Support for Offline Provisioning" for more information about this feature. Create a backup of the existing customized FormMetaData.xml and reapply the changes.

Modify the FormMetaData.xml as follows:

Note: In a clustered environment, perform this step on all nodes of the cluster.

1. Open the FormMetaData.xml file in a text editor. This file is in the *OIM_HOME*/config directory.
2. In the Form name="5" element of the FormMetaData.xml file, add the lines highlighted bold font in the following code block:

```
<Form name="5">
   <!-- Resource Name -->
   <AttributeReference editable="true"
optional="false">-502</AttributeReference>
   <!-- Description -->
   <AttributeReference editable="true"
optional="false">-503</AttributeReference>
   <!--Type-->
   <AttributeReference editable="true"
optional="true">-504</AttributeReference>
   <!-- Target -->
   <AttributeReference editable="true"
optional="true">-505</AttributeReference>
   <!-- Auto Prepopulate -->
   <AttributeReference editable="true"
optional="true">-506</AttributeReference>
   <!-- Allow Multiple -->
   <AttributeReference editable="true"
optional="true">-507</AttributeReference>
   <!-- Allow All -->
   <AttributeReference editable="true"
optional="true">-508</AttributeReference>
   <!-- Auto Save -->
```

```
   <AttributeReference editable="true"
optional="true">-509</AttributeReference>
   <!-- Auto Launch -->
   <AttributeReference editable="true"
optional="true">-510</AttributeReference>
   <!-- Self Request Allowed -->
   <AttributeReference editable="true"
optional="true">-511</AttributeReference>
   <!-- Provision By Resource Admin Only -->
   <AttributeReference editable="true"
optional="true">-512</AttributeReference>
   <!-- Off-line Provisioning -->
   <AttributeReference editable="true"
optional="true">-513</AttributeReference>
   <!-- Trusted Source -->
   <AttributeReference editable="true"
optional="true">-514</AttributeReference>
   <!-- Sequence Recon -->
   <AttributeReference editable="true"
optional="true">-515</AttributeReference>
</Form>

<!-- Resource Management section -->
  <!-- List of attributes that can be displayed in the "Resource" Form -->
  <Attribute name="-501" variantType="long" datalength="50"  map="Objects.Key"
/>
  <Attribute name="-502" label="taskdetails.label.resourcename"
    displayComponentType="TextField" variantType="String" dataLength="80"
    map="Objects.Name" />
  <Attribute name="-503"
    label="UserGroupPolicies.label.columnHeading.policyDescription"
    displayComponentType="TextField" variantType="String" dataLength="256"
    map="Structure Utility.Description" />
  <Attribute name="-504"  label="global.label.type"
   displayComponentType="LookupField" variantType="long" dataLength="256"
   map="Objects.Type">
  <ValidValues lookupCode="Lookup.Objects.Object Type"
   selectionColumn="lkv_encoded"/>
  </Attribute>
  <Attribute name="-505"  label="requestWizard.message.target"
   displayComponentType="TextField" variantType="String" dataLength="256"
   map="Objects.Order For" />
  <Attribute name="-506"  label="global.label.autoprepopulate"
   displayComponentType="CheckBox" variantType="String" dataLength="1"
   map="Objects.Auto Prepopulate" />
  <Attribute name="-507"  label="dualListTest.message.resourceallowmultiple"
   displayComponentType="CheckBox" variantType="String" dataLength="1"
   map="Objects.Allow Multiple" />
  <Attribute name="-508"  label="global.label.allowall"
   displayComponentType="CheckBox" variantType="String" dataLength="1"
    map="Objects.Allow All" />
  <Attribute name="-509"  label="global.label.autosave"
   displayComponentType="CheckBox" variantType="String" dataLength="1"
   map="Objects.Auto Save" />
  <Attribute name="-510"  label="global.label.autolaunch"
   displayComponentType="CheckBox" variantType="String" dataLength="1"
   map="Objects.Auto Launch" />
  <Attribute name="-511"  label="global.label.selfrequestallowed"
   displayComponentType="CheckBox" variantType="String" dataLength="1"
   map="Objects.Self Request Allowed" />
```

```
<Attribute name="-512"  label="global.label.provisionbyresourceadminonly"
 displayComponentType="CheckBox" variantType="String" dataLength="1"
 map="Objects.Admin Only" />
<Attribute name="-513"  label="global.label.offlineprovisioning"
 displayComponentType="CheckBox" variantType="String" dataLength="1"
 map="Objects.Off-line Provisioning" />
<Attribute name="-514"  label="global.label.trustedsource"
 displayComponentType="CheckBox" variantType="String" dataLength="1"
 map="Objects.Trusted Source" />
<Attribute name="-515"  label="global.label.sequencerecon"
 displayComponentType="CheckBox" variantType="String" dataLength="1"
 map="Objects.Sequence Recon" />
```

3. Save and close the file.

16.3.3.3 Upgrading Oracle Identity Manager on Oracle WebLogic Server

To upgrade Oracle Identity Manager on Oracle WebLogic Server:

1. Modify the `MaxPermSize` JVM memory setting as follows:
   a. In a text editor, open the *DOMAIN_HOME*/bin/setDomainEnv.sh (or setDomainEnv.cmd) file.
   b. Search for the following line:

      ```
      MEM_MAX_PERM_SIZE="-XX:MaxPermSize=128m"
      ```

   c. Change the memory setting from 128 to 256 as follows:

      ```
      MEM_MAX_PERM_SIZE="-XX:MaxPermSize=256m"
      ```

2. Modify the `MEM_ARGS` JVM memory settings as follows:
   a. Open the following file in a text editor:

      For Windows:

      DOMAIN_HOME/bin/xlStartWLS.cmd

      For Non-Windows:

      DOMAIN_HOME/bin/xlStartWLS.sh

   b. Modify the memory arguments as follows:

      For Microsoft Windows, if Sun JVM is used:

      ```
      MEM_ARGS=-Xms1280m -Xmx1280m -XX:PermSize=128m -XX:MaxPermSize=256m
      ```

      For Microsoft Windows, if BEA JRockit JVM is used:

      ```
      MEM_ARGS=-Xms1280m -Xmx1280m
      ```

      For UNIX, if Sun JVM is used:

      ```
      USER_MEM_ARGS="-Xms256m -Xmx1280m -XX:PermSize=128m -XX:MaxPermSize=256m"
      ```

      For UNIX, if BEA JRockit JVM is used:

      ```
      USER_MEM_ARGS="-Xms256m -Xmx1280m -XnoOpt"
      ```

3. Modify the Managed Server file for a Non-Windows platform as follows:
   a. In a text editor, open the *DOMAIN_HOME*/bin/xlStartManagedServer.sh file.
   b. Search for the following lines:

```
export param1=$1
export param2=$2
```

Change them to the following:

```
param1=$1
export param1
param2=$2
export param2
```

4. In the *OIM_HOME*/xellerate/setup/weblogic-setup.xml file:

   a. Search for the following element:

```
<wldeploy action="deploy"
source="${WL_APP_LOCATION}/OIMApplications/WL${application.filename}"
name="Xellerate"
user="${weblogic_login_user}"
password="${weblogic_login_password}"
verbose="true"
adminurl="t3://${weblogic_server_target_url}:${weblogic_server_admin_port}"
debug="${action.deploy.debug}"
targets="${wl.deploy.target}" />
```

   b. Add a timeout value of 5400 as shown:

```
<wldeploy action="deploy"
source="${WL_APP_LOCATION}/OIMApplications/WL${application.filename}"
name="Xellerate"
user="${weblogic_login_user}"
password="${weblogic_login_password}"
verbose="true"
adminurl="t3://${weblogic_server_target_url}:${weblogic_server_admin_port}"
debug="${action.deploy.debug}"
targets="${wl.deploy.target}"
timeout="5400" />
```

5. Apply the patch as follows:

   Note: It is recommended that you use the production mode for Oracle Identity Manager deployment. If the Oracle WebLogic Server domain is created in development mode, then the application of the patch might fail with the warning that the lock is obtained by another user. To avoid this issue, you must deselect the Automatically acquire lock option in the WebLogic admin console before you start applying the patch.

   a. In a nonclustered environment, stop and then start the server by running *OIM_HOME*/xellerate/bin/xlStartServer.sh or (xlStartServer.bat).

      In a clustered environment, start the admin server, managed servers, and the Node Manager (if you are using the Node Manager).

   b. Run the following command to apply the patch:

      OIM_HOME/xellerate/setup/patch_weblogic.cmd/sh *WEBLOGIC_ADMIN_PASSWORD OIM_DB_USER_PASSWORD*

Note: Ensure that the application server is running before you apply the Oracle Identity Manager patch files. After the patches are applied, you must stop and restart the application server for the patches to take effect.

Troubleshooting the Application of the Patch on Oracle WebLogic Server

If application of the patch fails on Oracle WebLogic Server, then perform the following steps:

1. Log in to the WebLogic admin console, and undeploy the Xellerate and Nexaweb application from.
2. Delete the xellerate.ear and Nexaweb.ear files from the *OIM_HOME*/xellerate/OIMApplications directory.

   Note: In a clustered environment, perform this step on all nodes of the cluster.

3. Delete the contents of the *OIM_HOME*/xellerate/webapp/precompiled directory.
4. Delete the ant_backup.jar, optional_backup.jar and xercesImpl_backup.jar files from the *OIM_HOME*/xellerate/ant/lib directory.
5. In a clustered environment, delete the xellerate and Nexaweb directories from the *BEA_HOME*/user_projects/domains/*DOMAIN_NAME*/servers/AdminServer/tmp/_WL_user directory.
6. In a clustered environment:

   Delete the xellerate and Nexaweb directories from the *BEA_HOME*/user_projects/domains/*DOMAIN_NAME*/servers/*MANAGED_SERVER_NAME*/tmp/_WL_user directory.

   Delete the xellerate and Nexaweb directories from the *BEA_HOME*/user_projects/domains/*DOMAIN_NAME*/servers/*MANAGED_SERVER_NAME*/stage directory.
7. Restart Oracle WebLogic Server.

   Note: In a clustered environment, restart the managed servers.

8. Open a session, and set the JAVA_HOME and PATH environment variables.
9. In the same session, rerun the patch_weblogic script.

16.3.3.4 Upgrading Oracle Identity Manager on JBoss Application Server

To upgrade Oracle Identity Manager on JBoss Application Server:

1. Open the following file in a text editor:

   On a nonclustered installation:

   JBOSS_HOME/server/default/deploy/jboss-web.deployer/server.xml

   On a clustered installation:

   JBOSS_HOME/server/all/deploy/jboss-web.deployer/server.xml

2. In this file, change the value of the emptySessionPath element to `false`.
3. Run the patch command as follows:

   OIM_HOME/xellerate/setup/patch_jboss.cmd (or patch_jboss.sh) *OIM_DB_USER_PASSWORD*

> **Note:** If your Oracle Identity Manager installation is running on an RHEL 5 computer with JBoss Application Server 4.2.3 and JDK 1.60.10, then set the JAVA_OPTS parameter to the following:
>
> ```
> JAVA_OPTS=%JAVA_OPTS% -XX:MaxPermSize=128m -XX:+UseConcMarkSweepGC
> -XX:+CMSClassUnloadingEnabled
> ```

16.3.3.5 Upgrading Oracle Identity Manager on IBM WebSphere Application Server

To upgrade Oracle Identity Manager on IBM WebSphere Application Server:

- In a nonclustered environment, run the following command to apply the patch:

> **Note:** Ensure that the application server is running before you apply the Oracle Identity Manager patch files. After the patches are applied, you must stop and restart the application server for the patches to take effect.

OIM_HOME/xellerate/setup/patch_websphere.cmd/sh *WEBSPHERE_ADMIN_PASSWORD OIM_DB_USER_PASSWORD*

- In a clustered environment:
  1. Ensure that the Network Deployment Manager and all the cluster members are running.
  2. Run the following command from the Network Deployment Manager:

     OIM_HOME/xellerate/setup/patch_websphere.sh (or patch_websphere.cmd) *WEBSPHERE_ADMIN_PASSWORD OIM_DB_USER_PASSWORD*

16.3.3.6 Upgrading Oracle Identity Manager on Oracle Application Server

To upgrade Oracle Identity Manager on Oracle Application Server:

1. Run the following script:

> **Note:** Ensure that the application server is running before you apply the Oracle Identity Manager patch files. After the patches are applied, you must stop and restart the application server for the patches to take effect.

OIM_HOME\xellerate\setup\patch_oc4j.cmd (or patch_oc4j.sh) *OAS_ADMIN_PASSWORD DATASOURCE_PASSWORD*

2. Restart the Oracle Identity Manager server. For a clustered installation, restart each node of the cluster.

16.3.4 Upgrading the Oracle Identity Manager Design Console

To upgrade the Design Console:

1. Create a backup of the *OIM_DC_HOME*\xlclient directory.
2. Replace the contents of the following directory with the contents of the *PATCH*/xlclient/lib directory:

   OIM_DC_HOME\xlclient\lib
3. Copy the following files:
   - XLDesktopClient.ear from *PATCH*/xlclient to *OIM_DC_HOME*\xlclient
   - xlFvcUtil.ear from *PATCH*\xlclient to *OIM_DC_HOME*\xlclient

If you are using IBM WebSphere Application Server as the application server, then update the xlDataObjectBeans.jar file as follows:

> **Note:** Ensure that you perform these steps after you have performed the procedure described in Section 16.3.3.5, "Upgrading Oracle Identity Manager on IBM WebSphere Application Server."

1. In a Web browser, connect to the WebSphere administrative console by using a URL of the following format:

   `http://HOST_NAME:PORT/admin`
2. Log in by using the Oracle Identity Manager administrator account that you specified during installation.
3. Click **Applications**, and then select **Enterprise Applications**.
4. Select **Xellerate application**.
5. Click **Export**.
6. Save the xellerate.ear file to a temporary directory.
7. Extract the xlDataObjectBeans.jar file from the xellerate.ear file.

> **Note:** Ensure that you extract the xlDataObjectBeans.jar file and not the xlDataObjects.jar file.

8. Copy the xlDataObjectBeans.jar file into the *OIM_DC_HOME*\xlclient\lib directory.

16.3.5 Upgrading the Oracle Identity Manager Remote Manager

To upgrade the Remote Manager:

1. Create a backup of the *OIM_RM_HOME*/xlremote/lib directory.
2. Replace the contents of the lib directory with the contents of the *PATCH*/xlremote/lib directory.

16.3.6 Redeploying the Diagnostic Dashboard

After upgrading to Oracle Identity Manager release 9.1.0.2, you must redeploy the Diagnostic Dashboard by performing the procedure described in one of the following sections:

- Section 16.3.6.1, "Redeploying the Diagnostic Dashboard on IBM WebSphere Application Server"
- Section 16.3.6.2, "Redeploying the Diagnostic Dashboard on JBoss Application Server"
- Section 16.3.6.3, "Redeploying the Diagnostic Dashboard on Oracle Application Server"
- Section 16.3.6.4, "Redeploying the Diagnostic Dashboard on Oracle WebLogic Server"

16.3.6.1 Redeploying the Diagnostic Dashboard on IBM WebSphere Application Server

To redeploy the Diagnostic Dashboard on IBM WebSphere Application Server, see "Installing the Diagnostic Dashboard" in *Oracle Identity Manager Administrative and User Console Guide for Release 9.1.0.2*.

In addition, perform the following steps:

> **Note:** It is assumed that you have already deployed the XIMDD.war from the *PATCH*/Diagnostic Dashboard directory.

1. Extract the xlDataobjectBeans.jar file from the xellerate.ear file deployed on the application server host computer. To do so:
   a. Log in to the WebSphere Admin console.
   b. From the Application menu, select Enterprise Application.
   c. Select xellerate.ear, click Extract, and then provide a path for the directory into which you want to extract the file.
2. Copy the xlDataobjectBeans.jar file into the following directory:

   WAS_HOME/profiles/*PROFILE_NAME*/installedApps/*CELL_NAME*/XIMDD.ear/XIMDD.war/WEB-INF/lib
3. Restart the application server.

16.3.6.2 Redeploying the Diagnostic Dashboard on JBoss Application Server

To redeploy the Diagnostic Dashboard on JBoss Application Server, use the following file:

PATCH/Diagnostic Dashboard/jboss/XIMDD.war

To redeploy the Diagnostic Dashboard, see "Installing the Diagnostic Dashboard" in *Oracle Identity Manager Administrative and User Console Guide for Release 9.1.0.2*.

16.3.6.3 Redeploying the Diagnostic Dashboard on Oracle Application Server

To redeploy the Diagnostic Dashboard on Oracle Application Server, see "Installing the Diagnostic Dashboard" in *Oracle Identity Manager Administrative and User Console Guide for Release 9.1.0.2*.

After you deploy the XIMDD.war file:

1. Open the following file in a text editor:

   ORACLE_HOME/j2ee/*OAS_INSTANCE_NAME*/application-deployments/XIMDD/orion-application.xml

2. Search for the following lines:

```
<imported-shared-libraries>
</imported-shared-libraries>
```

3. Replace these lines with the following lines:

```
<imported-shared-libraries>
<import-shared-library name="oim.xml.parser"/>
<remove-inherited name="apache.commons.logging"/>
</imported-shared-libraries>
```

4. Restart the servers by using the opmnctl utililty.

16.3.6.4 Redeploying the Diagnostic Dashboard on Oracle WebLogic Server

To redeploy the Diagnostic Dashboard on Oracle WebLogic Server, see "Installing the Diagnostic Dashboard" in *Oracle Identity Manager Administrative and User Console Guide for Release 9.1.0.2*.

16.3.7 Redeploying the SPML Web Service

If you are using SPML Web service along with Oracle Identity Manager, then you must redeploy the SPML Web service after you upgrade Oracle Identity Manager.

Note: On JBoss Application Server, ensure that the commons-discovery.jar file is in the following directory:

- For a nonclustered installation:

  JBOSS_HOME/server/default/lib

- For a clustered installation:

  JBOSS_HOME/server/all/lib

If the commons-discovery.jar file is not present in this directory, then download and copy it from the Apache Web site.

If you have customized the EAR file, then you must redo those changes in the EAR file and then redeploy it.

Note: See the application server vendor documentation for information about undeploying the application.

See *Oracle Identity Manager Tools Reference* for information about the deployment procedure.

16.3.8 Enabling the Integration with Oracle Role Manager

> **Note:** The procedure described in this section is optional. Perform this procedure only if you are integrating Oracle Identity Manager with Oracle Role Manager.

If you are integrating Oracle Identity Manager with Oracle Role Manager, then set the XL.OIM-ORM.Integration.Deployed property to `true`. See *Oracle Identity Manager Design Console Guide* for information about working with system properties.

16.3.9 Applying the Patch for Arabic Language Support

> **Note:** This section describes an optional procedure. Perform this procedure only if you want to use the Arabic locale. You need not perform this procedure if you were already using the Arabic locale before you upgraded to release 9.1.0.2.

If required, you can enable support for the Arabic language after upgrading to Oracle Identity Manager release 9.1.0.2. To enable support for the Arabic language:

1. Log in as the Oracle Identity Manager database schema owner.
2. Run the following script:

   PATCH/db/oracle/Scripts/dml_update_region_language_to_arabic.sql

16.3.10 Reapplying Customizations and Compiling Adapters

See Section 16.6.1, "Customizations in Release 9.1.0.2" for information about the changes made in Oracle Identity Manager user interface (UI) related files. After you apply the patch, reapply the customizations in the files.

In addition, compile all adapters. See *Oracle Identity Manager Design Console Guide* for instructions.

16.4 Resolved Issues

The following table lists issues resolved in Oracle Identity Manager Release 9.1.0.2:

Bug Number	Description
6885766	If users were added to groups using event handlers on user data objects instead of auto-group membership rules, the time taken for access policy evaluation and resource provisioning increased exponentially with the addition of each group.
7153285	The ORA-936 or ORA-921 error was encountered during reconciliation from Oracle Database.
7228951	The ORA-0911 error was encountered when the reconciliation archival utility was run on an Oracle Identity Manager installation for which the Japanese locale was set.
7190428	During reconciliation, a date field in Oracle Identity Manager was not updated if the date field in the reconciliation event was empty (NULL).

Bug Number	Description
5414750	The createDeleteReconciliationEvent method could delete OIM Users even during target resource trusted reconciliation.
7192812	During reconciliation by using a generic technology connector, the JAVA.LANG.NULLPOINTER exception was encountered if the connector tried to update a UDF.
7263248	Custom authentication login modules did not work on an Oracle Identity Manager installation running on Oracle Application Server.
6403137	During reconciliation, an exception was encountered if multivalued attribute data on the target system contained the single quotation mark (') character.
7372341	At the end of a trusted source reconciliation run, the Manager ID field on the OIM User form was not updated on the OIM User form.
7493603	An error was encountered on attempting to regenerate group or resource profiles for auditing.
7445039	The mav.mav_field_length field was not updated through process form changes. It could be updated only through a process task mapping update.
7432421	An exception was encountered if an SPML response to the SPML Web Service contained white space characters.
7558705	An update to the child form in an access policy resulted in loss of data about the state of check boxes (selected or deselected) on the parent form.
6429919	E-mail was not automatically sent to the requester (user) when the user's profile was edited.
7331148	A newly added UDF did not appear on the mapping page for the Generic Technology Connector feature.
7657868	A dependent resource remained in the Waiting state even after the parent resource reached the Provisioned state.
8206680	On an Oracle Identity Manager installation using Microsoft SQL Server 2005, an error was thrown while attempting to run the Resubmit Reconciliation Event task if the keyword `with` was encountered.
7621211	When an administrator reassigned a task, notification e-mail was not sent to the new assignee and administrator.
7591702	If there were a large number of user records in Oracle Identity Manager, then a user search performed with the asterisk (*) character or a blank value ended in a deadlock situation.
7455899	Access policies did not revoke child records after a reconciliation update was received.
8219167	When a connector definition was exported and then imported, mappings between child tables of the resource object form and the process form were lost.
7831629	Reconciliation failed if two reconciliation attributes had the same field name.
8220275	During target resource reconciliation, the No Match Found event was not created for target system records for which no match was found.
7562283	The request data in the process task adapter mapping returned the Request ID for the Add request for that instance instead of the request ID of the request that initiated the transaction.
8332225	The rules of the default complex password policy in Oracle Identity Manager were different from the password rules in Microsoft Active Directory
7411037	An exception was encountered if a task assignment failed while an API added an approval task.

Bug Number	Description
7330728	There was no API that could accept a Code Key value and find the corresponding Decode value.
6769920	A role could not be deleted by an access policy.
7684896	The e-mail notification feature for a reassigned task was not the same as the feature to send e-mail notification for an assigned task.
8302402	For an Oracle Identity Manager installation set to the Japanese locale, the parent organization name was not displayed in Japanese.
8223798	A resource child form could not be mapped to a process child form in the process definition.
8292615	A warning was displayed on attempting to select multiple resources during request-based provisioning.
7633906	On the Adapter Factory form of the Design Console, a query for an adapter failed if the name of the adapter contained the word `ordered`.
7045674	The Validation engine of the Generic Technology Connector feature accepted only hashtable parent data.
7299418	The Request Type list displayed on the Administrative and User Console showed values that are not supported in Oracle Identity Manager.
7151075	The Adapter Factory returned the following error message when adding an adapter of the Handle Error type: `Field adt_name must be populated before saving.`
7114985	The reconciliation manager table could not display more than 10000 rows.
7275601	When a user was configured as a proxy of the user's manager, the user could approve requests of which the user was the target beneficiary.
7268966	A DDL statement was run within a transaction, and the Commit Not Allowed exception was thrown by the createForm(Map) method.
6765667	Task notification e-mail was sent to proxy users who were in the Disabled state.
7257153	During process matching, the case-sensitive check of the reconciliation rule was not correctly applied.
6987230	An error was encountered on searching for a resource containing a UDF of the lookup field type.
7264986	Values returned by the tcAdpEvent.finalizeProcessAdapter adapter were truncated.
7112468	A user who was a member of the approver group could approve the user's own requests.
7477090	When a form was opened for editing, the items selected and saved in lists on the form were replaced by default entries in the lists.
7338467	When a resource was provisioned by an access policy with approval, the User resource access history report showed the name of the access policy in the Provisioned By column of the report.
7440144	Incorrect results were displayed when a pending approval was denied.
7257810	Provision requests for deleted users caused errors when the Scheduled Provisioning Task scheduled task was run.
7498288	The ServletException exception was encountered when a new user logged in to Oracle Identity Manager using Oracle Access Manager as SSO and changed the user's password.

Bug Number	Description
7382874	A dependency error was encountered while importing an XML file containing the definition of a process task that had a modified adapter.
7515549	The NullPointerException exception was encountered during an import on attempting to import child data dependent and the dependent data does not exist.
7322512	When a resource was provisioned through request-based provisioning, the request number was stored in the Provisioned By column. If the resource was later revoked through request-based provisioning, then the request number was not updated for new request.
7438761	Simultaneous access to the same resource did not result in one user getting an exclusive lock.
7577436	An assigned adapter was displayed in both the assigned and unassigned lists.
7418026	When a user was disabled by a group membership rule, the user's resource was not revoked by the access policy.
7492747	The Auto Save and Auto Prepopulate feature did not work when applied on two provisioning processes one after the other.
7562504	When a user is removed from a group, the User Profile management feature deletes the information about the child form. The NumberFormatException exception was encountered when Oracle Identity Manager tried to parse the version of the child form.
7635371	The password reset function did not work correctly with the minimum password age policy.
6372182	An error was encountered when a resource object was associated with multiple provision processes.
7551251	If a resource was requested for a user whose provisioning date was in the future, when the resource is eventually provisioned, the status of the resource remains at Provisioning although the tasks in the provisioning process are completed.
7576302	A logical entity adapter could not be configured to check if an input date argument was empty.
8261674	The following message was displayed on attempting to select a user on the Step 2: Select users page of the Request-Based Provisioning feature: `Bad User Selection made`
7832304	The logout page was displayed on attempting to log in to the Administrative and User Console.
8232551	The logout page was displayed on refreshing a page after logging in to the Administrative and User Console.
7589327	A user who provided wrong answers to the password challenge questions was not automatically set the Locked state.
7707746	A browser error was encountered on attempting to open a lookup field containing an entry with special characters that the browser did not support.
8213436	When the Group Membership report was run, the ORA-30004 error was encountered because the separator character used was also par of the data in the report.
7616311	An error was encountered if the generic technology connector reconciliation scheduled task did not find the parent identity data source file at the specified staging location.
7493763	The E-mail Address field does not accept some special characters.

Bug Number	Description
8201655	The ORA-1 error was encountered if a requester submitted a second Revoke Resource request on the same resource and the same user.

16.5 Known Issues and Workarounds

The following sections describe known issues related to Oracle Identity Manager release 9.1.0.2:

- Section 16.5.1, "General Known Issues"
- Section 16.5.2, "Design Console Known Issues"
- Section 16.5.3, "Reports Known Issues"
- Section 16.5.4, "Globalization Known Issues"

16.5.1 General Known Issues

This section describes known issues related to the general run-time operation of Oracle Identity Manager Release 9.1.0.2, including known issues for Oracle Identity Manager server and known issues for the Administrative and User Console not related to reporting.

This section contains the following topics:

- Section 16.5.1.1, "Exception May Be Thrown While Using SSO to Log In to Administrative and User Console When Oracle Identity Manager Is Installed in a UNIX/Linux Environment"
- Section 16.5.1.2, "Stack Overflow Exception Thrown When Importing an XML File"
- Section 16.5.1.3, "ConcurrentModificationException in JBoss Cluster Configuration When Replicating Session Data"
- Section 16.5.1.4, "Pending Approvals Cannot Be Filtered by Requester Name"
- Section 16.5.1.5, "All Records Returned When Filtering Records by the Date Type User Defined Field and Searching Using Character Strings"
- Section 16.5.1.6, "Date Value Entered in Incorrect Format in the Administrative and User Console Date Fields Causes an Error Message to Be Displayed"
- Section 16.5.1.7, "Errors When Modifying Settings and Assignments for Internal System-Seeded Users"
- Section 16.5.1.8, "Error Message Displayed After Single Sign-On Timeout Interval in Deployment Manager or WorkFlow Visualizer Windows"
- Section 16.5.1.9, "Null Pointer Exception Thrown When Running the purgecache.bat Utility"
- Section 16.5.1.10, "Challenge Questions Page Displayed in Error in Single Sign-On Mode When "Force to set questions at startup" System Property Set to TRUE"
- Section 16.5.1.11, "System Error May Occur When Accessing Administrative and User Console After Database Is Restarted"
- Section 16.5.1.12, "Warning Page May Be Displayed in the Administrative and User Console After Receiving "Illegal Script Tag or Characters" Message and Clicking the Back Button"

16.5.1.1 Exception May Be Thrown While Using SSO to Log In to Administrative and User Console When Oracle Identity Manager Is Installed in a UNIX/Linux Environment

An exception similar to the following one may be thrown the first time you log in to the Administrative and User Console using SSO in a UNIX/Linux environment:

```
[XELLERATE.WEBAPP],Class/Method: tcWebAdminHomeAction/setChallengeQuestions
encounter some problems: USER_QUES_NOT_DEFINED
Thor.API.Exceptions.tcAPIException: USER_QUES_NOT_DEFINED
```

To resolve this issue, you must use the Design Console to assign a value of `FALSE` to the `Force to set questions at startup` system property.

16.5.1.2 Stack Overflow Exception Thrown When Importing an XML File

When you import an XML file, a stack overflow exception may be thrown if the import operation changes the organizational hierarchy. You can safely ignore this exception.

16.5.1.3 ConcurrentModificationException in JBoss Cluster Configuration When Replicating Session Data

When replicating session data, the JBoss Application Server may fail and generate the following exception in a clustered configuration:

```
16:43:07,296 ERROR [JBossCacheManager] processSessionRepl: failed with
exception: java.util.ConcurrentModificationException
16:43:07,296 WARN [InstantSnapshotManager] Failed to replicate
sessionID:GzUYJdxlSLVxS7ssRtvWwQ**.tqx00
```

16.5.1.4 Pending Approvals Cannot Be Filtered by Requester Name

If you attempt to use the Requester filter to refine the results in the Pending Approvals page, a message indicating that the search did not return any results is displayed. You can use the Requester filter only to refine results by requester ID and not by requester first name or last name.

16.5.1.5 All Records Returned When Filtering Records by the Date Type User Defined Field and Searching Using Character Strings

In the Administrative and User Console, searching based on the Date Type User Defined Field may return all records instead of just the records matching the specified dates. Using character string input as search criteria may also return all records. To avoid these issues, use the following date format:

YYYY-MM-DD

16.5.1.6 Date Value Entered in Incorrect Format in the Administrative and User Console Date Fields Causes an Error Message to Be Displayed

All dates in the Administrative and User Console must be edited using the calendar icon associated with the **Date** field. Do not edit dates directly by entering text in a **Date** field. Instead, use that field's calendar icon to edit the date value.

16.5.1.7 Errors When Modifying Settings and Assignments for Internal System-Seeded Users

Do not modify any settings or assignments for internal system-seeded users. If you attempt to modify any settings or assignments for internal system-seeded users, then you may encounter errors.

16.5.1.8 Error Message Displayed After Single Sign-On Timeout Interval in Deployment Manager or WorkFlow Visualizer Windows

After a Single Sign-On session times out, clicking **Restart** in the Deployment Manager or WorkFlow Visualizer window of the Administrative and User Console may cause a "Client-Side error occurred" error message to be displayed. If this message is displayed, close the browser and then access the Administrative and User Console by using a new browser window.

16.5.1.9 Null Pointer Exception Thrown When Running the purgecache.bat Utility

When you run the `purgecache.bat` utility, the following exception is thrown:

```
java.lang.NullPointerException
     at
com.opensymphony.oscache.base.AbstractCacheAdministrator
     .finalizeListeners(Abs
tractCacheAdministrator.java:323)
     at
com.opensymphony.oscache.general.GeneralCacheAdministrator
     .destroy(GeneralCacheAdministrator.java:168)
     at net.sf.hibernate.cache.OSCache.destroy(OSCache.java:59)
     at
net.sf.hibernate.cache.ReadWriteCache.destroy(ReadWriteCache.java:215)
     at
net.sf.hibernate.impl.SessionFactoryImpl.close(SessionFactoryImpl.java:542)
```

This exception can be safely ignored.

16.5.1.10 Challenge Questions Page Displayed in Error in Single Sign-On Mode When "Force to set questions at startup" System Property Set to TRUE

In the Single Sign-On mode, when the `Force to set questions at startup` system property is set to `TRUE`, the Challenge Questions page is displayed instead of the Welcome page of the Administrative and User Console. In the Single Sign-On mode, the `Force to set questions at startup` system property must be set to `FALSE`.

16.5.1.11 System Error May Occur When Accessing Administrative and User Console After Database Is Restarted

Each application server exhibits different behavior when a database connection is lost during execution. While JBoss Application Server can automatically reestablish a database connection, Oracle WebLogic Server and IBM WebSphere Application Server cannot. For Oracle WebLogic, you can define settings for testing reserved connections,

in which case the connections are established automatically. For IBM WebSphere, you must configure your database for high-availability.

16.5.1.12 Warning Page May Be Displayed in the Administrative and User Console After Receiving "Illegal Script Tag or Characters" Message and Clicking the Back Button

In Microsoft Windows Server 2003 Service Pack 1 (SP1) environments, the "Warning: Page has Expired" page may be displayed if you click the Back button after the "Illegal Script tag or Characters" error message is displayed. You can go back to the first page for creation by clicking the Refresh button on the browser toolbar.

16.5.1.13 Benign Warning Messages May Appear in Oracle Application Server Log File After Installing Release 9.1.0.2 and Starting Oracle Application Server

After installing Oracle Identity Manager release 9.1.0.1 on Oracle Application Server and then starting Oracle Application Server, warning messages regarding files with the same name but that are not identical may appear in the Oracle Application Server log file. These warning messages are benign and can be safely ignored.

16.5.1.14 Deployment Manager Requires JRE 1.6.0_07

An export operation using the Deployment Manager may encounter problems when Microsoft Internet Explorer is configured to use Microsoft Virtual Machine. To reset the default Virtual Machine:

1. Download and install the `Sun JRE 1.6.0_07` from the following Web site:

   `http://java.sun.com/`

2. Select **Tools** from the Internet Explorer menu.
3. Select **Internet Options**.
4. Select the **Advanced** tab.
5. Scroll down to **Java (Sun)**.
6. Check **Use Java 2v1.6.0_xx for <applet>**.
7. Scroll down to **Microsoft VM**.
8. Deselect **Java console enabled** and **Java logging enabled**.
9. Restart the computer.

> **Note:** `JRE 1.6.0_07` is not required to run the Oracle Identity Manager Administrative and User Console—it is only required to run the Deployment Manager.

16.5.1.15 Exception May Be Encountered if IPv6 Is the Internet Protocol in Use

If IPv6 is the Internet protocol in use, then you may encounter the following exceptions in the Oracle Identity Manager logs:

- On JBoss Application Server and Linux with Sun JDK 5 or earlier:

  IP_MULTICAST_IF:

  java.net.SocketException: bad argument for IP_MULTICAST_IF: address not bound to any interface at

java.net.PlainDatagramSocketImpl.socketSetOption(Native Method) at
java.net.PlainDatagramSocketImpl.setOption(PlainDatagramSocketImpl.java:295)

- On Oracle WebLogic Server 10.3.0 and AIX 5.3 with IBM JDK 1.6:

  com.opensymphony.oscache.base.AbstractCacheAdministrator],Could not initialize listener

If you do not need IPv6 support, then you can avoid these exceptions by disabling IPv6 support in the JVM as follows:

1. Open the following script in a text editor:

   OIM_HOME/bin/xlStartServer.sh

2. Add the following line in the script:

   ```
   -Djava.net.preferIPv4Stack=true
   ```

3. Save the changes to the script, and then run it.

16.5.1.16 Multiple Entries for the Same Request ID Are Displayed on the Pending Approvals Page in Administrative and User Console

When more than one approval task is assigned to a user, multiple entries for the same request ID are displayed on the Pending Approvals page in the Administrative and User Console. You can select any of the displayed entries to perform the approval process.

16.5.1.17 Boolean Type Check Box of the User Defined Field Is Not Displayed on Request Submitted Form

The Request Submitted form of the Design Console does not display the Boolean Type User Defined Field check box. If the User Defined Field is set to the Boolean type, then the Request Submitted form displays the number 1 instead of the check box. If the Boolean type is not enabled, then the Request Submitted form displays a blank space.

16.5.1.18 "Illegal Script Tag or Characters" Message Is Displayed in Lookup Forms

In the Administrative and User Console, the "Illegal Script Tag or Characters" message is displayed if you enter the less than symbol (<), greater than symbol (>), or any combination of these symbols (such as << or >>) in a text field on any page that also has a lookup form, and then click the magnifying glass icon.

If this happens, close the lookup form, remove the illegal characters from the text field, and then click the magnifying glass icon to continue with the procedure.

> **See Also:** The "Special Character Restrictions" section in *Oracle Identity Manager Globalization Guide*

16.5.1.19 Error Message Logged When a Scheduled Task Is Viewed or Modified

When you view or modify a scheduled task on the Administrative and User Console, the following message may be recorded in the application server log file:

```
MessageDateFieldBean, localName='messageDateField': Illegal
character (space) in "name" attribute
```

You can ignore this message.

16.5.1.20 User Profile Information Specified in E-mail Definition Is Not Valid for Approval Tasks

The user profile information, which is specified in e-mail definitions of type `General`, is not valid for approval tasks.

16.5.1.21 Exception Thrown on Logging in to WebSphere 6.1.0.9

After installing IBM WebSphere Application Server 6.1.0.9, when you restart the server and log in to the Administrative Console as `xelsysadm`, an exception is thrown. However, this does not affect functionality and you can safely ignore the exception.

16.5.1.22 WSLoginFailedException May Be Thrown in IBM WebSphere Log

The `com.ibm.websphere.security.auth.WSLoginFailedException` exception may be thrown for IBM WebSphere 6.1.0.9 configurations. You can ignore this exception.

This exception has been acknowledged by IBM, and you can refer to the following IBM Web page for more information:

`http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg1PK47479`

16.5.1.23 IllegalArgumentException and CacheException May Be Thrown After Application Server Is Started

Note: This applies only to IBM WebSphere and Oracle Application Server.

The `java.lang.IllegalArgumentException` and `oracle.cabo.image.cache.CacheException` exceptions may be thrown after the application server is started. You can ignore these exceptions.

16.5.1.24 User Password Reset Is Not Supported by SPML Web Service When Password Policies Are Enabled

If password policies are enabled in Oracle Identity Manager, then the SPML Web Service does not support password reset operations.

16.5.1.25 Search Button Must Be Clicked Twice to Search for a Scheduled Task After Changing the State

On the Administrative and User Console, you can enable or disable a scheduled task displayed in the search results table for scheduled tasks. However, if you search for a scheduled task after you change its state, you must click the **Search** button once and then again for the task with the modified state to be displayed.

16.5.1.26 NullPointerException Written to Log File When Oracle Application Server Is Shut Down

When you shut down Oracle Application Server, the `java.lang.NullPointerException` from the com.thortech.xl.cache.CacheUtil component is written to the application server log file. You can safely ignore this exception.

16.5.1.27 Some Postinstallation Tests Offered by the Diagnostic Dashboard Are Displayed in the List of Preinstallation Tests

When you use the Diagnostic Dashboard, although the Test Basic Connectivity, Test Provisioning, and Test Reconciliation tests are available even before you install Oracle Identity Manager, you can use these tests only after you install Oracle Identity Manager.

16.5.1.28 Special Characters Are Not Allowed in Attestation Process Definition

Special characters are not supported in the attestation process definition. Only alphanumeric characters and the underscore (_) character can be included.

16.5.1.29 Columns Names Are Displayed Instead of Labels If an Attestation Scope Is Defined Using User-Defined Fields

While defining an attestation process using the Administrative and User Console, if an attestation scope is defined using user-defined fields (UDFs) on the User Scope or Resource Scope page, then columns names are displayed instead of labels in the list of selected attributes.

16.5.1.30 Reconciliation Event Does Not Exist/Reconciliation Message Failed Log Messages

During reconciliation, an error message similar to the following may be written to the logs:

```
[XELLERATE.JMS],The Reconciliation Event with key 512312 does not exist
[XELLERATE.JMS],Processing Reconciliation Message with ID 512312 failed.
```

Depending on the application server retry settings, these messages are retried for the specified number of times. If JMS is not able to process these messages after the specified number of retries, then these messages are moved to the dead letter queue.

16.5.1.31 Multiple Trusted Source Flag and Reconciliation Sequence Flag Not Displayed in the Administrative and User Console

On the Resource Detail page of the Administrative and User Console, the newly introduced Multiple Trusted Source flag and Reconciliation Sequence flag are not displayed. These flags can be viewed in the Design Console.

16.5.1.32 Resource Name Field of the Create Attestation Process Is Case-Sensitive

In the Create Attestation process, the Resource Name field is case-sensitive. To correctly configure the attestation process, you must use the exact spelling and case (uppercase and lowercase) of the resource name.

16.5.1.33 Retry Interval and Retry Attempt Limit Values Not Displayed on Task Details Page

The Retry Interval and Retry Attempt Limit values are not displayed on the Task Details page of the Workflow Visualizer.

16.5.1.34 Changes to JDBC Connection Pool Attributes May Result in Database User Account Getting Locked

If JDBC connection pool attributes are changed on Oracle Application Server, then the "ORA-28000: the account is locked" error message may be written to the application server log. When this error occurs, the database user account is locked. This is a

known issue with Oracle Application Server when using an indirect password in the connection pool. Oracle Identity Manager connection pools use an indirect password.

If you want to change a connection pool attribute by using the Oracle Application Server Administrative Console, then you can work around this problem as follows:

1. Log in to the Oracle Application Server Administrative Console, and stop the application named `Xellerate`.
2. Change the connection pool attributes.
3. Restart Oracle Application Server.
4. Log in to the Oracle Application Server Administrative Console, and start the `Xellerate` application.

16.5.1.35 Previously Viewed Workflow Displayed on Creating a New Workflow Event

In the Graphical Workflow Designer, when you click Save after adding a new Workflow Event, the previously viewed workflow is displayed instead of the newly created workflow event.

16.5.1.36 User ID Containing Special Characters Is Not Displayed in User ID Lookup Fields

During user creation in the Administrative and User Console, if special characters are included in the User ID value, then look-up fields for user IDs will not be able to display that specific user ID. For information about special character restrictions, refer to Oracle Identity Manager Globalization Guide.

16.5.1.37 Database Error May Be Thrown When Disabling an Organization

When disabling an organization that has child organizations, a database error message may be displayed in addition to the Oracle Identity Manager error message. To avoid this problem, remove parent-child associations before disabling an organization.

16.5.1.38 Session Timeout System Error Thrown During Workflow Creation Can Be Ignored

A session timeout error may be thrown during creation of a workflow. You can safely ignore this error.

16.5.1.39 Known Issues Related to Generic Technology Connectors

Refer to the "Known Issues of Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console*.

16.5.1.40 Exception May Be Thrown When a Scheduled Task Runs for Many Hours

For Oracle Identity Manager on Oracle Application Server, the following exception may be thrown when a scheduled task runs for many hours:

```
Primary Server went down going to get a fresh object elsewhere in the cluster.
com.evermind.server.rmi.RMIConnectionException: LRU connection
```

This exception has no impact on the functioning of Oracle Identity Manager and can be ignored.

16.5.1.41 Filter by Permission Name Field Might Not Accept Non-ASCII Characters

The Filter by Permission Name field on the (Group Details) Permissions page of the Administrative and User Console might not accept non-ASCII characters.

16.5.1.42 JspException Might Be Encountered

You might encounter exceptions similar to the following:

```
javax.servlet.jsp.JspException: Define tag cannot set a null value
```

You can ignore these exceptions because they do not affect the working of Oracle Identity Manager.

16.5.1.43 Java.Lang.Securityexception Exception Might Be Encountered

The Java.Lang.Securityexception: Insufficient Method Permission exception might be encountered when Oracle Identity Manager is running on JBoss Application Server. To work around this issue:

1. From the jira.jboss.org Web site, download the patch for issue JBAS-6236.
2. Create the xlSecurityManager.jar file out of the code in the patch.

   Note: Steps to create the JAR file are documented in the patch itself.

3. Copy the JAR file to the following location:
   - For a nonclustered installation:

     JBOSS_HOME/server/default/lib
   - For a clustered installation, copy the JAR file into the following directory on all the nodes:

     JBOSS_HOME/server/all/lib
4. Open the following file in a text editor:
   - For a nonclustered installation:

     JBOSS_HOME/server/default/conf/jboss-service.xml
   - For a clustered installation:

     JBOSS_HOME/server/default/conf/jboss-service.xml
5. In the XML file, search for the following lines:

   ```
   <!-- JAAS security manager and realm mapping -->
      <mbean code="org.jboss.security.plugins.JaasSecurityManagerService"
   ```

   Replace those lines with the following lines:

   ```
   <!-- JAAS security manager and realm mapping -->
         <mbean code="mysec.security.jboss.jaas.OpenJaasSecurityManagerService"
   ```
6. Restart the server.

16.5.1.44 HeadlessGraphicsEnvironment Exception Might Be Encountered on JBoss Application Server

The following error might be encountered if Oracle Identity Manager is running on JBoss Application Server:

```
java.lang.ClassCastException: sun.java2d.HeadlessGraphicsEnvironment cannot be
cast to sun.awt.Win32GraphicsEnvironment
```

This is a known issue of JDK. For more information, look up Bug 6358034 on the following Web site:

http://bugs.sun.com

16.5.1.45 Java.Lang.IllegalArgumentException Might Be Encountered

You might encounter exceptions similar to the following:

```
java.lang.IllegalArgumentException for creating image cache directory occured
```

You can ignore these exceptions because they do not affect the working of Oracle Identity Manager.

16.5.1.46 Login Attempt on an Idle Login Window May Display the Logout Page

Login attempt on an idle login window may display the logout page. Subsequent login attempts are successful. This does not have any functional impact on Oracle Identity Manager.

16.5.1.47 Connection with Oracle Database 11g Might Fail During Certain Oracle Identity Manager Operations

During certain Oracle Identity Manager operations, the connection with Oracle Database 11*g* might fail and the following error gets recorded in the log file:

```
java.sql.SQLException: Listener refused the connection with the following error:
ORA-12518, TNS:listener could not hand off client connection
```

When this happens, depending on the application server on which Oracle Identity Manager is running, you might have to restart Oracle Identity Manager.

16.5.1.48 tcDefaultSignatureImpl Exception Might Be Encountered When a Scheduled Task Is Run

The following exception might be recorded in the log file when a scheduled task is run:

```
ERROR [ACCOUNTMANAGEMENT] Class/Method: tcDefaultSignatureImpl/verifySignature
encounter some problems
```

However, the task is processed correctly on the next run.

16.5.1.49 System Error Encountered on Trying to View an Object Form on Oracle Identity Manager Using Microsoft SQL Server

You might encounter a system error when you try to view an object form on Oracle Identity Manager using Microsoft SQL Server 2005.

16.5.1.50 Values of Some Fields of an Access Policy process form Are Not Displayed While Editing

The following issue is observed on Oracle Identity Manager running on Oracle Database 11*g* release 1 (11.1.0.7):

While trying to edit an access policy that is attached to a resource object, values of some of the access policy process form fields might not be displayed. However, these values are present in the database. If required, you can enter new values and submit

them. The new values will be posted to the database, and the access policy will function as expected.

This issue is encountered because of Bug 7632407 in Oracle Database 11*g* release 1 (11.1.0.7). At the time of this release, there is no patch available for this issue. According to Bug 7632407, you can apply the following workaround if you encounter this issue:

Log in to Oracle Database as `sysdba`, and then run the following command:

```
set "_optimizer_join_elimination_enabled"=false
```

16.5.1.51 System Error Encountered on Viewing a Resource Form on an Oracle Identity Manager Installation Using Microsoft SQL Server

If a user's resource has been provisioned through request provisioning, then a system error might be encountered when you try to view the resource form from the user's Resource Detail page. This issue is encountered only on an Oracle Identity Manager installation using Microsoft SQL Server.

16.5.1.52 List of Open Tasks Not Displayed on an Oracle Identity Manager Installation Using Microsoft SQL Server

The following issue is observed only on Oracle Identity Manager using Microsoft SQL Server:

When you click Open Tasks on the Administrative and User Console, an exception might be encountered and the list of open tasks might not be displayed.

16.5.1.53 JMS Verification in the Diagnostic Dashboard May Fail in IBM-AIX and Oracle Weblogic Server Combination

The JMS verification in the Diagnostic Dashboard may fail in IBM-AIX and Oracle Weblogic Server combination. This does not affect the runtime component. You can ignore this error.

16.5.1.54 Not Enough Perm Memory While Using Oracle Identity Manager on Oracle Weblogic Server in HP-JDK

If you see any error related to "Permanent generation is full", then increase the Permgen memory in *WLS_DOMAIN_HOME*`/bin/xlStartWLS.cmd` and/or *WLS_DOMAIN_HOME*`/bin/xlStartManagedWLS.cmd` based on which script you use to start Oracle Identity Manager. Note that you may have to change the Server Start option on the Weblogic Admin Console if you are starting the Weblogic server by using the console.

16.5.1.55 Change Password Might Not Work on an Oracle Identity Manager Installation Running on Oracle WebLogic Server and AIX

On an Oracle Identity Manager installation running on Oracle WebLogic Server and AIX, the following error might be encountered when you try to change your password:

"Password does not satisfy the Policies"

16.5.1.56 Assigned Password Policy Is Removed when the Database User Management Connector for Release 9.0.4.1 Is Imported

A password policy assigned to a user is removed when the Database User Management connector for release 9.0.4.1 is imported using the Connector Installer.

16.5.1.57 User Locked Out of Administrative and User Console on Oracle Identity Manager Running on Oracle WebLogic Server

Oracle WebLogic Server has a built-in security feature for automatically locking out users who cross a specified number of invalid login attempts. The default is 5 invalid attempts. Oracle Identity Manager has a similar locking mechanism, and the default is 3 invalid attempts. After 3 invalid attempts, Oracle Identity Manager locks the user in the database. If the user continues to make invalid attempts at logging in, then the application server locks the user. When this problem occurs, the user must wait until the session times out and then try logging in again using valid login credentials.

The following configuration change might help avoid this issue:

> **Note:** Changes that you make by performing this procedure apply to all applications running on the application server.

1. Log in to the WebLogic Application Server console.
2. Go to Security Realms > REALM.
3. On the Configuration tab, select the **User Lockout** subtab.
4. You can apply one of the following approaches:
   - Approach 1:

     Deselect **Lockout Enabled**.
   - Approach 2:

     Modify the following parameters:
     - Lockout Threshold: The maximum number of consecutive invalid login attempts that can occur before a user's account is locked out.
     - Lockout Duration: The number of minutes that a user's account is locked out.
     - Lockout Reset Duration: The number of minutes within which consecutive invalid login attempts cause a user's account to be locked out.
     - Lockout Cache Size: The number of invalid login records (between 0 and 99999) that the server places in a cache.

16.5.1.58 Some Lookup Queries Might Show Only Code Key Values on the Administrative and User Console

If you want a lookup definition of type Lookup Query to show Decode values and store Code Key values, then the underlying lookup query must meet all of the following conditions:

- The SELECT clause must contain columns from the LKV table, LKU table, or both tables.
- The WHERE clause must contain a condition that uses the LKU_TYPE_STRING_KEY column of the LKU table.

The following is an example of this type of lookup query:

```
SELECT LKV_ENCODED,LKV_DECODED
FROM LKV LKV, LKU LKU
WHERE LKV.LKU_KEY=LKU.LKU_KEY
AND
```

```
LKU_TYPE_STRING_KEY='Lookup.EBS.UMX.Roles'
```

If the lookup query does not meet all of these conditions, then the lookup definition displays and stores only Code Key values.

16.5.1.59 Test Connectivity Option Does Not Work for the SoD Engine IT Resource

The Test Connectivity option does not work for the IT resource that you create to hold information about the SoD engine.

16.5.1.60 Users Data Object of Microsoft Active Directory Connector Overwrites the Users Data Object of Oracle Role Manager Integration Library

The following issue is observed if the Microsoft Active Directory connector is installed after the Oracle Role Manager Integration Library is installed:

The Users data object of the Microsoft Active Directory connector overwrites the Users data object of the Oracle Role Manager Integration Library.

To work around this issue:

1. Log in to the Design Console.
2. Expand **Development Tools**.
3. Click **Data Object Manager** under Business Rule Definition.
4. Search for and open **Users**.
5. Click the **Assign** button for Post-update.
6. Assign the **adpOIMUSERCREATEORUPDATEINORM** entity adapter.
7. Click the **Assign** button for Post-delete.
8. Assign the **adpOIMUSERDELETEINORM** entity adapter.
9. Click **Map Adapters**.
10. Select the **adpOIMUSERCREATEORUPDATEINORM** adapter.
11. Map the **userKey** variable to the **USR_KEY** entity field.
12. Select the **adpOIMUSERDELETEINORM** adapter.
13. Map the **userKey** variable to the **USR_KEY** entity field.
14. Save the changes.

16.5.1.61 Bulk Load Utility Can Load User Data Containing First Name Values That Are Up To 255 Characters in Length

The length of the USR.USR_FIRST_NAME column is 256 characters. However, the Bulk Load Utility can only import First Name values that are less than or equal 255 characters in length.

16.5.2 Design Console Known Issues

This section describes known issues related to tasks performed using the Release 9.1.0.2 Design Console—it does not contain known issues related to the installation of the Design Console or its translated text. This section contains the following topics:

- Section 16.5.2.1, "Invoking FVC Utility on IBM WebSphere May Display "Realm/Cell is Null" Error"

16.5.2.1 Invoking FVC Utility on IBM WebSphere May Display "Realm/Cell is Null" Error

When attempting to use the FVC utility in IBM WebSphere deployments, a dialog box with the error message `Realm/cell is Null` may be displayed. You can close the dialog box and ignore this error message to continue.

To avoid this issue entirely, change the properties in the *`WEBSPHERE_HOME`*`\AppClient\properties\sas.client.props` file to the following:

> **Note:** *WEBSPHERE_HOME* represents the location where IBM WebSphere is installed.

Change the existing values to the following:

- `Com.ibm.CORBA.loginSource = properties`
- `Com.ibm.CORBA.loginTimeout = 300`
- `Com.ibm.CORBA.securityEnabled = true`
- `Com.ibm.CORBA.loginUserid = xelsysadm`
- `Com.ibm.CORBA.loginPassword = xelsysadm`

16.5.2.2 Form Designer Feature Does Not Support Special Characters for Column Name

The Form Designer form in the Design Console will not save entries that contain any of the following special characters in the Column Name field:

; / % = | + , \ ' " < >

16.5.2.3 Default Tasks Not Added to Resource Object After Changing Its Process Definition Type

In the Design Console, after changing the Process Definition type for a Resource Object from Approval to Provisioning, or from Provisioning to Approval, the Resource Object is not updated with the default tasks associated with each type of Process Definition. To avoid this issue, do not change the Process Definition type after setting it initially.

16.5.2.4 Cannot Delete User Defined Fields When the Required and Visible Properties are Set to True

Attempting to delete User Defined Fields in the Design Console when the **Required** and **Visible** properties are set to **true** causes an error message to be displayed. To avoid this issue, first delete the properties and then delete the User Defined Column.

16.5.2.5 Cannot Save Multiple Rules Simultaneously

The Rule Designer feature in the Design Console cannot save multiple rules simultaneously. To avoid this issue, save each rule before creating additional rules.

16.5.2.6 Toolbars in Creating New Task Window May Be Disabled When Multiple Creating New Task Windows Are Open

Toolbars in the **Creating New Task** window may be disabled after adding event handlers or adapters from the **Integration** tab when using the same **Create New Task** window for a second time to add a task (by clicking the **New Form** icon). To avoid this issue, close the **Creating New Task** window before creating another task.

16.5.2.7 Error Thrown When the Caret (^) Character Is Encountered in a Challenge Question

While setting challenge questions in the `Lookup.WebClient.Questions` lookup definition, you must not include the caret (^) character in the text of the questions. The Design Console does not stop you from entering this character, but the Administrative and User Console will throw an error when this character is encountered.

16.5.2.8 Error Messages Displayed on the Password Policies Form Are Concatenated

An error message is displayed if there is conflicting input on the Password Policies form. For example, an error message is displayed if the minimum password length specified is greater than the maximum length. If there is more than one set of conflicting input, then the errors messages that are displayed are concatenated.

16.5.2.9 User Group Name Attribute for Reconciliation Mapping

While defining reconciliation field mappings for trusted sources, you must not use the User Group Name user attribute.

16.5.2.10 Single Quotation Mark Cannot Be Included in IT Resource Instance Name

Single quotation marks are not supported in the name of an IT resource. If a single quotation mark is included in the Name field on the IT Resources form, then a system error message is displayed.

16.5.2.11 Passwords As Child Table Fields Are Not Supported

Although you can use the Design Console to mark child table fields as password fields, Oracle Identity Manager does not support passwords as child table fields.

16.5.3 Reports Known Issues

This section describes known issues related to reporting functionality in Release 9.1.0.2. This section contains the following topics:

16.5.3.1 Group Membership History Report Does Not Differentiate Between Active and Deleted Groups

When you run a Group Membership History report, the report results do not differentiate between active and deleted groups.

16.5.3.2 User Disabled and User Unlocked Reports Display Current Values

The User Profile columns in the User Disabled and User Unlocked reports display current values instead of historical values.

16.5.3.3 Resource Name Lookup Window on the Input Parameters Page for Some Reports May Incorrectly Display Organization Resources

In the Administrative and User Console, clicking the **Resource Name** lookup icon on the **Input Parameters** page for various reports will display a lookup window. This lookup window may incorrectly display Organization resources in addition to User resources for the following reports:

- Resource Access List
- Entitlement Summary
- Resource Access List History
- Resource Password Expiration
- Account Activity in Resource
- Task Assignment History
- Rogue Accounts By Resource
- Fine Grained Entitlement Exceptions By Resource

Ignore the Organization resources listed in the lookup window. Running these reports for Organization resources will return no data.

16.5.3.4 Reports May Not Differentiate Between Information for Deleted Users and Information for Users Created with the Same User IDs As the Deleted Users

Reports may not differentiate between information for a deleted user and information for a user that was created with the same user ID as the deleted user, regardless of whether or not the User ID Reuse property is enabled.

16.5.3.5 java.lang.ClassNotFoundException or java.lang.NullPointerException May Be Encountered When You Run the GenerateSnapshot.sh or GenerateGPASnapshot.sh Script on Oracle WebLogic Server

When you run the GenerateSnapshot.sh or GenerateGPASnapshot.sh script on Oracle WebLogic Server, the java.lang.ClassNotFoundException or java.lang.NullPointerException may be encountered. If this happens, then first verify the value of the SQL_SERVER_DRIVER_DIR variable in the script. Then, change the value of the CLASSPATH environment variable in the script file from:

```
%CLASSPATH%;%SQL_SERVER_DRIVER_DIR%\msbase.jar;%SQL_SERVER_DRIVER_
DIR%\mssqlserver.jar;%SQL_SERVER_DRIVER_DIR%\msutil.jar;
```

To one of the following:

For Microsoft SQL Server:

```
%CLASSPATH%;%SQL_SERVER_DRIVER_DIR%\sqljdbc.jar;WL_HOME\server\lib\wlclient.jar
```

For Oracle Database

```
%CLASSPATH%;WL_HOME\server\lib\wlclient.jar
```

16.5.3.6 java.lang.ClassNotFoundException Might Be Encountered When You Run the GenerateSnapshot.sh or GenerateGPASnapshot.sh Script on JBoss Application Server

When you run the GenerateSnapshot.sh or GenerateGPASnapshot.sh script on JBoss Application Server, the java.lang.ClassNotFoundException might be encountered. If this happens, then:

Remove the following entries from the CLASSPATH variable in the script:

- ;%XEL_EXT%\log4j-1.2.8.jar
- msbase.jar
- mssqlserver.jar
- msutil.jar

Add the sqljdbc.jar and *JBOSS_HOME*/client/log4j.jar entries to the CLASSPATH variable in the script.

16.5.3.7 tcDataAccessException Encountered on Generating the Password Reset Success Failure Report on an Oracle Identity Manager Installation Using Microsoft SQL Server

While generating the Password Reset Success Failure report on an Oracle Identity Manager installation using Microsoft SQL Server, a system error might be encountered when you select the Weekly option from the Aggregation Frequency list.

16.5.3.8 Results Might Note Be Generated If UDF Is Added to the Resource Access List Report

If Oracle Identity Manager is using Microsoft SQL Server, then results might not be generated if you add a UDF to the Resource Access List report.

16.5.3.9 classnotfoundexception Exception Encountered While Running the UpgradeAttestation Script on an Oracle Identity Manager Installation Using Microsoft SQL Server

The classnotfoundexception exception might be encountered while running the UpgradeAttestation script on an Oracle Identity Manager installation using Microsoft SQL Server. If this exception is encountered, then open the UpgradeAttestation script in a text editor and implement the following changes:

1. Change `;$CLASS_PATH` to `:$CLASSPATH`.

   Note: Ensure that the semicolon (;) at the start of the text is replaced with a colon (:).

2. Ensure that the sqljdbc.jar file from the Microsoft SQL Server driver is included in the CLASSPATH.

16.5.3.10 Error Encountered When the UpgradeAttestation Script Is Run Twice on the Same Oracle Identity Manager Installation That Is Using Microsoft SQL Server

The UpgradeAttestation script is meant to be run only one on a particular Oracle Identity Manager installation that is using Microsoft SQL Server. If you run the script twice on the same Oracle Identity Manager installation, then the following error is thrown and attestation would not work after the upgrade:

```
com.microsoft.sqlserver.jdbc.SQLServerException: Column names in each table must
be unique.
Column name 'APD_ATTESTATION_DEFINITION' in table 'APD' is specified more than
once
```

16.5.3.11 Report Not generated If a UDF Is Added to the ResourceAccessList Report

If you run the ResourceAccessList report after adding a UDF, then a blank page is displayed.

16.5.3.12 System Error Encountered on Running the Policy List Report with a Wildcard Character on an Oracle Identity Manager Installation Using Microsoft SQL Server

If you try to run the Policy List Report with a wildcard character, then a system error might be encountered. This issue is encountered only on an Oracle Identity Manager installation using Microsoft SQL Server.

16.5.3.13 CORBA.NO_PERMISSION Exception Might Be Encountered on Running the Generatesnapshot or GenerateGPASnapshot Script

On an Oracle Identity Manager installation running on IBM WebSphere Application Server and using Microsoft SQL Server, you might encounter the CORBA.NO_PERMISSION exception when you run the Generatesnapshot or GenerateGPASnapshot script. To address this issue, map roles to user groups as follows:

1. Log in to the WebSphere Administrative Console.
2. Expand **Applications**, select **Enterprise Applications**, select **Xellerate**, and then select **Security role to user/group mapping**.
3. Select **Everyone**.
4. Click **OK**, and then click **Save**.
5. Restart the application server.
6. Rerun the GenerateSnapshot or GenerateGPASnapshot script.

16.5.3.14 ora-01858 Exception Might Be Encountered On Generating an Entitlement Report in a Non-English Locale

The ora-01858 exception might be encountered on generating an entitlement report in a non-English locale.

16.5.3.15 Error Encountered on Trying to Modify a Resource Through the Resource Management Feature

An error encountered on trying to modify a resource through the resource management feature. You can work around this error by clicking OK and closing the error message.

16.5.3.16 BI Publisher Reports Do Not Work on Microsoft SQL Server

The BI Publisher reports do not work on Microsoft SQL Server.

16.5.4 Globalization Known Issues

This section describes known issues in Release 9.1.0.2 related only to globalization or translation. This section contains the following topics:

16.5.4.1 Installer Programs for Non-English Languages May Contain Some English Text

The Installer programs for non-English languages may contain some untranslated text that is displayed in English.

16.5.4.2 Some Administrative and User Console Windows Display Text for Default Locale Setting After Timing Out

In the Administrative and User Console, if the Export and Import pages of the Deployment Manager or the Workflow Visualizer page are open and the session times out, then the text on these pages may be displayed in the language of the default locale of the system where Oracle Identity Manager is installed. After closing the session timeout window and clicking any of the Administrative and User Console menu options, the Oracle Identity Manager Logout page is displayed and may also be displayed in the language of the default locale of the system where Oracle Identity Manager is installed.

16.5.4.3 Notes Field on the Task Details Page Not Localized For Reconciliation Tasks

In the Administrative and User Console, some text in the **Notes** field on the **Task Details** page may be displayed in English in non-English environments. Task instances that have the following names may encounter this issue:

- Reconciliation Update Received
- Reconciliation Insert Received
- Reconciliation Delete Received

16.5.4.4 English Characters Required for Some Attributes

Release 9.1.0.2 requires that you use only English characters for the following:

- Installation paths and directory names
- Host names
- E-mail addresses
- If used, external certificate names and certificate content
- The Administrative and User Console requires that you use only English characters for the E-mail Address fields on the **Create/Edit User**, **Account Profile**, and **Self-Registration** pages. In addition, when installing the Remote Manager, you must use only English characters for the Service Name on the **Configuration** page.

Refer to *Oracle Identity Manager Globalization Guide* for detailed information about the character restrictions for various components and attributes.

16.5.4.5 Some Information in Workflow Visualizer May Be Displayed as Box Characters

Some information may be displayed as box characters in the Workflow Visualizer of the Administrative and User Console due to a known limitation with Java Applets and globalized characters. The browser JVM displays only those characters that are in the current locale of the system where Oracle Identity Manager is installed. Globalized characters are displayed correctly in applets only if you set the browser to the same locale as the system where Oracle Identity Manager is installed.

16.5.4.6 Report in Non-English Environments Requires English Values for Filter Parameters

In non-English environments, the following report requires that the given filter parameter use only English values:

Report: Entitlement Summary

Filter parameter: Account Status

For example, filtering on Account Status in the Entitlement Summary report in non-English environments and using a translated version of the status *Active* will return nothing. You must use the English value *Active*.

16.5.4.7 Deployment Manager Import and Export Features Include an Untranslatable String

The Administrative and User Console's Deployment Manager import and export features use the Java AWT file dialog box that shows the `All Files (*.*)` string in the dialog box filter. The `All Files (*.*)` string is not translated for any locale and is displayed in English. This limitation is caused by the Java implementation, and the string cannot be translated. For more information, refer to the Sun Microsystems report for Bug ID 4152317 at

`http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4152317`

16.5.4.8 Names of Log Files for Oracle Identity Manager Utilities Do Not Include Time Stamp for Some Non-English Locales

When you use the Reconciliation Archival utility or Task Archival utility, or Oracle Identity Manager Database Validator, the name of the log files for some non-English environments may not include the time stamp. For example, for the Reconciliation Archival utility, you may see a log file that looks something like `Arch_Recon_____15_56.log` instead of `Arch_Recon_Wed_31_2007_03_31.log`.

16.5.4.9 Pre-Populate Adapter Error Messages Do Not Support Localized Display of Date and Time

The server-side date and time displayed in the error message on the Administrative and User Console when a pre-populate adapter error is encountered are not localized.

16.5.4.10 Some Asian Languages Not Displayed Correctly With Sun JDK 1.4

Some Asian languages may not be displayed correctly with Sun JDK 1.4 on the Deployment Manager if you launch it on a non-Asian Windows computer in spite of installing a language package on the client host. If you encounter this issue, install SUN Java Plug-in 1.5.

16.5.4.11 Names of IT Resource Parameters Displayed in the Administrative and User Console Are Not Localized

The names of IT resource parameters displayed on the "Manage IT Resources" pages of the Administrative and User Console are not localized.

16.5.4.12 Inconsistent Ordering of Names in Columns of Some Reports in Non-English Environments

In non-English environments, the ordering of first and last names in some reports does not correspond to the browser locale of the logged in user. Table 16–4 lists the reports and their columns in which first and last names may be displayed in inconsistent

order. You can modify the display of first and last names by modifying the stored procedures for these reports.

Table 16–4 Reports and Columns in Which First and Last Names May Be Inconsistently Ordered

Report	Sectional Header	Sectional Table	Display Format
Attestation Requests by Process	Reviewer	NA	FirstName LastName
Attestation Process List	NA	Reviewer	FirstName LastName
Policy List	NA	Created By	FirstName MiddleName LastName
Policy Detail	Created By	NA	FirstName LastName
Organization Structure	NA	Manager Name	FirstName MiddleName LastName
Requests Initiated	NA	Requester	FirstName MiddleName LastName
Requests Details by Status	Requester	NA	FirstName MiddleName LastName
Group Membership	Group Created By	NA	FirstName LastName
Task Assignment History	NA	Assigner User Name	FirstName LastName
Account Activity in Resource	NA	Manager Name	FirstName LastName
User Resource Access History	NA	Manager Name, Provisioned By	FirstName LastName
Group Membership History	Group Created By	NA	FirstName LastName

16.5.4.13 Error Message Displayed While Trying to Delete Menu Items Is Not Localized

While trying to delete a menu item, you may encounter an error message that is not localized.

16.5.4.14 Localization to the Chinese (Simplified), Chinese (Traditional), and Portuguese (Brazilian) Languages Not Supported

If Oracle Single Sign-On is used to provide authentication service to Oracle Identity Manager, then localization to the Chinese (Simplified), Chinese (Traditional), and Portuguese (Brazilian) languages is not supported. This is due to a known bug (6728226) in the Oracle Single Sign-On Plug-in deployed on Oracle HTTP Server.

16.5.4.15 Group Name Field Is Displayed in English

The Group Name Field label is always displayed in English, regardless of the locale you set.

Note: Changes made in the resource bundles are listed in Section 16.6, "Customizations."

16.5.4.16 Resource Bundle Entry for SoD Not Localized

The following label in the resource bundle is displayed in English on the console even when you use a locale other than English:

global.xlmetadata.request.object.SoDResult=SOD Result

In addition, the TopologyName IT resource parameter label has not been translated.

16.5.4.17 UI Text on Generic Technology Connector Pages of Administrative and User Console Is Not Localized for the Arabic Language

UI text on the Generic Technology Connector pages of the Administrative and User console is not localized for the Arabic language.

16.6 Customizations

The following sections list all the Oracle Identity Manager user interface (UI) related files that have been modified:

- Section 16.6.1, "Customizations in Release 9.1.0.2"
- Section 16.6.2, "Customizations in Release 9.1.0.1"

16.6.1 Customizations in Release 9.1.0.2

The following sections list items customized in release 9.1.0.2:

- Section 16.6.1.1, "JavaServer Pages"
- Section 16.6.1.2, "Java Files"
- Section 16.6.1.3, "Properties File"

16.6.1.1 JavaServer Pages

The following JavaServer pages have been added or modified in release 9.1.0.2:

SystemVerificationWeb\pages\FilterErrorPage.jsp

SystemVerificationWeb\error.jsp

SystemVerificationWeb\Login.jsp

SystemVerificationWeb\welcome.jsp

SystemVerificationWeb\index.jsp

web\tiles\common\tjspFooter.jsp

web\tiles\common\tjspHeader.jsp

web\tiles\util\CIWGenCstUtil.jsp

web\tiles\util\DualListComponent.jsp

web\tiles\util\ReportFormFieldsDisplay.jsp

web\tiles\util\TableGenerator.jsp

web\tiles\util\TablePagingLinks.jsp

web\tiles\util\tcGenerateCreateITResourceForm.jsp

web\tiles\util\tjspForm.jsp

web\tiles\util\tjspGenerateCreateForm.jsp

web\tiles\util\tjspGenerateCreateOrganizationForm.jsp

web\tiles\util\tjspGenerateCreateUserForm.jsp

web\tiles\util\tjspGenerateEditForm.jsp

web\tiles\util\tjspGenerateSchTaskEditForm.jsp

web\tiles\AccessPoliciesSearchResultsTiles.jsp

web\tiles\AccessPolicyAllChildFormsFooterTiles.jsp

web\tiles\AccessPolicyChildFormFooterTiles.jsp

web\tiles\AccessPolicyDetailsTiles.jsp

web\tiles\AccessPolicyEditPopupChildFormTilesInclude.jsp

web\tiles\AccessPolicyEditPopupFormTilesInclude.jsp

web\tiles\AccessPolicyEditSequencePopupChildFormTilesInclude.jsp

web\tiles\AccessPolicyFinalStepFooterTiles.jsp

web\tiles\AccessPolicyFirstStepFooterTiles.jsp

web\tiles\AccessPolicyFormChildTablesTiles.jsp

web\tiles\AccessPolicyFormsNoticeWizardFooterTiles.jsp

web\tiles\AccessPolicyObjectFormTilesInclude.jsp

web\tiles\AccessPolicyObjProcFormsWizardFooterTiles.jsp

web\tiles\AccessPolicyProcessFormTilesInclude.jsp

web\tiles\AccessPolicyProvideChildDataTilesInclude.jsp

web\tiles\AddNotesForTaskTiles.jsp

web\tiles\ApprovalTaskHistoryTiles.jsp

web\tiles\ApprovalTasksAssignedToManagedUsersTiles.jsp

web\tiles\ApprovalTasksReassignToGroupTiles.jsp

web\tiles\ApprovalTasksReassignToUserTiles.jsp

web\tiles\AssignAdminUsersTiles.jsp

web\tiles\AssignResourceAdministratorsTiles.jsp

web\tiles\AssignResourceAuditObjectivesTiles.jsp

web\tiles\AssignResourceAuthorizersTiles.jsp

web\tiles\AssociatedOrganizationsForResourceTiles.jsp

web\tiles\AssociatedUsersForResourceTiles.jsp

web\tiles\AttestationAdminAclTiles.jsp

web\tiles\AttestationAssignAdministratorsTiles.jsp

web\tiles\AttestationDashboardTiles.jsp

web\tiles\AttestationEditDetailsTilesInclude.jsp

web\tiles\AttestationEditUserScopeTiles.jsp

web\tiles\AttestationExecuteRequestDetailsTiles.jsp

web\tiles\AttestationResourceScopeEditTilesInclude.jsp

web\tiles\AttestationSearchResultsTiles.jsp
web\tiles\AttestationUpdateAdministratorsTiles.jsp
web\tiles\AttestationUserScopeEditTilesInclude.jsp
web\tiles\AttestationViewAttRequestDetailsTiles.jsp
web\tiles\AttestationViewDelegationPathTiles.jsp
web\tiles\AttestationViewDetailsTiles.jsp
web\tiles\AttestationViewExecutionDelegationPathTiles.jsp
web\tiles\AttestationViewRequestDetailsTiles.jsp
web\tiles\AttestationWizardConfirmationTiles.jsp
web\tiles\AttestationWizardExitTiles.jsp
web\tiles\AttestationWizardFinalStepFooterTiles.jsp
web\tiles\AttestationWizardFirstStepFooterTiles.jsp
web\tiles\AttestationWizardFirstTiles.jsp
web\tiles\AttestationWizardResourceScopeTilesInclude.jsp
web\tiles\AttestationWizardScheduleTilesInclude.jsp
web\tiles\AttestationWizardSuccessPageTiles.jsp
web\tiles\AttestationWizardUserScopeTilesInclude.jsp
web\tiles\AttestExecuteHistoryTiles.jsp
web\tiles\changePasswordTiles.jsp
web\tiles\CIWAssignAccessPermissionITResourceTiles.jsp
web\tiles\CIWAssignGroupITResourceTiles.jsp
web\tiles\CIWConfirmDeleteAttributeTiles.jsp
web\tiles\CIWConfirmScheduleTaskTiles.jsp
web\tiles\CIWConInstallTiles.jsp
web\tiles\CIWCreateITResIncludeTiles.jsp
web\tiles\CIWCreateITResourceConnectionTestTiles.jsp
web\tiles\CIWCreateITResourceParametersTiles.jsp
web\tiles\CIWCreateScheduledTaskIncludeTiles.jsp
web\tiles\CIWEditITResourceTiles.jsp
web\tiles\CIWITResourceDependenciesTiles.jsp
web\tiles\CIWManageITResourceTiles.jsp
web\tiles\CIWManageScheduledTaskTiles.jsp
web\tiles\CIWPreInstallStepsTiles.jsp
web\tiles\CIWSchTaskAttributesTiles.jsp
web\tiles\CIWSelectConTiles.jsp
web\tiles\CIWSetITAccessPermissionTiles.jsp
web\tiles\CIWStatusBarTiles.jsp

web\tiles\CIWUpdatePermissionsTiles.jsp

web\tiles\CIWVerifyITResCreationTiles.jsp

web\tiles\CIWVerifyScheduleTaskTiles.jsp

web\tiles\CIWViewITResourceTiles.jsp

web\tiles\CIWViewScheduledTaskTiles.jsp

web\tiles\ConfigureFormDataFlowTiles.jsp

web\tiles\ConfigureReconDataFlowTiles.jsp

web\tiles\ConfirmManualCompleteTasksTiles.jsp

web\tiles\ConfirmReassignTasksTiles.jsp

web\tiles\ConfirmReassignTaskTiles.jsp

web\tiles\ConfirmResponsesForTasksTiles.jsp

web\tiles\ConfirmRetryTasksTiles.jsp

web\tiles\CreateAccessPolicyDetailTiles.jsp

web\tiles\CreateAccessPolicySuccessTiles.jsp

web\tiles\CreateAccessPolicyTiles.jsp

web\tiles\CreateConnectorExitTiles.jsp

web\tiles\CreateGenConTiles.jsp

web\tiles\DelegateEntityWizardFooterTiles.jsp

web\tiles\DenyResourcesByAccessPolicyDetailTiles.jsp

web\tiles\DenyResourcesByAccessPolicyTiles.jsp

web\tiles\detailTasksReassignToGroupTiles.jsp

web\tiles\detailTasksReassignToUserTiles.jsp

web\tiles\DirectProvisionOrganizationWizard_ExitTiles.jsp

web\tiles\DirectProvisionOrganizationWizard_
ProvideChildProcessDataTilesInclude.jsp

web\tiles\DirectProvisionOrganizationWizard_
ProvideChildResourceDataTilesInclude.jsp

web\tiles\DirectProvisionOrganizationWizard_
ProvideParentProcessDataTilesInclude.jsp

web\tiles\DirectProvisionOrganizationWizard_
ProvideParentResourceDataTilesInclude.jsp

web\tiles\DirectProvisionOrganizationWizard_VerifyProcessDataTiles.jsp

web\tiles\DirectProvisionOrganizationWizard_VerifyResourceDataTiles.jsp

web\tiles\DirectProvisionUserWizard_ExitTiles.jsp

web\tiles\DirectProvisionUserWizard_ProvideChildProcessDataTilesInclude.jsp

web\tiles\DirectProvisionUserWizard_ProvideChildResourceDataTilesInclude.jsp

web\tiles\DirectProvisionUserWizard_ProvideParentProcessDataTilesInclude.jsp

web\tiles\DirectProvisionUserWizard_ProvideParentResourceDataTilesInclude.jsp

web\tiles\DirectProvisionUserWizard_VerifyProcessDataTiles.jsp

web\tiles\DirectProvisionUserWizard_VerifyResourceDataTiles.jsp

web\tiles\DisplayPasswordPolicyTiles.jsp

web\tiles\MyProxyConfirmProxyAssignTiles.jsp

web\tiles\MyProxyConfirmProxyRemoveTiles.jsp

web\tiles\MyProxyNoProxyDefinedTiles.jsp

web\tiles\MyProxyViewProxyAssignTilesInclude.jsp

web\tiles\MyProxyViewTiles.jsp

web\tiles\OpenTasksTiles.jsp

web\tiles\OrgResourceProfileConfirmRetryTasksTiles.jsp

web\tiles\OrgResourceProfileProvisioningTasksTiles.jsp

web\tiles\ProvideProvisioningDataNoticeTiles.jsp

web\tiles\ProvisionedResourcesForUserTiles.jsp

web\tiles\ProvisionResourcesByAccessPolicyDetailTiles.jsp

web\tiles\ProvisionResourcesByAccessPolicyTiles.jsp

web\tiles\ReportDisplayTiles.jsp

web\tiles\ReportTabularDisplayTiles.jsp

web\tiles\requestApprovalDetailTiles.jsp

web\tiles\requestCommentAddTiles.jsp

web\tiles\requestCommentTiles.jsp

web\tiles\requestDetailTiles.jsp

web\tiles\requestEntityDetailTilesInclude.jsp

web\tiles\requestEntityTiles.jsp

web\tiles\requestHistoryTiles.jsp

web\tiles\requestMoreInfoObjectTiles.jsp

web\tiles\requestMoreInfoRequestTiles.jsp

web\tiles\requestOrganizationProvisionDetailTiles.jsp

web\tiles\requestProvisionDetailTiles.jsp

web\tiles\requestResourceResolutionTiles.jsp

web\tiles\requestResourceTiles.jsp

web\tiles\requestTrackTiles.jsp

web\tiles\requestTrackTilesInclude.jsp

web\tiles\ResourceAdministratorsTiles.jsp

web\tiles\ResourceAuditObjectivesTiles.jsp

web\tiles\ResourceAuthorizersTiles.jsp

web\tiles\ResourceProfileConfirmRetryTasksTiles.jsp

web\tiles\ResourceProfileProvisioningTasksTiles.jsp

web\tiles\ResourceWorkflowsTiles.jsp

web\tiles\SearchGroupTiles.jsp

web\tiles\SelectGroupsForAccessPolicyDetailTiles.jsp

web\tiles\SelectGroupsForAccessPolicyTiles.jsp

web\tiles\SetResponseForSingleTaskTiles.jsp

web\tiles\SpecifyAdminPermissionsTiles.jsp

web\tiles\SpecifyGroupAliasTiles.jsp

web\tiles\SpecifyResponsesForTasksTiles.jsp

web\tiles\TaskDetailsTiles.jsp

web\tiles\TaskHistoryTiles.jsp

web\tiles\TaskShowAllStatusTiles.jsp

web\tiles\TasksReassignToGroupTiles.jsp

web\tiles\TasksReassignToUserTiles.jsp

web\tiles\tjspAccessPolicyExitTiles.jsp

web\tiles\tjspAccountOptionsTiles.jsp

web\tiles\tjspAddResourceObjectTiles.jsp

web\tiles\tjspAddTargetUserErrorTiles.jsp

web\tiles\tjspAddTargetUserTiles.jsp

web\tiles\tjspAssignConfirmContentTiles.jsp

web\tiles\tjspAssignConfirmTiles.jsp

web\tiles\tjspAssignListContentTiles.jsp

web\tiles\tjspAssignListTiles.jsp

web\tiles\tjspChallengeQuestionTiles.jsp

web\tiles\tjspChangeChallengeQuestionsTiles.jsp

web\tiles\tjspChangePasswordCompleteTiles.jsp

web\tiles\tjspChangePasswordTiles.jsp

web\tiles\tjspCompleteDraftRequestTiles.jsp

web\tiles\tjspConfirmAssignOrganizationAdministratorsStep1Tiles.jsp

web\tiles\tjspConfirmAssignOrganizationResourceObjectsStep1Tiles.jsp

web\tiles\tjspConfirmMoveSubOrganizationsStep1Tiles.jsp

web\tiles\tjspConfirmUpdateOrganizationAdministratorsStep1Tiles.jsp

web\tiles\tjspConformationLogoffTiles.jsp

web\tiles\tjspCreateGroupTilesInclude.jsp

web\tiles\tjspCreateOrganizationTilesInclude.jsp

web\tiles\tjspCreateRequestHomeTiles.jsp

web\tiles\tjspCreateRequestTiles.jsp

web\tiles\tjspCreateUserIncludeTiles.jsp

web\tiles\tjspCustomLookupFormTiles.jsp

web\tiles\tjspDisplayCommentTiles.jsp

web\tiles\tjspDisplayTrackSearchTiles.jsp

web\tiles\tjspEditGroupTilesInclude.jsp

web\tiles\tjspEditOrganizationConfirmationTilesInclude.jsp

web\tiles\tjspEditUserTilesInclude.jsp

web\tiles\tjspListOfTasksTiles.jsp

web\tiles\tjspLoginHelpTiles.jsp

web\tiles\tjspLogoffTiles.jsp

web\tiles\tjspLogoffTimeoutTiles.jsp

web\tiles\tjspLogonTiles.jsp

web\tiles\tjspLookupFormTiles.jsp

web\tiles\tjspModifyProfileSavedTiles.jsp

web\tiles\tjspModifyProfileTilesInclude.jsp

web\tiles\tjspMoveOrganizationUsersConfirmationTiles.jsp

web\tiles\tjspPasswordExpiredTiles.jsp

web\tiles\tjspProvideChallengeAnswersConfirmTiles.jsp

web\tiles\tjspProvideChallengeAnswersTiles.jsp

web\tiles\tjspProvideDataChildFormTilesInclude.jsp

web\tiles\tjspProvideDataParentFormTilesInclude.jsp

web\tiles\tjspRegistrationHelpTiles.jsp

web\tiles\tjspRemoveTargetUserConfirmationTiles.jsp

web\tiles\tjspRequestActResourceVerificationTiles.jsp

web\tiles\tjspRequestAdditionalInformationTilesInclude.jsp

web\tiles\tjspRequestCommentTiles.jsp

web\tiles\tjspRequestEditCommentTiles.jsp

web\tiles\tjspRequestMoreInfoTiles.jsp

web\tiles\tjspRequestScheduleFooterTiles.jsp

web\tiles\tjspRequestScheduleTilesInclude.jsp

web\tiles\tjspRequestSelectResourceTiles.jsp

web\tiles\tjspRequestSelectTargetTiles.jsp

web\tiles\tjspRequestShowResolutionTiles.jsp

web\tiles\tjspRequestSubmitErrorTiles.jsp

web\tiles\tjspRequestSubmitTiles.jsp

web\tiles\tjspRequestTargetTypeTiles.jsp

web\tiles\tjspRequestVerificationTiles.jsp

web\tiles\tjspRequestWizardAdminTiles.jsp

web\tiles\tjspRequestWizardExitTiles.jsp
web\tiles\tjspRequestWizardFooterTiles.jsp
web\tiles\tjspRequestWizardResourceTiles.jsp
web\tiles\tjspResetPasswordCompleteTiles.jsp
web\tiles\tjspResetPasswordTiles.jsp
web\tiles\tjspSearchGroupResultsTiles.jsp
web\tiles\tjspSearchUserResultsTiles.jsp
web\tiles\tjspSelfRegistrationNotAllowedTiles.jsp
web\tiles\tjspSelfRegistrationResultTiles.jsp
web\tiles\tjspSelfRegistrationTiles.jsp
web\tiles\tjspSelfRegTrackRequestTiles.jsp
web\tiles\tjspSetChallengeAnswersConfirmTiles.jsp
web\tiles\tjspSetChallengeAnswersTiles.jsp
web\tiles\tjspSetChallengeQuestionsTiles.jsp
web\tiles\tjspShowFormTilesInclude.jsp
web\tiles\tjspTaskApprovalDetailsTiles.jsp
web\tiles\tjspTaskApprovalViewTasksTiles.jsp
web\tiles\tjspTrackRequestTilesInclude.jsp
web\tiles\tjspUserMemberOfAssignTiles.jsp
web\tiles\tjspUserMemberOfDeleteTiles.jsp
web\tiles\tjspUserMemberOfTiles.jsp
web\tiles\tjspVerifyPasswordTiles.jsp
web\tiles\tjspVerifyUserIdTiles.jsp
web\tiles\tjspViewAdministratorsOrganizationDetailsTiles.jsp
web\tiles\tjspViewGroupDetailsTiles.jsp
web\tiles\tjspViewOrganizationDetailsTiles.jsp
web\tiles\tjspViewProfileTiles.jsp
web\tiles\tjspViewResourceProfileOrganizationDetailsTiles.jsp
web\tiles\tjspViewResourcesAllowedOrganizationDetailsTiles.jsp
web\tiles\tjspViewSubOrganizationDetailsTiles.jsp
web\tiles\tjspViewUsersOrganizationDetailsTiles.jsp
web\tiles\tjspWebAdminHomeTiles.jsp
web\tiles\tjspWizardFooterTiles.jsp
web\tiles\tjspWizardHeaderTiles.jsp
web\tiles\UpdateResourceAdministratorsTiles.jsp
web\tiles\UserDefinedChildFormEditTilesInclude.jsp
web\tiles\UserDefinedFormEditTilesInclude.jsp

web\tiles\UserGroupAdministratorsAssignTiles.jsp
web\tiles\UserGroupAdministratorsTiles.jsp
web\tiles\UserGroupAdministratorsUpdatePermissionsTiles.jsp
web\tiles\UserGroupAssignMembershipRulesTiles.jsp
web\tiles\UserGroupAssignMenuItemsTiles.jsp
web\tiles\UserGroupAssignReportsTiles.jsp
web\tiles\UserGroupConfirmAssignMembershipRulesTiles.jsp
web\tiles\UserGroupConfirmDeleteMembershipRulesTiles.jsp
web\tiles\UserGroupMembershipRulesTiles.jsp
web\tiles\UserGroupMembersTiles.jsp
web\tiles\UserGroupMenuItemsTiles.jsp
web\tiles\UserGroupPermissionsTiles.jsp
web\tiles\UserGroupPoliciesTiles.jsp
web\tiles\UserGroupReportsTiles.jsp
web\tiles\UserGroupUnassignedPermissionsTiles.jsp
web\tiles\UserGroupUnassignedPoliciesTiles.jsp
web\tiles\UserGroupUpdatePermissionsTiles.jsp
web\tiles\UserProxyConfirmProxyAssignTiles.jsp
web\tiles\UserProxyConfirmProxyRemoveTiles.jsp
web\tiles\UserProxyNoProxyDefinedTiles.jsp
web\tiles\UserProxyViewProxyAssignTilesInclude.jsp
web\tiles\UserProxyViewTiles.jsp
web\tiles\VerifyAdminUsersTiles.jsp
web\tiles\VerifyInfoForAccessPolicyTiles.jsp
web\pages\FilterErrorPage.jsp
web\layouts\tjspClassicLayout.jsp
web\layouts\tjspMenuNoStruts.jsp
web\layouts\tjspPopUpLayout.jsp
web\gc\ConnectorConfigurationTiles.jsp
web\gc\ConnectorImagePopUpTiles.jsp
web\gc\ConnectorMappingTiles.jsp
web\gc\CreateConnectorBasicTiles.jsp
web\gc\CreateConnectorExitTiles.jsp
web\gc\CreateConnectorSuccessPageTiles.jsp
web\gc\GenConnectorPopUpLayout.jsp
web\gc\GenConnectorTableGenerator.jsp
web\gc\manageConnectorExitTiles.jsp

web\gc\ModifyConnectorAddEditValidationsTiles.jsp

web\gc\ModifyConnectorConfirmationTiles.jsp

web\gc\ModifyConnectorFieldInfoTiles.jsp

web\gc\tjspPopUpLayout.jsp

web\gc\tjspWizardFooterTiles.jsp

web\gc\tjspWizardHeaderTiles.jsp

web\gc\ValidateFormConnectorTiles.jsp

web\dm\dmImportConfirmation.jsp

16.6.1.2 Java Files

The following Java files have been modified in release 9.1.0.2:

src\com\thortech\xl\webclient\actions\ApprovalsAction.java

src\com\thortech\xl\webclient\actions\AssociatedEntitiesForResourceAction.java

src\com\thortech\xl\webclient\actions\AttestationWizardAction.java

src\com\thortech\xl\webclient\actions\ConnectorInstallProcessAction.java

src\com\thortech\xl\webclient\actions\Constants.java

src\com\thortech\xl\webclient\actions\CreateAccessPolicyAction.java

src\com\thortech\xl\webclient\actions\CreateConnectorAction.java

src\com\thortech\xl\webclient\actions\CreateConnectorPopUpAction.java

src\com\thortech\xl\webclient\actions\DelegateEntityAction.java

src\com\thortech\xl\webclient\actions\DirectProvisionUserAction.java

src\com\thortech\xl\webclient\actions\ManageAccessPoliciesAction.java

src\com\thortech\xl\webclient\actions\ManageAccessPoliciesForm.java

src\com\thortech\xl\webclient\actions\ManageAttestationAction.java

src\com\thortech\xl\webclient\actions\ManageAttestationDashboardAction.java

src\com\thortech\xl\webclient\actions\ManageAttestationTaskAction.java

src\com\thortech\xl\webclient\actions\ManageITResourceAction.java

src\com\thortech\xl\webclient\actions\ManageScheduledTaskAction.java

src\com\thortech\xl\webclient\actions\MyProxyAction.java

src\com\thortech\xl\webclient\actions\MyRequestAction.java

src\com\thortech\xl\webclient\actions\OpenTasksAction.java

src\com\thortech\xl\webclient\actions\OrgResourceProfileProvisioningTasksAction
.java

src\com\thortech\xl\webclient\actions\ProvisionedResourcesForUserAction.java

src\com\thortech\xl\webclient\actions\RegistrationHelpPageAction.java

src\com\thortech\xl\webclient\actions\RequestAction.java

src\com\thortech\xl\webclient\actions\RequestApprovalDetailAction.java

src\com\thortech\xl\webclient\actions\RequestCommentAction.java

src\com\thortech\xl\webclient\actions\RequestProvisionDetailAction.java

src\com\thortech\xl\webclient\actions\RequestStatusHistoryAction.java

src\com\thortech\xl\webclient\actions\RequestTrackAction.java

src\com\thortech\xl\webclient\actions\RequestTrackForm.java

src\com\thortech\xl\webclient\actions\ResourceAdministratorsAction.java

src\com\thortech\xl\webclient\actions\ResourceAuthorizersAction.java

src\com\thortech\xl\webclient\actions\ResourceProfileProvisioningTasksAction.jav
a

src\com\thortech\xl\webclient\actions\SearchGroupAction.java

src\com\thortech\xl\webclient\actions\TaskDetailsAction.java

src\com\thortech\xl\webclient\actions\tcChangePasswordAction.java

src\com\thortech\xl\webclient\actions\tcForgetPasswordAction.java

src\com\thortech\xl\webclient\actions\tcLogonAction.java

src\com\thortech\xl\webclient\actions\tcLookupFieldAction.java

src\com\thortech\xl\webclient\actions\tcManageGroupAction.java

src\com\thortech\xl\webclient\actions\tcManageOrganizationAction.java

src\com\thortech\xl\webclient\actions\tcManageUserAction.java

src\com\thortech\xl\webclient\actions\tcRequestActResourceAction.java

src\com\thortech\xl\webclient\actions\tcRequestUserProvisionResourceAction.java

src\com\thortech\xl\webclient\actions\tcRequestWizardAction.java

src\com\thortech\xl\webclient\actions\tcSearchOrganizationAction.java

src\com\thortech\xl\webclient\actions\tcSearchUserAction.java

src\com\thortech\xl\webclient\actions\tcSelfRegistrationAction.java

src\com\thortech\xl\webclient\actions\tcSelfRegTrackRequestAction.java

src\com\thortech\xl\webclient\actions\tcSetChallengeQuestionsAction.java

src\com\thortech\xl\webclient\actions\tcTaskApprovalDetailsAction.java

src\com\thortech\xl\webclient\actions\tcTrackRequestAction.java

src\com\thortech\xl\webclient\actions\tcUserMemberOfAction.java

src\com\thortech\xl\webclient\actions\tcWebAdminHomeAction.java

src\com\thortech\xl\webclient\actions\tcWebAdminHomeForm.java

src\com\thortech\xl\webclient\actions\UserDefinedFormAction.java

src\com\thortech\xl\webclient\actions\UserGroupAccessPoliciesAction.java

src\com\thortech\xl\webclient\actions\UserGroupAdministratorsAction.java

src\com\thortech\xl\webclient\actions\UserGroupAdministratorsForm.java

src\com\thortech\xl\webclient\actions\UserGroupMembersAction.java

src\com\thortech\xl\webclient\actions\UserGroupMembershipRulesAction.java

src\com\thortech\xl\webclient\actions\UserGroupMembershipRulesForm.java

src\com\thortech\xl\webclient\actions\UserProxyAction.java

16.6.1.3 Properties File

The following properties have been introduced to support localization of text in release 9.1.0.2:

Properties Added in xldd.properties

global.security.filter=<\\s*,<\\s*/\\s*,\\s*>,\\s*/\\s*>,\\s*;

global.label.filterErrorPage=Filter Error Page

global.image.clientlogo=/images/client_logo.gif

global.image.xelleratelogo=/images/xellerate-trans-grey.gif

global.image.spacer=/images/spacer.gif

global.error.illegalInput=Illegal Script Tag or Characters

global.image.error=/images/reject.gif

global.error.illegalInputDesc=The User Input Field contains script tags or special characters that are not allowed.

global.label.back=Back

global.label.indicatesrequiredfield=Indicates required field

global.label.button.login=Login

global.label.button.clear=Clear

global.label.asterisk=*

global.label.mandatoryField=Indicates Required Field

global.label.loginErrorPage=Login Error Page

global.error.invalidInput=Invalid Username or Password

global.error.message=Please Contact Administrator

global.label.retry=Try Relogin

logon.message.toLogin=To log in, enter your User ID and password.

logon.label.userid=User ID:

logon.label.password=Password:

logon.label.button.login=Login

logon.label.button.clear=Clear

logoff.link=LOGOUT

Properties Added in xlWebadmin.properties

button.exit=Exit

global.label.offlineprovisioning=Off-line Provisioning

global.label.trustedsource=Trusted Source

global.label.sequencerecon=Sequence Recon

global.error.searchAdviceMaxCount=Please refine your search criteria. The search results reached the max account {0}.

global.xlmetadata.request.object.SoDResult=SOD Status

createuser.error.endDateBeforeCurrentDate=User End Date Error

createuser.error.endDateBeforeCurrentDateDesc=User End date cannot be past or today.

attestation.message.instruction=1. Select the search criteria to use by clicking the appropriate option.
2. Enter the search parameter values.
3. Click the Search button.

(New)trackrequest.message.instruction=1. Select the search criteria to use by entering values in the appropriate search fields .
 2. Enter the search parameter value(s).
 3. Enter comma separated values for searching multiple Request IDs and Resource Names .
 4. Select multiple status by pressing Ctrl button and selecting appropriate values of status.
 5. Click the Search button.

(Old)trackrequest.message.instruction=1. Select the search criteria to use by clicking the appropriate option.
2. Enter the search parameter values.
3. Click the Search button.

(Old)trackrequest.error.select=Specify the search criteria to use by selecting an option.

(new)trackrequest.error.select=Select atleast one search criteria.

users.provisionedResources.text.resourceOfflinedStatus.provision=Provisioning In Queue

users.provisionedResources.text.resourceOfflinedStatus.enable=Enable In Queue

users.provisionedResources.text.resourceOfflinedStatus.disable=Disable In Queue

users.provisionedResources.text.resourceOfflinedStatus.revoke=Revoke In Queue

(New)requestWizard.label.mustselect.resource.instanceForEachUserOrg=You must select at least one resource instance of each resource for each user or organization.

(Old)requestWizard.label.mustselect.resource.instanceForEachUserOrg=You must select at least one resource instance for each user or organization.

request.requestDetail.text.processedOfflinedStatus.pending.provision=Provisioning In Queue

request.requestDetail.text.processedOfflinedStatus.pending.enable=Enable In Queue

request.requestDetail.text.processedOfflinedStatus.pending.disable=Disable In Queue

request.requestDetail.text.processedOfflinedStatus.pending.revoke=Revoke In Queue

request.button.deletecomment=deleteComment

requests.requestComments.message.delete=Delete

generic.dualList.error.badResourceSelection=Bad Resource Selection made

generic.dualList.error.badUserSelection=Bad User Selection made

(New)UserGroupMembers.error.noGroupMembersGroupsFound=There are no member groups in this group.

(Old)UserGroupMembers.error.noGroupMembersGroupsFound=There are member groups in this group.

global.error.invalidLookupValue=Invalid lookup value

UserGroupMembershipRules.label.filterByRuleName=Filter By Rule Name

UserGroupMembershipRules.button.SearchByRuleName=Search

UserGroupMembershipRules.button.SearchByUnassignedRuleName=Find

UserGroupAdministrators.error.cannotDeleteGroupWithMemberUsersSubgroups=Delete only if there are no users/group. Remove the users/group associated with the group, and then try again.

UserGroupAdministrators.error.cannotDeleteGroupWithAccessPolicy=Delete only if there are no access policy associated with the group. Remove the group from assoicated access policy, and then try again.

(New)passwordPolicy.message.complexPassword= Password must meet the following complexity criteria:
Must be at least six characters long.
Must belong to at least three out of five categories.
Uppercase alphabetic characters (A-Z)
Lowercase alphabetic characters (a-z)
Numerals (0-9)
Non-alphanumeric characters (for example: !, $, #, or %)
Unicode characters
Must not contain any of user ID, first name or last name when their length is larger than 2.

(Old)passwordPolicy.message.complexPassword= Password must meet the following complexity criteria:
Must be at least six characters long.
Must belong to at least three out of five categories.
Uppercase alphabetic characters (A-Z)
Lowercase alphabetic characters (a-z)
Numerals (0-9)
Non-alphanumeric characters (for example: !, $, #, or %)
Unicode characters
Must not contain three or more continuous characters from the user ID or full name.

tooltip.request.deleteRequestComments=Delete Request Comment

orm.integrated.feature.disabled=Feature available on ORM Console

Properties Added in xlDefaultAdmin.properties

global.locales.ar=ar

global.request.groups.selectedListDisplayFields.lables=

global.request.groups.selectedListDisplayFields=

global.emailValidate.filter=([\\w!#$%&'*+-/=?^_
`{|}~])+[@](\\w|[-]|[.])+[.]([a-zA-Z0-9])+

request.requestTrack.defaultFromDays=30

Properties Added in xlRichClient.properties

dm.import.message.substitutionFailed.ObjectDoesNotSupport=Object {0} {1} does not support substitutions.

16.6.2 Customizations in Release 9.1.0.1

The following sections list items customized in release 9.1.0.1:

- Section 16.6.2.1, "JavaServer Pages"
- Section 16.6.2.2, "Java Files"
- Section 16.6.2.3, "Properties File"

16.6.2.1 JavaServer Pages

The following JavaServer pages have been modified in release 9.1.0.1:

ModifyConnectorFieldInfoTiles.jsp

tjspMenuNoStruts.jsp

DualListComponent.jsp

ReportFormFieldsDisplay.jsp

tjspForm.jsp

tjspGenerateEditForm.jsp

AssignResourceAdministratorsTiles.jsp

CIWAssignGroupITResourceTiles.jsp

CIWEditITResourceTiles.jsp

CIWViewITResourceTiles.jsp

CIWViewScheduledTaskTiles.jsp

ConfigureReconDataFlowTiles.jsp

DirectProvisionUserWizard_ProvideChildProcessDataTilesInclude.jsp

DirectProvisionUserWizard_ProvideParentProcessDataTilesInclude.jsp

MyProxyViewProxyAssignTilesInclude.jsp

OrgResourceProfileProvisioningTasksTiles.jsp

requestDetailTiles.jsp

requestTrackTilesInclude.jsp

ResourceAdministratorsTiles.jsp

ResourceAuthorizersTiles.jsp

ResourceProfileProvisioningTasksTiles.jsp

SearchGroupTiles.jsp

SelectGroupToAssignToTaskTiles.jsp

SelectUserToAssignToTaskTiles.jsp

tjspConfirmAssignOrganizationAdministratorsStep1Tiles.jsp

tjspConfirmUpdateOrganizationAdministratorsStep1Tiles.jsp

tjspLogoffTimeoutTiles.jsp

tjspLogonTiles.jsp

tjspProvideChallengeAnswersConfirmTiles.jsp

tjspSearchOrganizationTiles.jsp

tjspSearchUserTiles.jsp

tjspSelfRegTrackRequestTiles.jsp

tjspSetChallengeAnswersConfirmTiles.jsp

tjspSetChallengeAnswersTiles.jsp

tjspSetChallengeQuestionsTiles.jsp

tjspUserMemberOfTiles.jsp

tjspVerifyUserIdTiles.jsp

tjspViewAdministratorsOrganizationDetailsTiles.jsp

UpdateResourceAdministratorsTiles.jsp

UserDefinedChildFormEditTilesInclude.jsp

UserDefinedFormEditTilesInclude.jsp

UserGroupAdministratorsAssignTiles.jsp

UserGroupAdministratorsTiles.jsp

UserGroupAdministratorsUpdatePermissionsTiles.jsp

UserGroupPermissionsTiles.jsp

UserGroupPoliciesTiles.jsp

UserGroupReportsTiles.jsp

UserGroupUnassignedPermissionsTiles.jsp

UserGroupUpdatePermissionsTiles.jsp

UserProxyNoProxyDefinedTiles.jsp

UserProxyViewProxyAssignTilesInclude.jsp

16.6.2.2 Java Files

The following Java files have been modified in release 9.1.0.1:

AssociatedEntitiesForResourceAction.java

CreateConnectorAction.java

CreateConnectorPopUpAction.java

CreateConnectorPopUpForm.java

DirectProvisionOrganizationAction.java

DirectProvisionUserAction.java

LoadDeploymentUtilityAction.java

ManageAccessPoliciesAction.java

ManageAttestationAction.java

ManageAttestationTaskAction.java

ManageITResourceAction.java

ManageITResourceForm.java

ManageScheduledTaskAction.java

ManageScheduledTaskForm.java

OpenTasksAction.java

OrgResourceProfileProvisioningTasksAction.java

OrgResourceProfileProvisioningTasksForm.java

ProvisionedResourcesForUserAction.java

RegistrationHelpPageAction.java

RequestAction.java

RequestTrackAction.java

ResourceAdministratorsAction.java

ResourceAdministratorsForm.java

ResourceAuthorizersAction.java

ResourceAuthorizersForm.java

ResourceProfileProvisioningTasksAction.java

ResourceProfileProvisioningTasksForm.java

ResourceWorkflowsAction.java

SearchGroupAction.java

SearchResourceAction.java

tcAction.java

tcChangePasswordAction.java

tcForgetPasswordAction.java

tcITResourceLookupFieldAction.java

tcLogonAction.java

tcLogonForm.java

tcLookupFieldAction.java

tcManageGroupAction.java

tcManageOrganizationAction.java

tcManageOrganizationForm.java

tcManageUserAction.java

tcModifyProfileAction.java

tcRequestProvisionResourceAction.java

tcRequestUserProvisionResourceAction.java

tcRequestWizardAction.java

tcSearchOrganizationAction.java

tcSearchUserAction.java

tcSelfRegistrationAction.java

tcSelfRegTrackRequestAction.java

tcSetChallengeQuestionsAction.java

tcUserMemberOfAction.java

tcUserMemberOfForm.java

UserDefinedFormAction.java

UserGroupAccessPoliciesAction.java

UserGroupAdministratorsAction.java

UserGroupAdministratorsForm.java

UserGroupMembersAction.java

UserGroupMembershipRulesAction.java

UserGroupMenuItemsAction.java

UserGroupPermissionsAction.java

UserGroupPermissionsForm.java

UserGroupReportsAction.java

UserGroupReportsForm.java

16.6.2.3 Properties File

> **Note:** If you have modified any of the properties files on your Oracle Identity Manager installation, then create a backup of those files before you overwrite the files with the ones from the PATCH directory. After you copy the files, make the same modifications in the newly copied files.

The following properties have been modified in the resource bundle for the Diagnostic Dashboard:

xldd.vdtest.xlSQL_display1=One or more 'Microsoft SQL Server Driver for JDBC' files were not found.

xldd.dftest.tValidateSQLServerDefinition_description=Oracle Identity Manager requires 'Microsoft SQL Server Driver for JDBC' to work with Microsoft SQL Server. This test verifies if these JDBC drivers are available to the application server.

xldd.dftest.sqlServer_description=Oracle Identity Manager requires 'Microsoft SQL Server Driver for JDBC' to work with Microsoft SQL Server. This test verifies if these JDBC drivers are available to the application server.

xldd.vdtest.driverNotFound=One or more 'Microsoft SQL Server Driver for JDBC' files were not found.

xldd.bctest.errors.itResourceName=The IT Resource Instance is not available. Enter a valid IT Resource Instance Name.

The following properties have been modified in the resource bundle for Oracle Identity Manager:

global.label.calendar=Select to access date picker

global.error.duplicateFormData=The entered form data already exists.

global.error.duplicateFormDataAdvice=Please select another field value.

user.label.filterByGroupName=Filter By Group Name

user.button.searchMemberGroupName=Search

UserGroupPolicies.error.noPermsToDelete=No Permission To Delete

UserGroupPolicies.error.noPermsToDeleteDescription=You don't have rights to Delete one or more selected Access policies.

label.atetstation.comment=Reassigning Attestation Process as Grace Period has expired. the reviewer for this Process was

trackrequest.error.selectUser=Please Specify Username.

AboutXl.message.header=© Oracle Corporation

resourceMgmt.resourceAdministrators.error.noAdminFoundWithSearchCriteria=No Administrator found with given search criteria

resourceMgmt.resourceAdministrators.button.searchAssignedGroup=Find

resourceMgmt.resourceAdministrators.button.searchUpdateGroup=Go

resourceMgmt.resourceAuthorizers.button.searchAssignedGroup=Find

resourceMgmt.resourceWorkflows.label.removeKeyCaseInsensitiveField=Click to remove the setting of case insensitive

resourceMgmt.resourceWorkflows.label.addKeyCaseInsensitiveField=Click to add the setting of case insensitive

UserGroupPermissions.message.FilterByPermissionName=Filter by Permission Name:

UserGroupPermissions.message.button.searchAssignedPermissionName=Find

UserGroupPermissions.message.button.searchUpdatePermissionName=Search

UserGroupPermissions.message.button.searchUnAssignedPermissionName=Go

manageOrganization.label.filterByGroupName=Filter By Group Name

manageOrganization.button.searchAssignedGroup=Search

manageOrganization.button.searchUnassignedGroup=Find

manageOrganization.button.searchUpdatePermissionGroup=Go

UserGroupReports.error.noPermsToDelete=No Permission to Delete.

UserGroupReports.error.noPermsToDeleteDescription=You have no permission to delete one or more selected reports.

UserGroupMembershipRules.error.noPermsToDelete=No Permision to Delete.

UserGroupMembershipRules.error.noPermsToDeleteDescription=You don't have rights to Delete one or more Rules.

UserGroupAdministrators.label.filterByGroupName=Filter By Group Name

UserGroupAdministrators.button.SearchByGroupName=Search

UserGroupAdministrators.button.SearchByUnassginedGroupName=Find

UserGroupAdministrators.button.SearchByUpdatePermissionGroupName=Go

UserGroupAdministrators.error.cannotDeleteGroup=Can not delete this group.

UserGroupAdministrators.error.noPermsToDelete=No Permision to Delete.

UserGroupAdministrators.error.noPermsToDeleteDescription=You don't have rights to Delete one or more selected Administrative Groups.

global.FormInfoDesc.Lookup.Change-self-password-menu-item=Change Self Password menu item

global.FormInfoDesc.Lookup.Create-generic-connector=Create Generic Technology Connector menu item

global.FormInfoDesc.Lookup.Manage-generic-connector=Manage Generic Technology Connector menu item

modifyConnector.label.caseInsensitive=Case-Insensitive

global.button.stopexecution=Stop Execution

manageITResource.resourceAdministrators.button.search=Search Group

manageITResource.resourceAdministrators.button.find=Find Group

manageITResource.resourceAdministrators.button.go=Filter Group

manageITResource.resourceAdministrators.label.filterByGroupName=Filter By Group Name

manageITResource.resourceAdministrators.error.adminNotFound=There are no administrators associated with this It Resource

global.resultSet.Form~Information.Description.Create~generic~connector=Create Generic Technology Connector menu item

global.resultSet.Form~Information.Description.Manage~generic~connector=Manage Generic Technology Connector menu item

global.resultSet.Form~Information.Description.Change~self~password~menu~item= Change Self Password menu item

16.7 Related Documents

For more information, see the other documents in the Oracle Identity Manager documentation set for release 9.1.0.2 at

http://www.oracle.com/technology/documentation/oim1014.html