Oracle® Fusion Middleware

Identity Management Release Notes

11*g* Release 2 (11.1.2.2)

E56629-04

February 2015

ORACLE®

Oracle Fusion Middleware Identity Management Release Notes, 11*g* Release 2 (11.1.2.2)

E56629-04

Contents

3 Upgrade and Migration Issues for Oracle Identity and Access Management

6 Oracle Entitlements Server

7 Oracle Adaptive Access Manager

11 Oracle Identity Management Integration

12 Oracle Fusion Middleware on IBM WebSphere

Preface

This preface includes the following sections:

Audience

This document is intended for users of Oracle Fusion Middleware 11*g* Release 2 (11.1.2).

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see these Oracle resources:

- *Oracle Fusion Middleware Documentation on Oracle Fusion Middleware Disk 1*
- *Oracle Fusion Middleware Documentation Library 11g Release 1 (11.1.1)*
- Oracle Technology Network at http://www.oracle.com/technology/index.html

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
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.

1 Introduction

This chapter introduces Oracle Fusion Middleware Identity Management Release Notes, 11g Release 2 (11.1.2.2). 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/technetwork/indexes/documentation/index.html

1.2 Purpose of this Document

This document contains the release information for Oracle Fusion Middleware 11g Release 2 (11.1.2.2). It describes differences between Oracle Fusion Middleware and its documented functionality.

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

1.3 System Requirements and Specifications

Oracle Fusion Middleware installation and configuration will not complete successfully unless users meet the hardware and software pre-requisite requirements before installation.

For more information, see "Review System Requirements and Specifications" in the *Oracle Fusion Middleware Installation Planning Guide*

1.4 Certification Information

This section contains the following:

1.4.1 Where to Find Oracle Fusion Middleware Certification Information

The latest certification information for Oracle Fusion Middleware 11g Release 2 (11.1.2.2) is available at the Oracle Fusion Middleware Supported System Configurations Central Hub:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

1.4.2 Certification Exceptions

This section describes known issues (exceptions) and their workarounds that are associated with Oracle Fusion Middleware 11g certifications. For a list of known issues that are associated with specific Oracle Fusion Middleware 11g Release 2 (11.1.2.2) components, see the Release Notes for the specific Oracle Fusion Middleware 11g Release 2 (11.1.2.2) component.

This section contains the following topics:

1.4.2.1 Certification Information for Oracle Fusion Middleware 11g R2 with Oracle Database 11.2.0.1

If you choose to configure Oracle Internet Directory with Database vault, do the following:

1. Apply patch 8897382 to fix bug 8897382.

   Note: The following workaround is required only if the Oracle Fusion Middleware version is 11.1.1.1.0 (11gR1). This issue will be fixed in 11.1.1.2.0.

2. Apply the workaround for bug 8987186 by editing `<OH>/ldap/datasecurity/dbv_oid_command_rules.sql` file and find the following declaration:

```
/declare
 begin
      dvsys.dbms_macadm.CREATE_COMMAND_RULE(
      command => 'CONNECT'
      ,rule_set_name => 'OID App Access'
      ,object_owner => '%'
      ,object_name => '%'
      ,enabled => 'Y');
```

```
 commit;
end;/
```

and change the line that is indicated in **bold**:

```
/declare
 begin
      dvsys.dbms_macadm.CREATE_COMMAND_RULE(
      command => 'CONNECT'
      ,rule_set_name => 'OID App Access'
      ,object_owner => '%'
      ,object_name => '%'
      ,enabled => 'Y');
 commit;
end;/
```

1.4.2.2 Excel Export Issue on Windows Vista Client

Vista prevents applets from creating files in the local file system if the User Account Control (UAC) system is turned on. You can experience this problem if you have the UAC setting enabled on Vista and if you use a component like Discoverer Plus. If you start Discoverer Plus and if you try exporting a worksheet to a specified directory, the exporting succeeds but you cannot see the exported file in the directory. The available workarounds is to disable UAC and set protection mode to OFF. Refer to Bugs 8410655 and 7328867 for additional information.

1.4.2.3 Oracle Forms and Oracle Reports 11*g* Installer Issues In Windows Vista and Windows XP

Only the design-time environments (Builders) are supported for Oracle Forms and Oracle Reports in Windows Vista and Windows XP.However, in the Configure Components screen in the Oracle Installer, the Server Components, Management Components and System Components are selected by default, but Developer Tools is deselected. When installing Oracle Forms Builder, or Oracle Reports Builder on Windows Vista and Windows XP computers, you must:

- Select **Developer Tools**, such as Oracle Forms Builder or Oracle Reports Builder. Their respective server components are automatically selected.
- Deselect all System Components and Management Components.
- Deselect the Portal and Discoverer tools. Two of the Discoverer components – Discoverer Admin and Discoverer Desktop – will be installed even if you do not select Discoverer in the Configure Components screen of the installer. This is the correct, expected behavior in 11.1.1.1.0.

For Oracle Forms, since the System Components including Oracle HTTP Server are not supported in Windows Vista and Windows XP, the following features are not supported:

1. Oracle Forms and Reports integration.
2. The creation of virtual directories.

1.4.2.4 Restrictions on Specific Browsers

The following browser issues have been observed.

1.4.2.4.1 Internet Explorer Browser Goes Blank When Adding Portlets in Oracle Webcenter If you add portlets in Oracle Webcenter by using Internet Explorer, then the page can go blank. When it does go blank, a download message appears on the browser's status bar. However, nothing is downloaded and the browser remains blank untill you click

the browser's back button. If this problem occurs, the portlets will appear only when you hit the browser's back button. This issue does not occur with Firefox.

As a workaround, click the browser's back button.

1.4.2.4.2 Unable to View the Output of a JSPX Page in Internet Explorer 7

When a JSPX page is deployed and is then accessed using Internet Explorer 7 (IE7), the XHTML source is displayed instead of the page contents. This occurs in both normal and osjp.next modes.

The workaround is to instruct application users to access the application with Firefox or Safari.

1.4.2.4.3 Unable to View the Output of SVG files in Internet Explorer 7

When a page using Scalar Vector Graphics is deployed and is then accessed using Internet Explorer 7 (IE7), the source is displayed instead of the page's graphic contents. This occurs in both normal and osjp.next modes.

The workaround for this issue is that Application developers should avoid using SVG graphics in their applications, as it is not natively supported in IE7. If they are used, a warning similar to the following should be added:

All current browsers, with the exception of Internet Explorer, support SVG files. Internet Explorer requires a plug-in to display SVG files. The plug-ins are available for free, for example, the Adobe SVG Viewer at http://www.adobe.com/svg/viewer/install/.

1.4.2.4.4 Java Plugin for Discoverer Plus Not Downloaded Automatically on Firefox

When you attempt to connect to Discoverer Plus by using the Mozilla Firefox browser on a computer that does not have Java 1.6 installed, Firefox does not download the JRE 1.6 plug-in automatically. Instead, Firefox displays the following message: "Additional plugins are required to display this page..."

The workaround is to download the JRE 1.6 plug-in by clicking the Install Missing Plugin link to install it manually.

1.4.3 JMSDELIVERYCOUNT Is Not Set Properly

When using AQ JMS with Oracle Database 11.2.0.1, JMXDELIVERYCOUNT is not set correctly.

The workaround is to apply patch 9932143 to Oracle Database 11.2.0.1. For more information, contact Oracle Support.

1.4.4 Viewer Plugin Required On Safari 4 To View Raw XML Source

You need a Safari plugin to view raw XML. If there is no plugin installed, you will see unformatted XML which will be difficult to read. This is because Safari applies a default stylesheet, which only displays the text nodes in the XML document.

As a workaround, go to **View > View Source** in the Safari menu bar to see the full XML of the metadata document. Also, selecting **File > Save** and choosing **XML Files** as the file type, will correctly save the XML metadata file with all the markup intact.

1.5 Downloading and Applying Required Patches

After you install and configure Oracle Fusion Middleware 11g Release 2 (11.1.2.2), there might be cases where additional patches are required to address specific known issues.

Patches for Oracle Fusion Middleware 11*g* are available from My Oracle Support:

`https://myoraclesupport.com/`

Table 1-1 lists some of the specific Oracle Fusion Middleware patches that were available at the time these release notes were published.

Table 1–1 Patches Required to Fix Specific Issues with Oracle Fusion Middleware ***11g***

Oracle Fusion Middleware Product or Component	Bug/Patch Number	Description
Oracle Virtual Directory	16943171	This patch is critical if you are using Oracle Unified Directory in active-active mode, as shown in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*. Failure to apply this patch might result in data inconsistency in the event of a failover.
Oracle IDM Tools	17008132	This patch corrects ACI issues affecting Oracle Unified Directory.
Oracle WebLogic Server	14182177	Fixes the error: `StuckThreads in AdminServer`.
Oracle Unified Directory	18461856	Fixes "Run LDAP User Create and Update Reconciliation job" failure.
Oracle Identity Management	18333689	Bundle Patch 11.1.2.2.1

There are mandatory patches that you must apply if you are enabling SSL on Oracle HTTP Server. For more information, see Section 2.1.3, "Mandatory Patches for Enabling SSL on Oracle HTTP Server"

In addition, there are some mandatory patches that must be applied for installing and configuring Oracle Identity Manager. For information about these patches, see Section 2.2.2, "Mandatory Patches Required for Installing Oracle Identity Manager"

Along with the Oracle Identity Manager patches, some of the Oracle Database versions require patches. To identify the patches required for Oracle Identity Manager 11*g* Release 2 (11.1.2) configurations that use Oracle Databases, see Section 10.1, "Patch Requirements"

1.6 Licensing Information

Licensing information for Oracle Fusion Middleware is available at:

`http://oraclestore.oracle.com`

Detailed information regarding license compliance for Oracle Fusion Middleware is available at:

`http://www.oracle.com/technetwork/middleware/ias/overview/index.html`

2

Installation and Configuration Issues for Oracle Identity and Access Management

This chapter describes issues associated with the installation and configuration process of Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0). It includes the following sections:

- Section 2.1, "General Issues and Workarounds"
- Section 2.2, "Installation Issues and Workarounds"
- Section 2.3, "Configuration Issues and Workarounds"

2.1 General Issues and Workarounds

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

- Section 2.1.1, "Simple Security Mode Does Not Work on AIX"
- Section 2.1.2, "Error Displayed in the Oracle Access Management Managed Server Logs"
- Section 2.1.3, "Mandatory Patches for Enabling SSL on Oracle HTTP Server"
- Section 2.1.4, "Optional: Setting log levels to SEVERE for WebLogic Servers in Identity and Access Management Domain"
- Section 2.1.5, "Modifying the Server Side Property for Oracle Identity Manager"
- Section 2.1.6, ""Identity and Access" Link Missing from the Enterprise Manager Console on Windows 2012"
- Section 2.1.7, "OAM Server Startup Fails After Applying WebLogic Server Patches"
- Section 2.1.8, "Applications Will Not Start After WebLogic Server is Updated"

2.1.1 Simple Security Mode Does Not Work on AIX

On AIX, the Simple security mode does not work with Oracle Access Management Server 11.1.2.

Workaround: Use either the `Open` or `Cert` security mode.

2.1.2 Error Displayed in the Oracle Access Management Managed Server Logs

When you try to edit the policy in the Oracle Access Management administration console log, the following error is displayed in the Oracle Access Management managed server logs:

```
<oracle.jps.policymgmt> <JPS-10606>
<Failed to distribute policy to PDP OracleIDM for catch exception
oracle.security.jps.service.policystore.PolicyStoreException: JPS-04028:
Application with name
"cn=OAM11gApplication,cn=jpsXmlFarm,cn=JPSContext,cn=jpsXmlRoot" does not
exist..>
```

This exception is displayed every ten minutes even when the server is idle.

Workaround:

1. Remove the following properties from the `jps-config.xml` file after the installation with `-C` option from `pdp.service` instance properties.

   ```
   <property
   name="oracle.security.jps.pdp.AuthorizationDecisionCacheEnabled"
   value="false"/>
              <property
   name="oracle.security.jps.ldap.policystore.refresh.interval" value="10000"/>
   ```

2. Add the following new property to `pdp.service` instance properties:

   ```
   <property
   name="oracle.security.jps.pd.client.PollingTimerInterval" value="10"/>
   ```

   The **value** is in seconds, set the appropriate value as required by Oracle Access Management. The changes must be made only for Oracle Identity Management installs like Oracle Identity Manager or Oracle Access Manager.

   The following is an example of a `pdp.service` instance in the `jps-config.xml` file after running the `configSecurityStore` command.

   ```
   <serviceInstance name="pdp.service" provider="pdp.service.provider">
              <description>Runtime PDP service instance</description>
              <property
   name="oracle.security.jps.runtime.pd.client.policyDistributionMode"
   value="mixed"/>
              <property name="oracle.security.jps.runtime.instance.name"
   value="OracleIDM"/>
              <property name="oracle.security.jps.runtime.pd.client.sm_name"
   value="OracleIDM"/>
              <property
   name="oracle.security.jps.pdp.AuthorizationDecisionCacheEnabled"
   value="false"/>
              <property name="oracle.security.jps.policystore.refresh.enable"
   value="true"/>
              <property
   name="oracle.security.jps.ldap.policystore.refresh.interval" value="10000"/>
          </serviceInstance>
   ```

2.1.3 Mandatory Patches for Enabling SSL on Oracle HTTP Server

This section describes the mandatory patches to be downloaded and installed for enabling SSL on Oracle HTTP Server.

> **Note:** For information about any additional patches that you must apply, see Section 1.5, "Downloading and Applying Required Patches"

Platform	Patch
Solaris (64 bit)	14264658
Microsoft Windows x64 (64 bit)	14264658
Solaris x86-64 (64 bit)	14264658
IBM AIX (64 bit)	14264658
Linux x86-64	14264658

To download the patches, do the following:

1. Log in to My Oracle Support.
2. Click **Patches & Updates**.
3. Select **Patch name or Number**.
4. Enter the patch number.
5. Click **Search**.
6. Download and install the patch.

2.1.4 Optional: Setting log levels to SEVERE for WebLogic Servers in Identity and Access Management Domain

To change log levels to `SEVERE`, do the following:

1. `Logging.xml` must have `level=SEVERE` for all log handlers and loggers (`OAM_Server1, OIM_Server1, SOA`).
2. Log in to `Admin Console http://Hostname:port/console`.
3. Click **Lock and Edit** to unlock the domain.)
4. Click **Servers** link.
5. Click on the server you want to make changes to.
6. Click **Logging**.
7. Click **Advanced**.
8. Do the following to change the log levels in **Message destination(s):**

Message destinations	Severity Level Desired	Default Setting
Log File	warning	Trace
Standard out	error	Notice
Domain log broadcaster	error	Notice
Memory Buffer Severity	error	Blank

9. Click **Save**.
10. Click **Activate Changes**
11. Restart Servers

Repeat the process for all desired servers (`OAM_Server1, OIM_Server1, SOA`).

2.1.5 Modifying the Server Side Property for Oracle Identity Manager

The `scheduler.disabled` system property is required if you want to control scheduler start or stop on a clustered setup.The `scheduler.disabled` system property must be set to `true` if you don't want to start scheduler service on that node of cluster and vice-versa.

Following are the steps to modify the `scheduler.disabled` system property using Weblogic console:

1. Log in to the Oracle WebLogic Administration Console using the WebLogic administrator credentials.
2. Under **Domain Structure**, click **Environment > Servers**. The Summary of Servers page is displayed.
3. Click on the Oracle Identity Manager server name (for example, `oim_server1`). The Settings for `oim_server1` is displayed.
4. Click **Configuration > Server Start**.
5. In the **Arguments** text box, change the existing property `scheduler.disabled = false/true`.
6. Click **Save**.
7. Click **Activate Changes**.
8. Restart the Oracle Identity Manager Managed Server.

Note: After you modify the `scheduler.disabled` system property, you must start the Managed Server using the Node Manager.

2.1.6 "Identity and Access" Link Missing from the Enterprise Manager Console on Windows 2012

When you install Oracle Identity and Access Management on Windows 2012, the **Identity and Access** link does not appear on the Enterprise Manager Console.

Workaround:

As a workaround, you must complete the following steps after configuring Oracle Identity Manager:

1. Copy the *ORACLE_HOME*`\server\setup\templates\wls\oim-mbeans.xml` file to the *DOMAIN_HOME*`\config\fmwconfig\mbeans` directory.
2. Create a new directory called `oim` at the following location:

   DOMAIN_HOME`\config\fmwconfig\mbeans`
3. Copy the *ORACLE_HOME*`\server\setup\templates\wls\oim-clustermbean.jar` file to the *DOMAIN_HOME*`\config\fmwconfig\mbeans\oim` directory.
4. Restart the OIM server.

2.1.7 OAM Server Startup Fails After Applying WebLogic Server Patches

For releases 11.1.1.5 to 11.1.2.x, after applying WebLogic Server patches using the Patchset Assistant tool, if you try to create a new OAM domain, and try to start the

OAM servers, the OAM Administration Server and OAM Managed Servers fails to start.

The following error is displayed:

```
Patched WLS Will Break Access to OAM Policy Store - "OAMSSA-06252:
The policy store is not available;"
```

Workaround:

As a workaround, complete the following steps:

1. Using a text editor, open the *DOMAIN_HOME/bin*/SetDomainEnv.cmd file (on Windows) or *DOMAIN_HOME**bin*\SetDomainEnv.sh (on UNIX), and add the following lines:

   ```
   WLS_PATCHVERSION=WLS_version_no
   export $WLS_PATCHVERSION
   ```

   where *WLS_version_no* is wls_patch1035 if you are using Oracle WebLogic Server 10.3.5, or *WLS_version_no* is wls_patch1036 if you are using Oracle WebLogic Server 10.3.6.

2. Search for JAVA_PROPERTIES in the SetDomainEnv.cmd file (on Windows) or SetDomainEnv.sh (on UNIX), and add the following:

   ```
   JAVA_PROPERTIES="-Dplatform.home=${WL_HOME} -Dwls.home=${WLS_HOME}
   -Dweblogic.home=${WLS_HOME} -Dwlspatch=${WLS_PATCHVERSION} "
   ```

3. Restart the OAM Administration Server and OAM Managed Servers.

2.1.8 Applications Will Not Start After WebLogic Server is Updated

After applying the latest patches to Oracle WebLogic Server, the WL_HOME/server/lib/weblogic.policy file must be edited to include the following entry in order for Middleware services such as Discoverer, Access Manager, and Identity Manager to start:

```
grant codeBase "file:MW_HOME/WLS/patch_jars/-" {
      permission java.lang.RuntimePermission "oracle.*","read";
};
```

Replace *MW_HOME* with the location of your Middleware home directory.

Replace *WLS* with one of the following:

- patch_wls1034 for WebLogic Server version 10.3.4
- patch_wls1035 for WebLogic Server version 10.3.5
- patch_wls1036 for WebLogic Server version 10.3.6

2.2 Installation Issues and Workarounds

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

2.2.1 Error when Installing Oracle Identity Manager Design Console

When you are trying to install Oracle Identity Manager Design Console on a Windows machine that has firewall between the machine and the Oracle Identity Manager server, the following error message is displayed when you run the `config.cmd` command:

```
Error in validating the Hostname field value.Entered host is not up and running
```

To install Oracle Identity Manager Design Console, you must open port 7 in the firewall.

2.2.2 Mandatory Patches Required for Installing Oracle Identity Manager

This section describes the necessary patches that you must apply for installing and configuring Oracle Identity Manager.

Note: This section provides the mandatory patches that were available at the time of publishing the release notes. For additional changes and revised patch requirements, see My Oracle Support Document ID 1600323.1.

Table 2–1 provides information about the mandatory patches required for Oracle Identity Manager. Please note that these patches can be applied in any order.

For information about any additional patches that you must apply, see Section 1.5, "Downloading and Applying Required Patches"

Table 2–1 Patches Required to Fix Specific Issues with Oracle Identity Manager 11gR2 (11.1.2.2.0)

Oracle Fusion Middleware Product or Component	Patch Number/Name	When to Apply?	Description
Oracle WebLogic Server	18398295	After installing Oracle Identity and Access Management	This Oracle WebLogic Server patch is required only if you are using Multi Byte Character Set. Follow the `README.txt` file for patching instructions.
Oracle WebLogic Server	14404715	After installing Oracle Identity and Access Management	This is a mandatory Oracle WebLogic Server patch. Follow the `README.txt` file for patching instructions.
Oracle WebCenter Portal	18334433	After installing Oracle Identity and Access Management	This is a mandatory Oracle WebCenter Portal patch. Follow the `README.txt` file for patching instructions.
Oracle Fusion Middleware - Dynamic Monitoring Service	18748961	After installing Oracle Identity and Access Management	This is a mandatory Dynamic Monitoring Service patch. Follow the `README.txt` file for patching instructions.
Enterprise Manager for Fusion Middleware	18334644	For IBM WebSphere, apply this patch before the cell creation for changes to take effect.	This is a mandatory Enterprise Manager patch only if you are using IBM WebSphere. Follow the `README.txt` file for patching instructions.
Oracle Business Process Management Suite	19190139	After installing Oracle SOA Suite	This is a mandatory Oracle Business Process Management Bundle Patch 11.1.1.7.5 patch. Follow the `README.txt` file for patching instructions.
Oracle Business Process Management Suite	17897950, 18244420, 19457718, 19471000, 18416233, 19702081, 16677877, 19926333	After installing Oracle SOA Suite	These mandatory Oracle Business Process Management Suite patches need to be applied after Oracle Business Process Management has been upgraded to Bundle Patch 11.1.1.7.5 using patch 19190139. Select patch version 11.1.1.7.5, download the patches, and follow the `README.txt` file for patching instructions.
Oracle Platform Security for Java	19281598	After installing Oracle Identity and Access Management	This is a mandatory Oracle Platform Security Services (OPSS) patch if you are using IBM WebSphere 7.0.0.33. Follow the `README.txt` file for patching instructions.
Oracle Application Development Framework	20265562	After installing Oracle Identity and Access Management	This is a mandatory Oracle Application Development Framework patch. Follow the `README.txt` file for patching instructions.

Table 2–1 (Cont.) Patches Required to Fix Specific Issues with Oracle Identity Manager 11gR2 (11.1.2.2.0)

Oracle Fusion Middleware Product or Component	Patch Number/Name	When to Apply?	Description
Oracle Application Development Framework	18373763	After installing Oracle Identity and Access Management	This Oracle Application Development Framework patch is required only for Oracle Identity Manager cluster upgrade on the IBM WebSphere platform.
Oracle Business Intelligence Publisher	16556157	After installing Oracle BI Publisher 11.1.1.7.0	This is an Oracle Business Intelligence Publisher patch. If you want to run Reports on Oracle Identity Manager 11.1.2.2.0, you must install Oracle BI Publisher 11.1.1.7.0, and then apply the patch number 16556157. Follow the `README.txt` file for patching instructions.
Oracle Virtual Directory - Identity Virtualization Library (libOVD)	19779563, 18762607	After installing Oracle Identity and Access Management	These patches are mandatory Oracle Virtual Directory 11*g* Release 1 (11.1.1.7.0) patches if you are using Identity Virtualization Library (libOVD). Note that these patches are classified as Oracle Virtual Directory patches. Select patch version 11.1.1.7.0, download the patches, and follow the `README.txt` file for patching instructions.
Oracle Virtual Directory	17196811	After installing Oracle Identity and Access Management	This is an Oracle Virtual Directory patch. Follow the `README.txt` file for patching instructions.
Oracle Unified Directory	19157573	After installing Oracle Unified Directory	This is a mandatory patch for deployments where Oracle Identity Manager is configured to LDAPSync with Oracle Unified Directory 11*g* Release 2 (11.1.2.2) as the LDAP identity store. If you have Oracle Unified Directory patch 18461856 applied in your environment, then roll it back before applying patch 19157573. For patching instructions, refer to My Oracle Support Document ID 1905631.1, which is available from My Oracle Support.
Silent Installation of Oracle Identity Manager	18270453		This patch contains an archive of custom scripts and response files required for the end-to-end silent installation and configuration of Oracle Identity Manager. The archive contains scripts for silent installation on Oracle WebLogic Server and on IBM WebSphere. For more information, see "End-to-End Silent Installation and Configuration for Oracle Identity Manager" in the *Oracle Fusion Middleware Installation Planning Guide*.

Table 2–1 (Cont.) Patches Required to Fix Specific Issues with Oracle Identity Manager 11gR2 (11.1.2.2.0)

Oracle Fusion Middleware Product or Component	Patch Number/Name	When to Apply?	Description
Oracle Identity Manager	18494370	After Installing Oracle Identity and Access Management 11.1.2.2.0	This is a mandatory Oracle Identity Manager patch if you are upgrading to 11.1.2.2.0 on IBM WebSphere Platform.
Oracle Service Delivery Platform	17565911	After installing Oracle Identity and Access Management	This is a mandatory Service Delivery Platform patch if you are upgrading to Oracle Identity Manager 11*g* Release 2 (11.1.2.2). Follow the `README.txt` file for patching instructions.
Repository Creation Utility (RCU)	`R2PS2_RCU_Patch_files-1.zip` `R2PS2_RCU_Patch_files-2.zip`		This is a mandatory Repository Creation Utility patch that must be applied if the following error is encountered when running Repository Creation Utility (RCU) during Oracle Identity Manager 11*g* Release 2 (11.1.2.2) installation: `RCU-6136: Error while trying to execute SQLPlus action` Oracle Identity Manager Database schema creation fails in some 64-bit operating system environments because the existing SQLPlus shell binary might not be supported on these environments. To fix this issue, refer to My Oracle Support Document ID 1681410.1, which is available from My Oracle Support. This Support Note provides important information about this patch that must be applied to RCU. This patch consists of the `R2PS2_RCU_Patch_files-1.zip` and the `R2PS2_RCU_Patch_files-2.zip` files required for the Oracle Identity Manager schema.

To download the patches, do the following:

1. Log in to My Oracle Support.
2. Click **Patches & Updates**.
3. Select **Patch name or Number**.
4. Enter the patch number.
5. Click **Search**.
6. Download and install the patch.

Patching Instructions

If you are using Oracle WebLogic Server, the patching instructions are mentioned in the `README.txt` file that is provided with each patch.

If you are using IBM WebSphere, follow the instructions provided below:

1. Navigate to *Patch_Home* directory where the patch is located.
2. Set the environment variable ORACLE_HOME to point to the *SOA_HOME* directory.

   For example:

   ```
   setenv ORACLE_HOME /mydirectory/myfolders/Oracle_SOA1
   ```
3. Set the environment variable PATH to point to the OPatch directory.

   For example:

   ```
   setenv PATH /mydirectory/myfolders/Oracle_SOA1/OPatch:$PATH
   ```
4. Execute the opatch command, as follows:

   ```
   opatch apply -jdk Path_To_IBM_jdk
   ```
   For example:

   ```
   opatch apply -jdk WAS_HOME/java
   ```

2.2.3 JPS Keystore Service Initialization Failure in Join Domain Scenario for Oracle Access Management Domain

In a join domain scenario between Oracle Identity Manager and Oracle Access Management, the keystore file configured in Oracle Platform Security Services configuration does not exist but passwords are already available from OIM installation in the Credential Store Framework store. Hence, when Oracle Access Management Server tries to store the key store file, it fails as the key already exists.

Workaround:

- Before starting the Administration server, copy the key store file from Oracle Identity Manager domain to Oracle Access Management domain's key store location.

  For example: Copy the default keystore (.jks) file from <OIM domain>/config/fmwconfig to <OAM domain>/config/fmwconfig.

  > **Note:** This step should be performed after you have configured the Oracle Access Management domain using config.sh but before you start the Administration Server.

- In Oracle Identity Manager domain, look for default context in jps-config.xml.
- Under this locate keystore service and keystore file location.
- Copy this keystore (.jks) file to the location defined in Oracle Access Management domain key store location under Oracle Platform Security Services (jps-config.xml) configuration.

2.2.4 Prerequisite Checks Fails When Installing SOA on Windows 2012

When you install SOA on Windows 2012, the prerequisite checks fails.

Workaround:

This error can be ignored by specifying -ignoreSysPrereqs when you start the Oracle SOA Suite installer.

2.2.5 Oracle Universal Installer Fails to Apply One-off Patches if a 32-Bit JVM is in MW_HOME

At the end of the installation, the 11*g* Release 2 Oracle Universal Installer also applies the one-off patches using OPatch. When applying the patches, the installer does not use the specified JVM, but it uses the JVM that is present in the `MW_HOME`. The `MW_HOME` has a 32-bit JVM. This results in OPatch failure.

Workaround:

The Oracle Universal Installer successfully applies the one-off patches using OPatch, when the Oracle WebLogic Server is installed with a 64-bit JVM in the `MW_HOME`.

2.2.6 Opatch Errors When Applying One-off Patches During Oracle Identity and Access Management Installation

During the Oracle Identity and Access Management 11*g* Release 2 (11.1.2) installation, you may see Opatch errors when the installer applies one-off patches. The following errors are displayed in the logs:

Error-1

```
 OPatch failed with error code 39
  ]
      stderr=[[ Error during Prerequisite for apply Phase]. Detail: OPatch
  failed during prerequisite checks: Prerequisite check
  "CheckPatchApplicableOnCurrentPlatform" failed.
  Prerequisite check "CheckApplicable" failed.
  ]
```

Description and Workaround:

These are warning messages which can be ignored.

Error-2

```
OPatch failed with error code 25
]
    stderr=[[ Error during Oracle Home discovery Phase]. Detail: OPatch
failed: ApplySession failed to prepare the system.
To run in silent mode, OPatch requires a response file for Oracle
Configuration Manager (OCM).
Please run "/scratch/FMW_OAM/Oracle_OAM/OPatch/ocm/bin/emocmrsp" to generate
an OCM response file. The generated response file
can be reused on different platforms and in multiple OPatch silent installs.

To regenerate an OCM response file, Please rerun
"/scratch/FMW_OAM/Oracle_OAM/OPatch/ocm/bin/emocmrsp".
```

Description and Workaround:

This issue occurs if the OPatch version in the *`MW_HOME`* is 11.1.0.10.x. The workaround for this issue is to revert back to OPatch version 11.1.0.9.9 before applying one-off patches.

2.2.7 Prerequisite Checks Fails When Installing Oracle Identity and Access Management on Oracle Enterprise Linux 6

When you try to install Oracle Identity and Access Management on an Oracle Enterprise Linux 6 bare metal x64 machine, the prerequisite checks fails.

Workaround:

Start the installer using the `-ignoreSysPrereq` parameter.

```
./runInstaller -ignoreSysPrereq
```

2.2.8 Prerequisite Checks Fails When Installing Oracle Identity and Access Management On Red Hat Enterprise Linux 6.x

When you try to install Oracle Identity and Access Management on Red Hat Enterprise Linux 6.x, the prerequisite checks fails.

Workaround:

This issue has two workarounds. You can choose to perform any of them. The workarounds are:

- Install **redhat-lsb-core-4.0-7.el6** for x86_64 package. For information about supported operating systems and version, see *Oracle Fusion Middleware System Requirements and Specifications*.
- Apply Patch number 16963926. For information about downloading the patch and applying it, refer to the instructions described in Section 2.2.2, "Mandatory Patches Required for Installing Oracle Identity Manager".

2.2.9 SOA-INFRA Component Fails to Start up After Installing SOA in Silent Mode

Oracle Identity Manager requires Oracle SOA Suite. This issue occurs when you install and configure Oracle SOA Suite in silent mode. After installing and configuring Oracle SOA Suite in silent mode, when you start the soa-infra component, it fails with the following error message in the server log file (*<domain home>*`/servers/soa_server1/logs/soa_server1.log`):

```
java.lang.NoClassDefFoundError: weblogic/sca/api/ScaReferenceProcessor.
```

The workaround for this issue is described in the following support note:

The soa-infra Component Is Down After A Fresh SOA Installation. The soa_server1.log Reports a java.lang.NoClassDefFoundError weblogic/sca/api/ScaReferenceProcessor (Doc ID 1332553.1)

2.3 Configuration Issues and Workarounds

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

2.3.1 Default Cache Directory Error

When you start the Oracle Fusion Middleware Configuration Wizard, by running the `config.cmd` or the `config.sh` command, the following error message is displayed:

```
*sys-package-mgr*: can't create package cache dir
```

The error message indicates that the default cache directory is not valid. You can change the cache directory by including the`-Dpython.cachedir=<valid_directory>` option in the command line.

2.3.2 Launching Oracle Identity Manager Configuration Wizard on AIX with JDK7

You can not launch Oracle Identity Manager Configuration Wizard on AIX with JDK7, when you run the script `$<ORACLE_HOME>/bin/config.sh`

The Oracle Universal Installer window appears if you add the `-jreLoc` option in the command line: `$<ORACLE_HOME>/bin/config.sh -jreLoc <JRE_HOME>`

2.3.3 Unable to Add Weblogic Password in the Fusion Middleware Configuration Wizard

In the Fusion Middleware Configuration Wizard, you cannot add Weblogic password in the **Configure Administrator User Name and Password** screen.

Workaround:

When you are prompted to enter the Weblogic user password, you may not be able to enter the password. Click **Next** to go to the next screen. You will be prompted of an error: **Password cannot be empty**. Go back to the previous screen and type in the password again.

Note: Before running the Oracle Fusion Middleware Configuration Wizard, ensure that you have installed the following:

- Oracle WebLogic Server
- Oracle SOA Suite (Oracle Identity Manager Users Only)
- Oracle Identity and Access Management

2.3.4 Mandatory Steps to Complete After Installing Oracle Access Management or Oracle Identity Manager

The following are the steps that must be followed after installing Oracle Access Management 11*g* Release 2 (11.1.2) or Oracle Identity Manager 11*g* Release 2 (11.1.2):

1. Ensure that the following pre-requisites are met, before moving to step 2:
   a. Ensure that you have configured the domain using the *IAM_ORACLE_HOME*/common/bin/config.sh script.
   b. Ensure that you have configured the Database Security Store using the following commands:

```
IAM_ORACLE_HOME/common/bin/wlst.sh IAM_ORACLE_
HOME/common/tools/configureSecurityStore.py -d <domaindir> -c IAM -p <opss_
schema_password> -m [create/join]
```

2. Copy the jps-config.xml file to jps-config.xml_old for recovery and reference.
3. Do the following to edit the jps-config.xml file:
   a. Look for the XML element

```
<serviceInstance name="pdp.service" provider="pdp.service.provider">
```

   b. Delete the following two entries:

```
<property name="oracle.security.jps.pdp.AuthorizationDecisionCacheEnabled"
value="false"/>
<property name="oracle.security.jps.ldap.policystore.refresh.interval"
value="10000"/>
```

   After you delete the first two properties their default values will be set. The default values are true and 600000 (10 minutes) respectively:

   c. Add following entry in same section:

```
<property name="oracle.security.jps.pd.client.PollingTimerInterval"
value="31536000"/>
```

   d. The edited XML must look like the following:

```
<serviceInstance name="pdp.service" provider="pdp.service.provider">
            <description>Runtime PDP service instance</description>
            <property
name="oracle.security.jps.runtime.pd.client.policyDistributionMode"
value="mixed"/>
            <property name="oracle.security.jps.runtime.instance.name"
value="OracleIDM"/>
            <property name="oracle.security.jps.runtime.pd.client.sm_name"
value="OracleIDM"/>
          <property name="oracle.security.jps.policystore.refresh.enable"
value="true"/>
          <property
name="oracle.security.jps.pd.client.PollingTimerInterval"
value="31536000"/>
</serviceInstance>
```

2.3.5 Use Absolute Paths While Running configureSecurityStore.py With -m Join

The Configure Security Store fails to create the policy store object when using variables such as ORACLE_HOME and MW_HOME while running configureSecurityStore.py with

the -m join parameter. Specify absolute paths for ORACLE_HOME and MW_HOME while running the command with -m join parameter.

2.3.6 Security Store Join Fails on Windows

On Windows, when you run the command configSecurityStore.py, the -m validate option succeeds, but the following error gets reported towards the end of the command:

```
c:\Amy_OPAM\Oracle\Middleware\Oracle_RC3\common\bin>wlst.cmd
..\tools\configureSecurityStore.py -d
c:\Amy_OPAM\Oracle\Middleware\user_projects\domains\OPAM_RC3_Domain2 -c IAM
-m join -p welcome1 -k c:\Amy_OPAM\software\RC3\ -w welcome1

Error: Failed to join security store, unable to locate diagnostics data.
Error: Join operation has failed.
```

Workaround:

Ignore the error. Even though the error gets reported there is no functional impact because the newly created server with the join option can start successfully and continue to service requests.

2.3.7 Weblogic Server Configuration Wizard does not support JDK6 on AIX7

Weblogic Server configuration wizard displays the warning CFGFWK-60895 for 1.6.0.9.2 JDK on AIX 7 for Oracle Access Management, Oracle Adaptive Access Manager, and Oracle Privileged Account Manager.

Workaround:

1. Install Weblogic Server.
2. Install SOA.
3. Install Oracle Identity and Access Management.
4. Run the configuration wizard.
5. Create an Oracle Identity Manager (OIM) domain.
6. Create domain's for Oracle Access Management, Oracle Adaptive Access Manager, and Oracle Privileged Account Manager.
7. You get the warning CFGFWK-60895: The selected JDK version is lower than recommended minimum version.
8. Click **Cancel** and select a different JDK or Click **OK** to proceed with same.

> **Note:** Warning CFGFWK-60895 does not interfere with functionality.

2.3.8 Access Policy Manager Deployments Do Not Target Administration Server in Cluster Scenario

When you select the Oracle Entitlements Server template for Administration server, by default Access Policy Manager is deployed to the administration server.

But when a cluster for any component is created with > 1 server instance, then APM is targeted to the clustered servers and not the administration server, which causes the servers within the cluster to come up in administration mode.

For example, if you have a domain with one instance of Oracle Identity Manager, SOA and Oracle Access Management, the Access Policy Manager is targeted to the administration server. However, if you create another instance of Oracle Identity Manager, so that it has two instances at the time of domain creation, then the Access Policy Manager is deployed to the clustered servers (in this case Oracle Identity Manager server) and not administration server.

Workaround:

1. Log in to Weblogic administration console.
2. Click **Deployments**.
3. Click **oracle.security.apm (11.1.1.3.0)**.
4. Click **Targets**.
5. Click **Lock & Edit**.
6. Select **oracle.security.apm (11.1.1.3.0)**.
7. Click **Change Targets**.
8. Select **AdminServer**.
9. Click **Yes**.
10. Click **Activate Changes** and restart the administration server.

2.3.9 Requests Fail with ClassCastException

When you install Oracle Identity Manager on Weblogic Server (10.3.5.0), the request fails with the following exception:

```
Unable to instantiate the workflow process due to: Tasklist mapping failed for
workflowdefinition: default/DefaultRequestApproval!1.0 due to
oracle.bpel.services.workflow.query.ejb.TaskQueryService_oz1ipg_HomeImpl_1035_
WLStub cannot be cast to
oracle.bpel.services.workflow.query.ejb.TaskQueryServiceRemoteHome.
```

This happens when initiating the approvals for a request.

Workaround:

For Weblogic Server 10.3.5 you must download and install patch 12944361. Weblogic Server 10.3.6 do not require this patch

2.3.10 Modify PKCS11-Solaris Security Provider Before Running the `configSecurityStore.py` Command When Using Sun JDK 1.7

The command `configSecurityStore.py` fails to run when installing Oracle Identity and Access Management 11*g* Release 2 components on Solaris 10 SPARC or higher versions, using JDK 1.7. This occurs because of the implementation of PKCS11-Solaris security provider.

Workaround:

- Back up the file `$JAVA_HOME/jre/lib/security/java.security`
- Open the file `$JAVA_HOME/jre/lib/security/java.security` in a text editor and modify the provider list

Ensure that `sun.security.pkcs11.SunPKCS11` is at the beginning of the provider list. Modify the provider list, as in the following example:

```
security.provider.1=sun.security.pkcs11.SunPKCS11
  ${java.home}/lib/security/sunpkcs11-solaris.cfg
  security.provider.2=com.oracle.security.ucrypto.UcryptoProvider
  ${java.home}/lib/security/ucrypto-solaris.cfg
...
```

2.3.11 Server Startup Failure

If you start the OES domain without running the `configureSecurityStore.py` script, the server fails to start with following exception:

```
oracle.security.jps.service.keystore.KeyStoreServiceException: Failed to
perform cryptographic operation Caused by: javax.crypto.BadPaddingException:
Given final block not properly padded
```

Workaround:

The workaround is to export the domain encryption key from a domain in the same logical Oracle Identity and Access Management deployment already configured to work with the database security store, and then run the `configureSecurityStore.py` script.

`exportEncryptionKey(jpsConfigFile=`*`jpsConfigFile_Loc`*`,keyFilePath=`*`keyFilePath`*`,keyFilePassword=`*`keyFilePassword`*`)`
where:

`jpsConfigFile_Loc` - is the absolute location of the file `jps-config.xml` in the domain from which the encryption key is being exported.

`keyFilePath` - is the directory where the file `ewallet.p12` is created; note that the content of this file is encrypted and secured by `keyFilePassword`.

`keyFilePassword` - is the password to secure the file `ewallet.p12`; note that this same password must be used when importing that file.

2.3.12 OES Configuration Using JBoss as a Security Module Throws Error on AIX

When you try to configure JBoss Security Module on an AIX operating system, it throws a `java.lang.ClassNotFoundException` error.

Workaround:

Complete the following steps:

1. Go to the following directory:

   `JAVA_HOME``/jre/lib/security`

2. Open the `java.security` file and search for `policy.provider` attribute. The value of the attribute `policy.provider` is set to `org.apache.harmony.security.fortress.DefaultPolicy`.

   You must delete the existing value of the `policy.provider` attribute and change it to `sun.security.provider.PolicyFile`.

2.3.13 Configuring Database Security Store Fails with JVM Error

When you configure the Database Security Store using the following `configureSecurityStore.py` script,

```
oracle_common/common/bin/wlst.sh
$ORACLE_HOME/common/tools/configureSecurityStore.py -d DOMAIN_HOME -c IAM -m
create -p OPSS_SCHEMA_PASSWORD
```

the configuration fails with a JVM error. The following error is displayed:

```
JRE version:7.0_25
Java VM:OpenJDK 64-Bit Server VM(23.7-b01 mixed mode linux-amd64 compressed
oops)
Problematic frame:
V [libjvm.so+0x773ec7] JVM_handle_linux_signal+0x54df7
```

Workaround:

The above error occurs because the JVM process tries to access a memory location that the operating system has not given access to.

As a workaround, re-configure the Database Security Store using the following command:

```
$JAVA_HOME/bin ./java -jar wls1036_generic.jar
```

2.3.14 Configuring SSL When Configuring Database Security Store

To configure Database security store, you must run `configureSecuritystore.py` script. To configure SSL when running `configureSecuritystore.py` script, you must complete the following steps:

> **Note:** it is assumed that, at this point, Keystore and Truststore are already created using the command `keytool`.

1. Update the Database URL in the JDBC configuration file `opss-jdbc.xml` by doing the following:
   a. Open the file *DOMAIN_HOME*`/config/jdbc/opss-jdbc.xml` for editing.
   b. Edit the Database URL on line 5 to change it from:

      `jdbc:oracle:thin:@<db_host>:<db_port>/<service_name>`

      to

      `jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)(HOST=<db_host>)(PORT=<db_port>)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=<service_name>)))`

   c. Add the following properties:

```
<property>
<name>javax.net.ssl.keyStore</name>
<value>path_to_keystore</value>
</property>
<property>
<name>javax.net.ssl.keyStorePassword</name>
<value>keystore_password</value>
</property>
<property>
<name>javax.net.ssl.trustStore</name>
<value>path_to_truststore</value>
</property>
<property>
<name>javax.net.ssl.trustStorePassword</name>
<value>truststore_password</value>
```

```
</property>
<property>
<name>oracle.net.ssl_version</name>
<value>TLS_version</value>
</property>
```

Where,

path_to_keystore refers to the absolute path to the keystore. For example, /scratch/certs/dbcerts/mycerts/keystore.jks.

keystore_password refers to the password of the key store.

path_to_truststore refers to the absolute path to the truststore. For example, /scratch/certs/dbcerts/mycerts/truststore.jks.

truststore_password refers to the password of the trust store.

TLS_version refers to the Transport Layer Security (TLS) version. If the Database server is configured to use the TLS version 1.0, you must specify 1.0.

d. Save the file and exit.

2. Edit the domain configuration file setDomainEnv.sh by doing the following:

a. Open the file *$MW_HOME*/ user_projects/domains/*DOMAIN_HOME*/bin/setDomainEnv.sh for editing.

b. Edit the line 368 to change it from:

```
EXTRA_JAVA_PROPERTIES="
-Dweblogic.security.IgnoreHostNameVerification=true
-Dweblogic.security.SSL.ignoreHostnameVerification=true ${EXTRA_
JAVA_PROPERTIES}"
```

to

```
EXTRA_JAVA_PROPERTIES="
-Dweblogic.security.IdentityKeyStore=CustomIdentity
-Dweblogic.security.CustomIdentityKeyStoreFileName=<path_to_
identity_keystore_file>
-Dweblogic.security.CustomIdentityKeyStorePassPhrase=<identity_
keystore_pass_phrase>
-Dweblogic.security.Identity.KeyStoreType=<identity_keystore_type>
-Dweblogic.security.TrustKeyStore=CustomTrust
-Dweblogic.security.CustomTrustKeyStoreFileName=<path_to_trust_
keystore_file> -Dweblogic.security.CustomTrustKeyStoreType=<trust_
keystore_type>
-Dweblogic.security.CustomTrustKeyStorePassPhrase=<trust_keystore_
pass_phrase> -Dweblogic.security.IgnoreHostNameVerification=true
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.SSL.protocolVersion=TLS1 ${EXTRA_JAVA_
PROPERTIES}"
```

For example:

```
EXTRA_JAVA_PROPERTIES=" -Dweblogic.security.IdentityKeyStore=CustomIdentity
-Dweblogic.security.CustomIdentityKeyStoreFileName=/scratch/certs/dbcerts/m
ycerts/keystore.jks
-Dweblogic.security.CustomIdentityKeyStorePassPhrase=Password1
-Dweblogic.security.Identity.KeyStoreType=JKS
-Dweblogic.security.TrustKeyStore=CustomTrust
-Dweblogic.security.CustomTrustKeyStoreFileName=/scratch/certs/dbcerts/myce
```

```
rts/truststore.jks
-Dweblogic.security.CustomTrustKeyStoreType=JKS
-Dweblogic.security.CustomTrustKeyStorePassPhrase=Password2
-Dweblogic.security.IgnoreHostNameVerification=true
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.SSL.protocolVersion=TLS1 ${EXTRA_JAVA_PROPERTIES}"
```

c. Save the file and exit.

3. Edit the WLST script by doing the following:

a. Open the file *$MW_HOME*/wlserver_10.3/common/bin/wlst.sh for editing.

b. Update the following line:

```
JVM_ARGS="-Dprod.props.file='${WL_HOME}'/.product.properties
${WLST_PROPERTIES} ${JVM_D64} ${MEM_ARGS} ${CONFIG_JVM_ARGS}"
```

to change it to

```
JVM_ARGS="-Dprod.props.file='${WL_HOME}'/.product.properties
${WLST_PROPERTIES} ${JVM_D64} ${MEM_ARGS} ${CONFIG_JVM_ARGS}
-Djavax.net.ssl.trustStorePassword=<trust_store_password>
-Djavax.net.ssl.keyStorePassword=<key_store_password>
-Djavax.net.ssl.keyStore=<path_to_keystore>
-Djavax.net.ssl.trustStore=<path_to_truststore> -Doracle.net.ssl_
version=<TLS_version>"
```

For example:

```
JVM_ARGS="-Dprod.props.file='${WL_HOME}'/.product.properties ${WLST_
PROPERTIES} ${JVM_D64} ${MEM_ARGS} ${CONFIG_JVM_ARGS}
-Djavax.net.ssl.trustStorePassword=password1
-Djavax.net.ssl.keyStorePassword=password2
-Djavax.net.ssl.keyStore=/scratch/certs/dbcerts/mycerts/keystore.jks
-Djavax.net.ssl.trustStore=/scratch/certs/dbcerts/mycerts/truststore.jks
-Doracle.net.ssl_version=1.0"
```

In the above example, the property "-Doracle.net.ssl_version=1.0" represents that the Database server is configured to use the Transport Layer Security (TLS) version 1.0.

c. Save the file and exit.

4. Edit the configureSecurityStore.py script by doing the following:

a. Open the file *$MW_HOME*/*IDM_HOME*/common/tools/configureSecurityStore.py for editing.

b. Edit the line 241 to change it from:

```
full_command_parts = ("java -Doracle.security.jps.config=", jps_
config_xml_path, "
oracle.security.jps.internal.api.credstore.CredstoreUtil",
```

to

```
full_command_parts = ("java
-Djavax.net.ssl.trustStorePassword=<truststore_password>
-Djavax.net.ssl.keyStorePassword=<keystore_password>
-Djavax.net.ssl.keyStore=<path_to_keystore>
-Djavax.net.ssl.trustStore=<path_to_truststore> -Doracle.net.ssl_
version=<TLS_version> -Doracle.security.jps.config=", jps_config_
```

```
xml_path, "
oracle.security.jps.internal.api.credstore.CredstoreUtil",
```

For example:

```
full_command_parts = ("java -Djavax.net.ssl.trustStorePassword=password1
-Djavax.net.ssl.keyStorePassword=password2
-Djavax.net.ssl.keyStore=/scratch/certs/dbcerts/mycerts/keystore.jks
-Djavax.net.ssl.trustStore=/scratch/certs/dbcerts/mycerts/truststore.jks
-Doracle.net.ssl_version=1.0
-Doracle.security.jps.config=", jps_config_xml_path, "
oracle.security.jps.internal.api.credstore.CredstoreUtil",
```

c. Edit the line 282 to change it from:

```
full_command_parts = ("java -Doracle.security.jps.config=", jps_
config_xml_path, "
oracle.security.jps.internal.api.credstore.CredstoreUtil",
```

to

```
full_command_parts = ("java
-Djavax.net.ssl.trustStorePassword=<truststore_password>
-Djavax.net.ssl.keyStorePassword=<keystore_password>
-Djavax.net.ssl.keyStore=<path_to_keystore>
-Djavax.net.ssl.trustStore=<path_to_truststore> -Doracle.net.ssl_
version=<TLS_version> -Doracle.security.jps.config=", jps_config_
xml_path, "
oracle.security.jps.internal.api.credstore.CredstoreUtil",
```

For example:

```
full_command_parts = ("java -Djavax.net.ssl.trustStorePassword=password1
-Djavax.net.ssl.keyStorePassword=password2
-Djavax.net.ssl.keyStore=/scratch/certs/dbcerts/mycerts/keystore.jks
-Djavax.net.ssl.trustStore=/scratch/certs/dbcerts/mycerts/truststore.jks
-Doracle.net.ssl_version=1.0
-Doracle.security.jps.config=", jps_config_xml_path, "
oracle.security.jps.internal.api.credstore.CredstoreUtil",
```

d. Edit the line 734 to change it from:

```
= ("java -Xms512M -Xmx512M ",
"oracle.security.jps.internal.tools.configuration.ldap.LdapServiceE
nabler ", command)
```

to

```
= ("java -Xms512M -Xmx512M
-Djavax.net.ssl.trustStorePassword=<truststore_password>
-Djavax.net.ssl.keyStorePassword=<keystore_password>
-Djavax.net.ssl.keyStore=<path_to_keystore>
-Djavax.net.ssl.trustStore=<path_to_truststore> -Doracle.net.ssl_
version=<TLS_version> ",
"oracle.security.jps.internal.tools.configuration.ldap.LdapServiceE
nabler ", command)
```

For example:

```
= ("java -Xms512M -Xmx512M -Djavax.net.ssl.trustStorePassword=password1
-Djavax.net.ssl.keyStorePassword=password2
-Djavax.net.ssl.keyStore=/scratch/certs/dbcerts/mycerts/keystore.jks
-Djavax.net.ssl.trustStore=/scratch/certs/dbcerts/mycerts/truststore.jks
```

```
-Doracle.net.ssl_version=1.0 ",
"oracle.security.jps.internal.tools.configuration.ldap.LdapServiceEnabler
", command)
```

e. Edit the line 774 to change it from:

```
full_command_parts = ("java -Xms512M -Xmx512M ",
"oracle.security.jps.internal.tools.configuration.ldap.LdapServiceE
nabler ", command)
```

to

```
full_command_parts = ("java -Xms512M -Xmx512M
-Djavax.net.ssl.trustStorePassword=<truststore_password>
-Djavax.net.ssl.keyStorePassword=<keystore_password>
-Djavax.net.ssl.keyStore=<path_to_keystore>
-Djavax.net.ssl.trustStore=<path_to_truststore> -Doracle.net.ssl_
version=<TLS_version> ",
"oracle.security.jps.internal.tools.configuration.ldap.LdapServiceE
nabler ", command)
```

For example:

```
full_command_parts = ("java -Xms512M -Xmx512M
-Djavax.net.ssl.trustStorePassword=password1
-Djavax.net.ssl.keyStorePassword=password2
-Djavax.net.ssl.keyStore=/scratch/certs/dbcerts/mycerts/keystore.jks
-Djavax.net.ssl.trustStore=/scratch/certs/dbcerts/mycerts/truststore.jks
-Doracle.net.ssl_version=1.0 ",
"oracle.security.jps.internal.tools.configuration.ldap.LdapServiceEnabler
", command)
```

f. Save the `configureSecurityStore.py` script and exit.

5. Edit the `startWebLogic` script by doing the following:

a. Open the file *DOMAIN_HOME*`/bin/startWebLogic.sh` for editing.

b. Edit line 28 to change it from:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dlaunch.main.class=${SERVER_CLASS}
-Dlaunch.class.path="${CLASSPATH}"
-Dlaunch.complete=weblogic.store.internal.LockManagerImpl -cp ${WL_
HOME}/server/lib/pcl2.jar"
```

to

```
JAVA_OPTIONS="${JAVA_OPTIONS}
-Djavax.net.ssl.trustStorePassword=<truststore_password>
-Djavax.net.ssl.keyStorePassword=<keystore_password>
-Djavax.net.ssl.keyStore=<path_to_keystore>
-Djavax.net.ssl.trustStore=<path_to_truststore> -Doracle.net.ssl_
version=<TLS_version> -Dlaunch.main.class=${SERVER_CLASS}
-Dlaunch.class.path="${CLASSPATH}"
-Dlaunch.complete=weblogic.store.internal.LockManagerImpl -cp ${WL_
HOME}/server/lib/pcl2.jar"
```

For example:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Djavax.net.ssl.trustStorePassword=password1
-Djavax.net.ssl.keyStorePassword=password2
-Djavax.net.ssl.keyStore=/scratch/certs/dbcerts/mycerts/keystore.jks
-Djavax.net.ssl.trustStore=/scratch/certs/dbcerts/mycerts/truststore.jks
```

```
-Doracle.net.ssl_version=1.0 -Dlaunch.main.class=${SERVER_CLASS}
-Dlaunch.class.path="${CLASSPATH}"
-Dlaunch.complete=weblogic.store.internal.LockManagerImpl -cp ${WL_
HOME}/server/lib/pcl2.jar"
```

c. Save the file and exit.

Note: If you have Managed Server, you must update the script *DOMAIN_HOME*`/bin/startManagedWebLogic.sh` as described for `startWebLogic.sh` script.

---

6. Configure the Database security store by running the configureSecurityStore.py script. For more information, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

After you configure the Database security store, start the domain. You can now verify that it uses DB SSL connection.

3

Upgrade and Migration Issues for Oracle Identity and Access Management

This chapter describes issues associated with the upgrade and migration process of Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0). It includes the following sections:

- Section 3.1, "Upgrade Issues"
- Section 3.2, "Migration Issues"

3.1 Upgrade Issues

This section describes issues related to upgrading the following:

- Upgrading Oracle Identity and Access Management components from 11g Release 2 (11.1.2.1.0) to 11g Release 2 (11.1.2.2.0)
- Upgrading Oracle Identity and Access Management components from 11g Release 2 (11.1.2) to 11g Release 2 (11.1.2.2.0)
- Upgrading Oracle Identity and Access Management components from 11g Release 1 (11.1.1.7.0) to 11g Release 2 (11.1.2.2.0)
- Upgrading Oracle Identity and Access Management components from 11g Release 1 (11.1.1.5.0) to 11g Release 2 (11.1.2.2.0)
- Upgrading Oracle Identity and Access Management components from 9.1.x.x to 11g Release 2 (11.1.2.2.0)

For the list of upgrade, migration, and patching issues reported in 11g Release 2 (11.1.2.1.0), see "Upgrade, Migration, and Patching Issues for Oracle Identity and Access Management" in the *Oracle Fusion Middleware Release Notes* for 11g Release 2 (11.1.2.1.0).

For the list of upgrade issues reported in 11g Release 2 (11.1.2), see "Upgrade and Migration Issues for Oracle Identity and Access Management" in the *Oracle Fusion Middleware Release Notes* for 11*g* Release 2 (11.1.2).

3.1.1 Upgrade Issues and Workarounds

This section describes general issues and workarounds related to the upgrade scenarios. It includes the following topic:

- Section 3.1.1.1, "Upgrade User Form Does Not Upgrade UDF of Type LOV Correctly"
- Section 3.1.1.2, "Updating System Mbean Configuration"

3.1.1.1 Upgrade User Form Does Not Upgrade UDF of Type LOV Correctly

This issue occurs when you upgrade Oracle Identity Manager 9.x or Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0). The LOV fields for User, Role, and Organization Forms on User Interface are not upgraded correctly.

You must apply the following workaround before you click on `Upgrade User Form` or `Upgrade Role Form` or `Upgrade Organization Form`. This workaround should not be applied after `Upgrade User Form` is completed.

The workaround is as follows:

1. Log in to the `/sysadmin` console using the following URL:

   `http://`*`OIM_HOST`*`:`*`OIM_PORT`*`/sysadmin`

2. Create and activate a sandbox.
3. Click **Form Designer**.
4. Search for **User form**, and open it.
5. For each LOV UDF, create the UDF with the name same as the UDF name in the `User.xml` file. Make sure you select both **Searchable** and **Searchable Picklist**.
6. Repeat for all the searchable LOV fields of Role and Organization forms.
7. Publish the sandbox.

3.1.1.2 Updating System Mbean Configuration

In Oracle Access Manager Release 2 (11.1.2.2.0), the System Mbean Configuration files have been modified to remove the dependency on domain home. The `copyMbeanXmlFiles` command moves the domain Mbean jars out of the domain home to eliminate any future upgrade or patching issues.

After you have applied the 11.1.2.2.0 patch, you must run the following WLST commands to complete the patching process for OAM:

1. After applying the 11.1.2.2.0 patch set, use the Patch Set Assistant to update the Oracle Access Manager Components as described in "Updating Your Schemas with Patch Set Assistant".

   Make sure that you select Oracle Access Manager on the **Select Component** screen.

2. After a successful run of the Patch Set Assistant, navigate to the following directory and execute the `copyMbeanXmlFiles` command, as shown in the example below.

   You must specify the directory paths for your Middleware and OAM Oracle homes. Directories below are shown as examples only.

   On Unix operating systems:

   ```
   cd $ORACLE_HOME/common/bin/wlst.sh
   copyMbeanXmlFiles ('/MW_HOME/user_projects/domains/my_domain',' '/MW_
   HOME/Oracle_IDM') where 2nd parameter <OAM_ORACLE_HOME> is optional.
   ```

   On Windows operating systems:

   ```
   cd $ORACLE_HOME/common/bin/wlst.sh
   copyMbeanXmlFiles('C:\\Oracle\\MW_HOME\\user_projects\domains\\my_
   domain','C:\\Oracle\\MW_HOME\\Oracle_IDM') where 2nd parameter <OAM_ORACLE_
   HOME> is optional.
   ```

3. After a successful run of the above command, verify that the 11.1.2.2.0 Mbean XML files are copied to the following locations:

   ```
   <DOMAIN_HOME>/config/fmwconfig/mbeans
   ```

   ```
   <DOMAIN_HOME>/config/fmwconfig
   ```

3.1.1.3 SOA Email Notification Does Not Work

In an Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0) deployment that has been upgraded from 11g Release 2 (11.1.2.2.0) or 11*g* Release 2 (11.1.2), SOA email notification may not work in some cases. To ensure that the workaround described in this section is applicable, do the following:

1. Ensure that the WebLogic Administration Server and SOA Managed Server(s) are running.
2. Log in to the Oracle Enterprise Manager.
3. Expand **Weblogic Domain** in the left pane.
4. Right-click on the ***WLS_DOMAIN***, and select **System MBeans Browser**.
5. Go to **Application Defined MBeans**, and click the following in the order specified:
   a. oracle.as.soainfra.config
   b. WorkflowIdentityConfig
   c. human-workflow
   d. WorkflowIdentityConfig.ConfigurationType
   e. jazn.com
   f. WorkflowIdentityConfig.ConfigurationType.ProviderType
   g. JpsProvider
   h. WorkflowIdentityConfig.ConfigurationType.ProviderType.PropertyType

i. jpsContextName

6. Check the **Value** attribute. If value is `default`, the workaround described in this section is not applicable, and you should check email driver configuration in Enterprise Manager.

   If value is `oim`, you must apply the workaround described in this section.

To workaround this issue, complete the following steps:

1. Update the JpsContextName MBean. To do so:
   a. Login to Oracle Enterprise Manager.
   b. On the left pane, expand **Weblogic Domain**.
   c. Right-click ***WLS_DOMAIN***, and select **System MBeans Browser**.
   d. Go to **Application Defined MBeans**, **com.oracle.sdp.messaging**, **Server: soa_server1**, **Application:usermessagingserver**, **SDPMessagingServerConfig**, **ServerConfig**, **JpsContextName**.
   e. Enter oim as the value, and click **Apply**.
2. Restart the SOA Server.

3.1.1.4 AD User Management Connector Issues

After you have applied the Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) patch, the AD User Management 11.1.1.5.0 reconciliation profile used for Oracle Identity Manager may be overwritten.

To correct this issue, open the "Active Directory Organization Recon" job and clear the last token listed (if it its has a specified value) and run the job.

3.1.1.5 Harmless Error After Applying Interim Patch 14481477

If Interim Patch 14481477 was applied to the existing Oracle Identity and Access Management 11g Release 2 (11.1.2.0.0) environment before applying the 11.1.2.2.0 patch, you may see the following warning. You can safely ignore this error message.

Error Message:

```
OUI-10221:The install touches a component that is patched by interim
patches'Interim Patch# 14481477'. The interim patches affect other components not
included in the install.
You may rollback the interim patches 'Interim Patch# 14481477'using OPatch for
consistency before performing the upgrade. You may also choose to ignore this
warning and continue with the upgrade. If you choose to continue, the conflicting
patches will be removed from the inventory. However, some files that are not
updated during the upgrade may be left behind. Contact Support to check
applicability and availability of interim patches 'Interim Patch# 14481477' for
this install.
Do you want to ignore the patch conflicts and continue with the upgrade?.
```

3.1.1.6 Delete WebLogic Server TMP Directories

After you have applied the Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) patch, some of the transaction screens may not open properly. To correct this issue, delete the server-level temporary directories as described below.

1. Shut down all of the managed servers.
2. Navigate to the following directory:

```
cd $MIDDLEWAREHOME/user_projects/domains/$<DOMAINNAME>/servers/
```

3. For each of the servers located in the `/servers` directory, delete the contents of the `_WL_user` folder in the `/tmp` directory.

   For example, if you have an OIM Managed Server on a Unix operating system, you would remove the contents of the **/_WL_user** directory in the following location:

   ```
   $MW_HOME/user_
   projects/domains/$<DOMAINNAME>/servers/$OIMMANAGEDSERVERNAME/tmp/_WL_user
   ```

4. Repeat the process for each server in the `/servers` directory and restart the managed servers.

3.1.1.7 Classpath Issue While Patching Oracle Identity Manager Middle Tier

If you receive the following error message while updating your Oracle Identity Manager (OIM) Middle Tier from 11.1.2.0.0 to 11.1.2.2.0, you must update the `ucp.jar` classpath in the `OIMUpgrade.sh` script.

Error Message:

```
Exception in thread "main" java.lang.NoClassDefFoundError:
oracle/ucp/jdbc/PoolDataSourceFactory
```

To correct this issue, update the `OIMUpgrade.sh` script as described below:

1. Navigate to `<MW_HOME>/Oracle_IDM1/server/bin`
2. Open `OIMUpgrade.sh` in edit mode.
3. Replace the path for `$OIM_HOME/server/ext/ucp.jar` in MDSJARS classpath settings with the following:

   ```
   $MW_HOME/oracle_common/modules/oracle.ucp_11.1.0.jar
   ```

4. Save the `OIMUpgrade.sh` file and then run OIM Middle Tier upgrade as described in "Upgrading Oracle Identity Manager Middle Tier Using Property File".

3.1.1.8 OAuth Service Policy is Missing After Upgrade

This issue occurs if you upgrade an Oracle Access Management 11.1.2.0.0 environment to version 11.1.2.2.0. The `ms_oauth/oauth2/**` policy that is required for OAuth Services is missing. To correct this issue, complete the following steps.

1. Follow the steps in the "Configuring a WebGate to Support Mobile and Social" section of the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
2. Add the encrypted password from Mobile Services to the OAuthServiceProvider configuration:
   a. Sign in to the Oracle Access Management console.

      The Launch Pad opens.

   b. In the **Mobile and Social** section, click **Mobile Services**.

      The "Welcome to Oracle Access Management Mobile and Social - Mobile Services" page opens.

   c. In the **Service Providers** section, select **OAMAuthentication** and click **Edit**.

      The OAMAuthentication "Service Provider Configuration" page opens.

d. In the **WebGate Agent** section, locate the **Encrypted Password** field, click **Show in clear text**, and copy the password.

e. Click the **Launch Pad** tab and click **OAuth Service** in the **Mobile and Social** section.

   The OAuth Identity Domains page opens.

f. Click the identity domain in use. If multiple identity domains are in use, repeat steps **f** through **i** for each one.

   The Identity Domain Configuration page opens.

g. Click the **OAuth Service Providers** tab, then click **OAuthServiceProvider**.

   The Service Provider configuration page opens.

h. In the **Attributes** section, locate the **oam.ENCRYPTED_PASSWORD** attribute name and paste the encrypted password into the **Value** field.

i. Click **Save**.

3.1.1.9 "Prerequisite check "CheckApplicable" failed" and "Required component(s) missing" Messages in Access Manager Upgrade Logs

This issue occurs when you upgrade Oracle Access Management Access Manager 11*g* Release 2 (11.1.2) to 11.1.2.2.0. The upgrade logs have the messages **"the Prerequisite check "CheckApplicable" failed"** and **"Required component(s) missing"**. You can ignore these messages.

3.1.1.10 Errors While Starting OIM Server After Successful Upgrade

This issue occurs when you upgrade Oracle Identity Manager to 11.1.2.2.0. After the successful upgrade, when you start the Oracle Identity Manager Server for the first time, the following error messages are displayed in the OIM server log:

```
<Nov 15, 2013 6:27:17 AM PST> <Emergency> <oracle.dfw.incident> <BEA-000000>
<incident 5 created with problem key "DFW-99998
[java.lang.NoClassDefFoundError][oracle.iam.request.repository.RequestDatasetU

pdateListener.metadataObjectChanged][oracle.iam.console.identity.sysadmin.ear]

">
<Nov 15, 2013 6:27:17 AM PST> <Emergency> <oracle.dfw.incident> <BEA-000000>
<incident 3 created with problem key "DFW-99998
[java.lang.NoClassDefFoundError][oracle.iam.request.repository.RequestDatasetU

pdateListener.metadataObjectChanged][oracle.iam.console.identity.self-service.

ear]">
<Nov 15, 2013 6:27:17 AM PST> <Emergency> <oracle.dfw.incident> <BEA-000000>
<incident 4 created with problem key "DFW-99998
[java.io.FileNotFoundException][oracle.iam.platform.utils.SpringBeanFactory.cr

eateBeanFactory][oracle.iam.console.identity.self-service.ear]">
<Nov 15, 2013 6:27:17 AM PST> <Emergency> <oracle.dfw.incident> <BEA-000000>
<incident 2 created with problem key "DFW-99998
[java.io.FileNotFoundException][oracle.iam.platform.utils.SpringBeanFactory.cr

eateBeanFactory][oracle.iam.console.identity.sysadmin.ear]">
```

This is a known issue. The workaround for this issue is to restart the Oracle Identity Manager Server.

3.1.1.11 obLockedOn Attribute Missing From Oracle Internet Directory After Upgrading Access Manager to 11.1.2.2.0

This issue occurs when you upgrade Oracle Access Management Access Manager 11*g* Release 2 (11.1.2) to 11.1.2.2.0. After upgrading Access Manager 11.1.2 to 11.1.2.2.0, the `obLockedOn` attribute will be missing from the Oracle Internet Directory (OID). You must add this attribute back to the Oracle Internet Directory.

The workaround for this issue is as follows:

1. Manually add the `obLockedOn` attribute to the schema.
2. Import the LDIF to OID by running the `ldapmodify` command.
3. Edit the `oam_user_write_acl_users_oblockedon_template.ldif` to give oamSoftwareUser permission to modify `obLockedOn`.
4. Import the modified `oam_user_write_acl_users_oblockedon_template.ldif`.

3.1.1.12 Exception When Upgrading Oracle Identity Manager Middle Tier

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 1 (11.1.1.7.0), or 11*g* release 1 (11.1.1.5.0), or 9.1.x.x to 11.1.2.2.0. The following exception is displayed when you upgrade Oracle Identity Manager middle tier:

```
Error Code: 900
Call: EXECUTE PROCEDURE OIM_RECOMPILE_DB_OBJECTS()
Query: DataModifyQuery()
Dec 16, 2013 10:15:39 PM com.thortech.util.logging.Logger info
INFO: Result Size = 1 PACKAGE STATUS = VALID
Dec 16, 2013 10:15:39 PM com.thortech.util.logging.Logger info
INFO: Recompiling packages - RDBMS
[EL Warning]: 2013-12-16 22:15:39.957--ClientSession(476657190)--Exception
[EclipseLink-4002] (Eclipse Persistence Services - 2.3.1.v20111018-r10243):
org.eclipse.persistence.exceptions.DatabaseException
Internal Exception: java.sql.SQLSyntaxErrorException: ORA-00900: invalid SQL
statement
```

This is a harmless exception. You can ignore this exception.

3.1.1.13 Active Directory User Management 11.1.1.5.0 Connector May Not Work After Upgrading Oracle Identity Manager to 11.1.2.2.0

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 2 (11.1.2) with Active Directory 11.1.1.5.0 connector to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0). After you upgrade Oracle Identity Manager 11.1.2 to 11.1.2.2.0, Active Directory user management 11.1.1.5.0 reconciliation profile gets corrupted.

The workaround for this issue is as follows:

You must regenerate the reconciliation profile by completing the following steps:

1. Log in to the Oracle Identity Manager 11.1.2.2.0 Design Console by running the following command from the location *ORACLE_HOME*`/designconsole/`:

   On UNIX: `./xlclient.sh`

   On Windows: `xlclient.cmd`
2. Expand **Resource Management**.
3. Click **Resource Objects**.
4. Search for the name **Xellerate Organization**.

5. In the Resource Object details page, go to the **Object Reconciliation** tab.
6. Click **Create Reconciliation Profile**. A message will pop up when the profile is created successfully.

3.1.1.14 Error While Starting OIM Server After Upgrading OIM 9.1.x.x to 11.1.2.2.0

This issue occurs when you upgrade Oracle Identity Manager 9.1.x.x to 11.1.2.2.0. After upgrading to 11.1.2.2.0, when you start the OIM Server, the following error is displayed:

```
<Oct 3, 2013 2:26:09 AM PDT> <Error>
<oracle.iam.platform.utils.SpringBeanFactory> <BEA-000000> <Instantiating
Spring Bean Factory Failed.IOException parsing XML document from class path
resource [META-INF/iam-spring-config.xml]; nested exception is
java.io.FileNotFoundException: class path resource
[META-INF/iam-spring-config.xml] cannot be opened because it does not exist>
```

This error message can be ignored.

3.1.1.15 Warning Message While Logging in to OAAM Admin or OAAM Offline Server After Upgrade

This issue occurs when you upgrade Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.1.0) to 11*g* Release 2 (11.1.2.2.0). After upgrading to 11.1.2.2.0, when you log in to the OAAM Admin Server or OAAM Offline Server for the first time, the following warning message is displayed:

```
[oracle.mds] [tid: [ACTIVE].ExecuteThread: '3' for queue:
'weblogic.kernel.Default (self-tuning)'] [userId: ruleAdmin1] [ecid:
d19903e12f34a6b2:72dcd919:141cc6b890e:-8000-0000000000000620,0] [APP:
oaam_admin#11.1.2.0.0] Error occurred when raising audit event "<none>" for
component "ADF-MDS".[[
```

This is a harmless warning message. You can ignore this warning.

3.1.1.16 Error in Upgrade log file After Upgrading OAAM Admin and OAAM Offline Servers

This issue occurs when you upgrade Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2) to 11*g* Release 2 (11.1.2.2.0). After you upgrade OAAM Admin Server and OAAM Offline Server to 11.1.2.2.0, the following error is seen in the upgrade log file:

```
"<Oct 10, 2013 2:47:19 PM PDT> <Error>
<oracle.adfinternal.view.page.editor.utils.ReflectionUtility> <WCS-16178>
<Error instantiating class -
oracle.adfdtinternal.view.faces.portlet.PortletDefinitionDTFactory> "
```

This is a harmless error message. You can ignore this error.

3.1.1.17 Error Message While Starting OAAM Admin and Managed Servers After Upgrade

This issue occurs when you upgrade Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2.2.0). After the upgrade process, when you start the OAAM admin and managed servers, the following exception is displayed as a notification:

```
[2013-10-24T13:20:01.698-07:00] [oaam_admin_server1] [NOTIFICATION] []
[oracle.adfdt.model.mds.MDSApplicationService] [tid: [ACTIVE].ExecuteThread:
'3' for queue: 'weblogic.kernel.Default (self-tuning)'] [userId: <anonymous>]
```

```
[ecid: d19903e12f34a6b2:-55051c63:141ebc57e5a:-8000-000000000000019f,0] [APP:
oaam_admin#11.1.2.0.0] [[
oracle.mds.exception.NoTipCustomizationLayerException: MDS-00091: Unable to
customize /oracle/oaam/view/DataBindings.cpx, empty or null value for tip
customization layer user
at oracle.mds.core.MDSSession.getMutableMO(MDSSession.java:4150)
at oracle.mds.core.MDSSession.getMutableMO(MDSSession.java:2110)
at oracle.mds.core.MDSSession.getMutableMO(MDSSession.java:1985)
at
oracle.adfdt.model.mds.MDSApplicationService.findApplication(MDSApplicationSer
vice.java:58)
at
oracle.adfdt.model.mds.MDSModelDesignTimeContext.initServices(MDSModelDesignTi
meContext.java:232)
at
oracle.adfdt.model.mds.MDSModelDesignTimeContext.<init>(MDSModelDesignTimeCont
ext.java:82)
at
oracle.adfdt.mds.MDSDesignTimeContext.<init>(MDSDesignTimeContext.java:81)
at
oracle.adfdt.mds.MDSDesignTimeContext.<init>(MDSDesignTimeContext.java:69)
at
oracle.adfinternal.view.page.editor.Page.getDesignTimeBindingContainer(Page.ja
va:618)
at
```

This is a harmless error message. You can ignore this error.

3.1.1.18 Some Apps are in Prepared State After Upgrade

After you upgrade Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2.2.0), the following Apps are in 'Prepared' state:

- `oaam_admin`
- `oaam_offline`
- `oaam_server`

This is a known issue. The workaround for this issue is to login to the WebLogic console and start these three apps manually.

3.1.1.19 Error When Accessing OAAM

After you upgrade Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.7.0) to 11*g* Release 2 (11.1.2.2.0), when you login to EM, and click **Identity & Access** and then click **OAAM**, the following error message is displayed:

```
"Oracle Adaptive Access Manager Cluster" is down.
```

To resolve this issue, perform the following steps:

1. Open the file *$DOMAIN_HOME*`/config/fmwconfig/mbeans/oaam-cluster-mbeans.xml` in a text editor.
2. Change the location attribute value in the `<runtime-mbeans>` xml tag from `oaam/oaam_mbeans.jar` to `${oracle.oaam.home}/mbeans/lib/oaam_mbeans.jar`.

3.1.1.20 Grant/Revoke Requests Cannot be Viewed After OIM Upgrade

This issue occurs after you upgrade Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2.2.0). Grant/revoke requests raised for roles with `OIM Roles` role

category cannot be viewed after upgrade. After upgrade, when you create a request in 11.1.1.5.0, the following error message is displayed in the UI:

```
IAM-7130211 : No Detail found for specified catalog item.
```

These requests are not valid in 11*g* Release 2 (11.1.2.2.0), as these roles are not to be added to the Catalog.

3.1.1.21 Error During REQUEST_TYPE Upgrade

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2.2.0). Following error is displayed in the middle tier upgrade logs during `REQUEST_TYPE` upgrade:

```
oracle.mds.exception.MDSRuntimeException: MDS-00003: error connecting to the
database
Exception occurred while getting connection:
oracle.ucp.UniversalConnectionPoolException: Cannot get Connection from
Datasource: java.sql.SQLException: Listener refused the connection with the
following error:
ORA-12519, TNS:no appropriate service handler found
    at
oracle.mds.internal.persistence.db.fcf.ConnectionManagerCallback.<init>(Connec
tionManagerCallback.java:77)
    at
oracle.mds.persistence.stores.db.DBMetadataStore.checkRepositoryCompatibility(
DBMetadataStore.java:1004)
    at
oracle.mds.persistence.stores.db.DBMetadataStore.checkCompatibility(DBMetadata
Store.java:1269)
    at
oracle.mds.persistence.stores.db.DBMetadataStore.<init>(DBMetadataStore.java:4
47)
    at
oracle.mds.persistence.stores.db.DBMetadataStore.<init>(DBMetadataStore.java:3
99)
    at oracle.iam.oimupgrade.standalone.utils.MDSUtil.<init>(MDSUtil.java:82)
    at
oracle.iam.oimupgrade.standalone.feature.request.UnsupportedRequestTypeUpgrade
.updateRequestMetaData(UnsupportedRequestTypeUpgrade.java:120)
    at
oracle.iam.oimupgrade.standalone.feature.request.UnsupportedRequestTypeUpgrade
.doUpgrade(UnsupportedRequestTypeUpgrade.java:75)
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
```

Even though the above error message is displayed, `REQUEST_TYPE` upgrade is reported as successful. However, for new modify profile requests, track requests page will show Request Type as blank.

To resolve this issue, perform the following steps:

1. Set upgraded flag to `N` for the `REQUEST_TYPE` upgrade feature by running the following query:

   Note: The query must be run as OIM Schema user.

   ```
   update Upgrade_feature_state set
   FEATURE_UPGRADE_STATE='LOADED',IS_FEATURE_UPGRADED='N' where feature_id like
   'PS1PS2UPG.REQUEST_TYPE';
   ```

```
commit;
```

2. Rerun the middle tier upgrade. For more information, see the Upgrading Oracle Identity Manager Middle Tier section of the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity and Access Management*.

3.1.1.22 Exception in Log File After OAAM Upgrade

This issue occurs after you upgrade Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2.2.0). After the upgrade process, when you start the OAAM admin and managed servers, the following exception is displayed as a warning in the `AdminServer-Diagnostic.log` file:

```
WARNING "JAVAX.MANAGEMENT.INSTANCENOTFOUNDEXCEPTION"
```

This is a harmless error message. You can ignore this error.

3.1.1.23 OAAM Administration Server Shows Version 11.1.2.1.0 After Upgrade

This issue occurs when you upgrade Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.1.0) Bundle Patch 01 (BP01) to 11.1.2.2.0, and if you had not applied Bundle Patch 01 correctly. If you had not applied BP01 correctly when you upgraded OAAM 11.1.2.1.0 to 11.1.2.1.0 BP01, and if you still upgrade to 11.1.2.2.0, you will continue to see the product version as 11.1.2.1.0 on the OAAM Administration Server.

The workaround for this issue is as follows:

1. Check if the servers have directory named `stage` at the location *`MW_HOME`*`/user_projects/domains/<domain_name>/<server_name>/stage` and if `oaam_admin.ear` is present in the `stage` directory.
2. If `oaam_admin.ear` file is present in the `stage` directory, you must undeploy the `oaam_admin.ear` application, and deploy it again using the WebLogic Administration console. When you install the `oaam_admin.ear` application, make sure you select **I will make the deployment accessible from the following location** on the **Source Availability** screen, and point to the location *`ORACLE_HOME`*`/oaam/oaam_admin/ear/oaam_admin.ear` directory.

3.1.1.24 OAAM Admin Redeploy Does Not Work When Upgrading OAAM to 11.1.2.2.0

This issue occurs when you upgrade Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.1.0) Bundle Patch 01 (BP01) to 11.1.2.2.0. When upgrading OAAM to 11.1.2.2.0, OAAM_Admin redeploy does not work.

The workaround for this issue is to undeploy the `oaam_admin.ear` application, and deploy it again to the target `oaam_admin_server1` from the location *`ORACLE_HOME`*`/oaam/oaam_admin/ear/oaam_admin.ear`. You can deploy the application using WebLogic Administration console or WLST command.

3.1.1.25 Identifying and Recompiling INVALID Schema Objects After Upgrading Oracle Identity Manager to 11.1.2.2.0

After you upgrade Oracle Identity Manager to 11.1.2.2.0, few OIM Database objects may temporarily be in `INVALID` state due to alterations in underlying dependencies. Such objects get auto compiled on first time invocation in Oracle Database. However, you can optionally recompile the `INVALID` objects. To identify and recompile the `INVALID` schema objects, do the following:

1. Identify INVALID schema objects by running the following SQL query as SYS or DBA schema owner:

   ```
   SELECT owner,object_type,object_name, status FROM dba_objects WHERE
   status='INVALID' AND owner in ('<Schema_Name>') ORDER BY owner, object_
   type, object_name;
   ```

2. Recompile the INVALID objects by executing the following block for each of the affected schemas as SYS or DBA schema owner:

   ```
   BEGIN

   UTL_RECOMP.recomp_serial('<Schema_Name>');

   END;
   ```

3.1.1.26 Error While Executing ConfigureSecurityStore.py

During the Oracle Entitlements Server 11.1.2.2.0 upgrade process, Opatch (17403853) does not get applied, and when you execute configureSecurityStore.py, the following error message is displayed:

```
Caused by: javax.persistence.RollbackException: Exception [EclipseLink-4002]
(Eclipse Persistence Services - 2.3.1.v2011 1018-r10243):
org.eclipse.persistence.exceptions.DatabaseException
Internal Exception: java.sql.BatchUpdateException: ORA-00001: unique
constraint (RC5WIN_OPSS.IDX_JPS_RDN_PDN) violated .
Error Code: 1
Query: InsertObjectQuery(EntryId = 12238:Attribute RowId = 52658 dn =
cn=CredentialStore,cn=IAM,cn=JPSContext,cn=jpsroot)
        at
org.eclipse.persistence.internal.jpa.transaction.EntityTransactionImpl.commitI
 nternal(EntityTransactionImpl.java:102)
        at
org.eclipse.persistence.internal.jpa.transaction.EntityTransactionImpl.commit(
EntityTransactionImpl.java:63)
        at
oracle.security.jps.internal.policystore.rdbms.JpsDBDataManager$8.run(JpsDBDat
aManager.java:1487)
        at
oracle.security.jps.internal.policystore.rdbms.JpsDBDataManager.internalCommit
Txn(JpsDBDataManager.java:1492)
```

The workaround for this issue is to perform all upgrade steps in the correct sequence. To fix the above issue, perform the upgrade steps in the following sequence:

1. Run Opatch to apply the patch 17403853.
2. Re-run configureSecurityStore.py.

3.1.1.27 Error Message While Starting Oracle Identity Manager Managed Server After Upgrade

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) high availability environments to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0).

When you start the Oracle Identity Manager Server for the first time after upgrading the Oracle Identity Manager middle tier, the following error is displayed:

```
<AuthPolicyMergeListener : loadPolicies() : Problem in seeding authorization
policies. Please verify if you have run Middle Tier Upgrade before starting
OIM Server. Please restart the application after running Middle Tier Upgrade.
If the problem still occurs, refer to the documentation to manually update
```

```
the authorization policies access denied
(oracle.security.jps.service.policystore.PolicyStoreAccessPermission
Context:APPLICATION Context Name:OracleIdentityManager Admin
Resource:APPLICATION_POLICY Actions:manage)>
java.security.AccessControlException: access denied
(oracle.security.jps.service.policystore.PolicyStoreAccessPermission
Context:APPLICATION Context Name:OracleIdentityManager Admin
Resource:APPLICATION_POLICY Actions:manage)
```

The workaround for this issue is to restart the Oracle Identity Manager Server.

3.1.1.28 LabelExistsException While Starting Oracle Identity Manager Server After Upgrade

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) high availability environments to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0).

When you start the Oracle Identity Manager Server after upgrading Oracle Identity Manager 11.1.2.1.0 high availability environments to 11.1.2.2.0, the following exception is thrown:

```
<Dec 15, 2013 10:19:11 PM PST> <Error> <oracle.mds> <BEA-000000> <An
Exception occured during the pre-deploy label creation:
preDeployLabel_OIMMetadata#11.1.2.0.0
oracle.mds.versioning.LabelExistsException: MDS-01906: A label with same name.
preDeployLabel_OIMMetadata#11.1.2.0.0 already exists.
```

The workaround for this issue is to restart the Oracle Identity Manager Server.

3.1.1.29 Null Pointer Exception While Creating IDS or ESSO Profile After Upgrading Oracle Access Manager

This issue occurs when you create IDS or ESSO profile after upgrading Oracle Access Manager 11g Release 1 (11.1.1.5.0) to Access Manager 11g Release 2 (11.1.2.2.0).

The workaround for this issue is as follows:

1. Create the directory *$DOMAIN_HOME*/config/fmwconfig/ovd/ids.
2. Copy the files from *$MW_HOME*/oracle_common/modules/oracle.ovd_11.1.1/domain_config/ovd/ids/* to *$DOMAIN_HOME*/config/fmwconfig/ovd/ids/.
3. Copy the file *$MW_HOME*/oracle_common/modules/oracle.ovd_11.1.1/domain_config/mbeans/ovd-ids-mbeans.xml to *$DOMAIN_HOME*/config/fmwconfig/mbeans.
4. Restart the WebLogic Administration Server and the Access Manager Managed Server(s).

3.1.1.30 Error When Accessing My Entitlements Page After Upgrading Oracle Identity Manager to 11.1.2.2.0

This issue occurs when you upgrade Oracle Identity Manager 11g Release 2 (11.1.2) to 11g Release 2 (11.1.2.2.0). After upgrading Oracle Identity Manager 11.1.2 to 11.1.2.2.0, when you access My Entitlements page, the following error is displayed:

```
javax.el.PropertyNotFoundException: The class
'oracle.iam.ui.authenticated.myaccess.bean.MyAccessEntitlementsBean' does not
have the property 'selectedUserDeleted'.
```

The workaround for this issue is as follows:

1. Export the file `/oracle/iam/ui/authenticated/myaccess/pages/mdssys/cust/site/site/myEntitlements.jsff.xml` from MDS ('oim-ui' partition). For information about exporting file to MDS, see "Exporting Metadata Files to MDS" in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.
2. Open the `myEntitlements.jsff.xml` file and replace all the occurrences of "`pageFlowScope.MyAccessEntitlementsBean.selectedUserDeleted`" with "`backingBeanScope.MyAccessEntitlementsReqBean.selectedUserDeleted`".
3. Import the `myEntitlements.jsff.xml` file back to MDS. For information about importing file from MDS, see "Importing Metadata Files from MDS" in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.

3.1.1.31 Exception When you Click on 'Edit' link After Creating Application Instance

This issue occurs when you upgrade Oracle Identity Manager 11g Release 2 (11.1.2.1.0) high availability environments to 11.1.2.2.0. After you create an application instance, when you click on the `Edit` link, the following exception is thrown:

```
[2013-12-19T05:28:48.624-08:00] [oim_server2] [ERROR] []
[oracle.adfinternal.view.faces.config.rich.RegistrationConfigurator] [tid:
[ACTIVE].ExecuteThread: '1'

for queue: 'weblogic.kernel.Default (self-tuning)'] [userId: xelsysadm]
[ecid: 004vUC_6tzS1VcP5Ifp2if0006XN000CMz,0:1] [APP:

oracle.iam.console.identity.sysadmin.ear#V2.0] [URI: /sysadmin/faces/home]
ADF_FACES-60096:Server Exception during PPR, #3[[
oracle.adf.controller.security.AuthorizationException: ADFC-0619:
Authorization check failed:
'/WEB-INF/oracle/iam/ui/platform/common/templates/account-form-

template.xml#account-form-template' 'VIEW'.
        at
oracle.adf.controller.internal.security.AuthorizationEnforcer.handleFailure(Au
thorizationEnforcer.java:182)
```

The workaround for this issue is to run the Middle Tier upgrade utility on the node that hosts the Administration Server.

3.1.1.32 'Generate Entitlement Forms' Option not Available on Clicking 'Regenerate View' After Upgrading Oracle identity Manager

This issue occurs after you upgrade Oracle Identity Manager 11g Release 2 (11.1.2) or 11g Release 2 (11.1.2.1.0) to 11.1.2.2.0.

After you upgrade Oracle Identity Manager to 11.1.2.2.0, when you click Regenerate View for the existing forms that contain entitlement attributes, the Generate Entitlement Forms option is not displayed. Use one of the following workarounds when this issue occurs:

- Create new form for the affected application instance. The new form should work as expected, that is Generate Entitlement Forms option will be available for new forms.
- Manually fix the existing form. The procedure for fixing the application instances whose entitlement attributes use Lookup code in the process form is different from the procedure for fixing the application instance whose entitlement attributes use

Lookup Query in the process form. The entitlement attributes which use Lookup Code in the process form are represented as Lookup fields in the Form Designer. The entitlement attributes which use Lookup Query in the process form are represented as Text fields in the Form Designer. Depending upon what the entitlement attributes are using, complete one of the following procedures to manually fix the forms:

If the entitlement attribute is represented as Lookup field in the Form Designer, complete the following steps:

- Go to Form Designer.
- Select the form that you want to fix.
- Open the entitlement attribute, and make sure you select Entitlement checkbox under Advanced section.
- Save the changes.
- Repeat the above steps for all the entitlement attributes.

If the entitlement attribute is represented as Text field in the Form Designer, complete the following steps:

- You must manually fix the Form EO xml files. To do this, export the oim-ui MDS partition as a zip file by following the steps described in "Exporting Metadata Files to MDS" in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.
- Unzip the zip file. The Form EO xml files that need to be modified are located at `/persdef/sessiondef/oracle/iam/ui/runtime/form/model/<FORM_NAME>/entity/mdssys/cust/site/site` directory, where `<FORM_NAME>` is the name of the Form. The directory will contain one EO xml for parent form and `N` EO xmls for `N` child forms, where `N` is the number of child forms.
- Open the child form EO xml in a text editor. Find the definition of the entitlement attribute and add the following property definition within the `<Properties>` section of the attribute definition:

  ```
  <Property Name="oimEntitlement" Value="Y"/>
  ```

  Repeat this step to fix all the child form EO xmls that have entitlement attributes.
- Recreate the zip file and import it back using Enterprise Manager. For more information about importing metadata files, see "Importing Metadata Files from MDS" Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.

3.1.1.33 Error While Upgrading Oracle Identity Manager Binaries Due to Wrong OPatch version

This issue occurs when you upgrade Oracle Identity Manager binaries to 11*g* Release 2 (11.1.2.2.0). The supported OPatch version for Oracle Identity Manager upgrade is 11.1.0.9.9. Different OPatch version might cause patch application failure. The following error will be displayed in the install logs if incorrect OPatch version is used:

```
OPatch failed with error code 73
]
   stderr=[ApplySession failed: ApplySession failed to prepare the system.
To run in silent mode, OPatch requires a response file for Oracle Configuration
Manager (OCM).
Please run "/oracle/middleware/iam/OPatch/ocm/bin/emocmrsp" to generate an OCM
```

```
response file. The generated response file
can be reused on different platforms and in multiple OPatch silent installs."
```

The workaround for this issue is to ensure that the OPatch version in *OIM_HOME* and *MW_HOME*/oracle_common is 11.1.0.9.9, before you upgrade Oracle Identity Manager binaries to 11.1.2.2.0.

After binary upgrade, check the installer logs at the following location:

- On UNIX: *ORACLE_INVENTORY_LOCATION*/logs

  To find the location of the Oracle Inventory directory on UNIX, check the file *ORACLE_HOME*/oraInst.loc.

- On Windows: *ORACLE_INVENTORY_LOCATION*\logs

  The default location of the Oracle Inventory Directory on Windows is C:\Program Files\Oracle\Inventory\logs.

The following install log files are written to the log directory:

- install*DATE-TIME*_STAMP.log
- install*DATE-TIME*_STAMP.out
- installActions*DATE-TIME*_STAMP.log
- installProfile*DATE-TIME*_STAMP.log
- oraInstall*DATE-TIME*_STAMP.err
- oraInstall*DATE-TIME*_STAMP.log

If any OPatch fails, apply the failed patches manually.

3.1.1.34 Pre-Upgrade Report for OIM Detects Your Existing OIM version as 11.1.2.0.0 Though the Actual Version is 11.1.2.1.0

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) environments which was upgraded from Oracle Identity Manager 11*g* Release 2 (11.1.2.0.0), to 11.1.2.2.0. When you generate the pre-upgrade report, it detects your existing OIM version as 11.1.2.0.0 instead of 11.1.2.1.0. If you check the schema version using the query `select * from schema_version_registry`, it shows 11.1.2.1.0. This occurs if XSD table values are not updated after schema upgrade.

The workaround for this issue is to manually update the version number in the XSD table, and then run the pre-upgrade report again. To do this, update XL_PATCH_BASE 11.1.2.0.0 to XL_PATCH_BASE 11.1.2.1.0 in the XSD table using the following query:

```
update XSD set XSD_VALUE='11.1.2.1.0' where XSD_CODE='XL_PATCH_BASE'
```

3.1.1.35 Exception When Opening a User After Upgrading Oracle Identity Manager

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) to 11*g* Release 2 (11.1.2.2.0).

After you upgrade Oracle Identity Manager to 11.1.2.2.0, when you open a user, the following exception is displayed:

```
javax.servlet.ServletException: OracleJSP error:
oracle.mds.exception.MDSRuntimeException: MDS-00010: DuplicateRefException. In
 document /oracle/iam/ui/runtime/form/view/pages/userCreateForm.jsff there are
 multiple elements with the same ID upfl_user.
```

The workaround for this issue is to add `DataControl=CatalogAMDataControl` entry in the `userDetailsPageDef.xml` file. To do this, complete the following steps:

1. Export the metadata file `userDetailsPageDef.xml` to MDS. The following is the full path to the file to be exported:

   `/oracle/iam/ui/manageusers/pages/mdssys/cust/site/site/userDetailsPageDef.xml`

   For information about exporting metadata files to MDS, see "Exporting Metadata Files to MDS" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

2. Open the exported file in a text editor.
3. Add the entry `DataControl=CatalogAMDataControl`, if it does not exists already.
4. Save the file.
5. Import the `userDetailsPageDef.xml` back into the MDS. For information about importing metadata file, see "Importing Metadata Files from MDS" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

3.1.1.36 Exception When Upgrading Oracle Access Manager System Configurations Using upgradeConfig() Command

This issue occurs if you are upgrading Oracle Access Manager 11*g* Release 2 (11.1.2.0.0) environments which was previously upgraded from 11*g* Release 1 (11.1.1.5.0), to Oracle Access Manager 11*g* Release 2 (11.1.2.2.0).

When you run the `upgradeConfig()` command to upgrade the Access Manager system configurations, the following exception is displayed:

```
oracle.security.am.upgrade.framework.psfe.PSFEFramework process
SEVERE: Exception has occurred while processing featureID: OAMEntityStore.
Stopping the process after calling rollback.
oracle.security.am.upgrade.framework.psfe.PSFEException: Plugin
oracle.security.am.upgrade.framework.psfe.plugin.PolicyEntityPlugin reported
validation failure for featureID: OAMEntityStore
```

The workaround for this issue is as follows:

1. Stop the Administration Server and the Access Manager Managed Server(s) if they are running.
2. Back up the `upgrade.properties` file located at *`$DOMAIN_HOME`*`/config/fmwconfig`. This is the same folder where `oam-config.xml` is located.
3. Run the `upgradeConfig()` command.

3.1.1.37 IllegalArgumentException When Upgrading Oracle SOA Suite as Part of Oracle Identity Manager Upgrade

When you upgrade Oracle SOA Suite to 11*g* Release 1 (11.1.1.7.0) as part of the Oracle Identity Manager upgrade process, the following exception is displayed:

```
Exception [TOPLINK-106] (Oracle TopLink - 11g Release 1 (11.1.1.6.0) (Build
111018)): oracle.toplink.exceptions.DescriptorException
Exception Description: The method [setSuccessStatusType] on the object is throwing
an exception.
Argument: [null]
Internal Exception: java.lang.reflect.InvocationTargetException
Target Invocation Exception: java.lang.IllegalArgumentException: The
successStatusType must be of success type and not equal to null
```

```
Mapping: oracle.toplink.mappings.TransformationMapping[successStatusType]
Descriptor: RelationalDescriptor(oracle.sdpinternal.messaging.AddressImpl -->
[DatabaseTable(ADDRESS)])
```

The workaround for this issue is to apply patch 17565911.

3.2 Migration Issues

This section describes issues related to the following scenarios:

- Migrating Oracle Access Manager 10*g* to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0)
- Migrating Oracle Adaptive Access Manager 10*g* to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.2.0)
- Migrating Oracle Single Sign-On 10*g* to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0)
- Migrating Sun OpenSSO Enterprise 8.0 to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0)
- Migrating Sun Java System Access Manager 7.1 to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0)
- Migrating Oracle Identity Analytics 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0).
- Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0)
- Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0)
- Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0)

3.2.1 Migration Issues and Workarounds

This section describes general issues and workarounds related to the migration scenarios. It includes the following topics:

3.2.1.1 osso.conf Files may be Copied to Alternate File Location If Upgrading Oracle Single Sign-On 10g Fails

This issue occurs when you upgrade Oracle Single Sign-On 10*g* to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0). If errors occurs during the execution of the Upgrade Assistant which require you to re-run the process, there is a possibility that required `osso.conf` files will not be generated, in the location specified in the Upgrade Assistant Summary screen, at the end of the process.

If this occurs, the `osso.conf` files needed to complete the upgrade, can also be found in the following directory:

`<MW_HOME>/user_projects/domains/<Domain_Home>/output/upgrade`

3.2.1.2 Server Logs and Assessment Report for Certain Scenarios Show Only English Messages

Known issue.

The server logs and assessment report shows only English messages when you migrate the following components to Oracle Access Management Access Manager 11g Release 2 (11.1.2.2.0):

- Oracle Access Manager 10*g*
- Sun OpenSSO Enterprise 8.0
- Sun Java System Access Manager 7.1

3.2.1.3 Registering Policy Agent 2.2 Using RREG Fails Due to Unavailability of Agent Template

This issue occurs when you register Policy Agent 2.2 in Oracle Access Management 11.1.2.2.0 Server using Remote Registration tool (RREG), during migration. This is because of the unavailability of the agent template.

The workaround for this issue is as follows:

1. Copy the `oam-admin.ear` from the following directory to a temporary location:

   On Unix: *MW_HOME*`/oam/server/apps/`

   On Windows: *MW_HOME*`\oam\server\apps\`

2. Unpack the `oam-admin.ear` file in any desired location. The `oam-admin.ear` contains `ngam-ui.war` file.
3. Unpack the `ngam-ui.war` file in any desired location. The `ngam-ui.war` contains `oam-migrate.jar` file.
4. Unpack the `oam-migrate.jar` file in any desired location.
5. Go to the following directory from the location where you have unpacked the `oam-migrate.jar`:

   On UNIX: `oracle/security/am/migrate/OpenSSO/resources/templates/`

   On Windows: `oracle\security\am\migrate\OpenSSO\resources\templates\`

6. Complete the following steps depending on the type of 2.2 Policy Agent:

   - **For 2.2 J2EE Agent:**

     On UNIX: Copy the `AMAgent.template` from the directory `../templates/j2eeagents` to the location *MW_HOME*`/`*RReg_Home*`/templates/opensso/j2eeagents`

On Windows: Copy the `AMAgent.template` from the directory `..\templates\j2eeagents` to the location *`MW_HOME`*`\RReg_`*`Home`*`\templates\opensso\j2eeagents`

- **For 2.2 Web Agent:**

  On UNIX: Copy the `AMAgent.template` from the directory `../templates/webagents` to the location *`MW_HOME`*`/RReg_`*`Home`*`/templates/opensso/webagents`

  On Windows: Copy the `AMAgent.template` from the directory `..\templates\webagents` to the location *`MW_HOME`*`\RReg_`*`Home`*`\templates\opensso\webagents`

3.2.1.4 Assessment Report for OAM 10*g* Incremental Migration Shows Artifacts that are not Selected

This issue occurs when you migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.2.0. When you perform incremental migration in `evaluate_only` mode, the assessment report contains the following:

- Authentication schemes that were not selected for migration
- All host identifiers instead of the selected ones

This is a known issue. In this case, extra artifacts of type authentication scheme and host identifiers get migrated; However, this will not cause any adverse impact on the usage of migrated policies.

3.2.1.5 Assessment Report for OAM 10*g* Delta Migration Shows Artifacts that are not Selected

This issue occurs when you migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.2.0. When you perform delta migration, all host identifiers and authentication schemes appear in the assessment report, and the delta migration tries to create all host identifiers and authentication schemes again.

This is a known issue. In this case, extra artifacts of type authentication scheme and host identifiers get migrated; However, this will not cause any adverse impact on the usage of migrated policies.

3.2.1.6 Oracle Access Management 11g Release 2 (11.1.2.0.0) Coexistence, Upgrade, and Migration Supplement

Oracle Fusion Middleware Migration Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) discusses how to migrate various Single Sign-On and Access Management environments to Oracle Access Management 11*g* Release 2 (11.1.2.2.0). You should use this guide for information about upgrade, migration, and coexistence procedures.

If necessary, you can read the following support note for any late-breaking information and changes:

My Oracle Support document ID 1473025.1

4

Oracle Fusion Middleware Administration

This chapter describes issues associated with general Oracle Fusion Middleware administration issues involving Identity Management. It includes the following topics:

- Section 4.1, "General Issues and Workarounds"
- Section 4.2, "Configuration Issues and Workarounds"
- Section 4.3, "Documentation Errata"

4.1 General Issues and Workarounds

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

- Section 4.1.1, "Clarification About Path for OPMN"
- Section 4.1.2, "Fusion Middleware Control May Return Error in Mixed IPv6 and IPv4 Environment"
- Section 4.1.3, "Limitations in Moving from Test to Production"
- Section 4.2.1, "Configuring Fusion Middleware Control for Windows Native Authentication"

4.1.1 Clarification About Path for OPMN

OPMN provides the `opmnctl` command. The executable file is located in the following directories:

- *ORACLE_HOME*/opmn/bin/opmnctl: The opmnctl command from this location should be used only to create an Oracle instance or a component for an Oracle instance on the local system. Any opmnctl commands generated from this location should not be used to manage system processes or to start OPMN.

  On Windows, if you start OPMN using the opmnctl start command from this location, OPMN and its processes will terminate when the Windows user has logged out.

- *ORACLE_INSTANCE*/bin/opmnctl: The opmnctl command from this location provides a per Oracle instance instantiation of opmnctl. Use opmnctl commands from this location to manage processes for this Oracle instance. You can also use this opmnctl to create components for the Oracle instance.

  On Windows, if you start OPMN using the opmnctl start command from this location, it starts OPMN as a Windows service. As a result, the OPMN parent process, and the processes which it manages, persist after the MS Windows user has logged out.

4.1.2 Fusion Middleware Control May Return Error in Mixed IPv6 and IPv4 Environment

If your environment contains both IPv6 and IPv4 network protocols, Fusion Middleware Control may return an error in certain circumstances.

If the browser that is accessing Fusion Middleware Control is on a host using the IPv4 protocol, and selects a control that accesses a host using the IPv6 protocol, Fusion Middleware Control will return an error. Similarly, if the browser that is accessing Fusion Middleware Control is on a host using the IPv6 protocol, and selects a control that accesses a host using the IPv4 protocol, Fusion Middleware Control will return an error.

For example, if you are using a browser that is on a host using the IPv4 protocol and you are using Fusion Middleware Control, Fusion Middleware Control returns an error when you navigate to an entity that is running on a host using the IPv6 protocol, such as in the following situations:

- From the Oracle Internet Directory home page, you select Directory Services Manager from the Oracle Internet Directory menu. Oracle Directory Services Manager is running on a host using the IPv6 protocol.
- From a Managed Server home page, you click the link for Oracle WebLogic Server Administration Console, which is running on IPv6.
- You test Web Services endpoints, which are on a host using IPv6.
- You click an application URL or Java application which is on a host using IPv6.

To work around this issue, you can add the following entry to the /etc/hosts file:

```
nnn.nn.nn.nn  myserver-ipv6 myserver-ipv6.example.com
```

In the example, *nnn.nn.nn.nn* is the IPv4 address of the Administration Server host, myserver.example.com.

4.1.3 Limitations in Moving from Test to Production

Note the following limitations and known problems in moving from a test to a production environment:

- If your environment includes Oracle WebLogic Server which you have upgraded from one release to another (for example from 10.3.4 to 10.3.5), the pasteConfig scripts fails with the following error:

  ```
  Oracle_common_home/bin/unpack.sh line29:
  WL_home/common/bin/unpack.sh No such file or directory
  ```

  To work around this issue, edit the following file:

  ```
  MW_HOME/utils/uninstall/WebLogic_Platform_10.3.5.0/WebLogic_Server_10.3.5.0_
  Core_Application_Server.txt file
  ```

  Add the following entries:

  ```
  /wlserver_10.3/server/lib/unix/nodemanager.sh
  /wlserver_10.3/common/quickstart/quickstart.cmd
  /wlserver_10.3/common/quickstart/quickstart.sh
  /wlserver_10.3/uninstall/uninstall.cmd
  /wlserver_10.3/uninstall/uninstall.sh
  /utils/config/10.3/setHomeDirs.cmd
  /utils/config/10.3/setHomeDirs.sh
  ```

- When you are moving Oracle Virtual Directory, the Oracle instance name in the source environment cannot be the same as the Oracle instance name in the target environment. The Oracle instance name in the target must be different than the name in the source.
- After you move Oracle Virtual Directory from one host to another, you must add a self-signed certificate to the Oracle Virtual Directory keystore and EM Agent wallet on Host B. Take the following steps:

  a. Set the ORACLE_HOME and JAVA_HOME environment variables.

  b. Delete the existing self-signed certificate:

  ```
  $JAVA_HOME/bin/keytool -delete -alias serverselfsigned
    -keystore ORACLE_INSTANCE/config/OVD/ovd_component_
  name/keystores/keys.jks
    -storepass OVD_Admin_password
  ```

  c. Generate a key pair:

  ```
  $JAVA_HOME/bin/keytool -genkeypair
    -keystore ORACLE_INSTANCE/config/OVD/ovd_component_
  name/keystores/keys.jks
    -storepass OVD_Admin_password -keypass OVD_Admin_password -alias
  serverselfsigned
    -keyalg rsa -dname "CN=Fully_qualified_hostname,O=test"
  ```

  d. Export the certificate:

  ```
  $JAVA_HOME/bin/keytool -exportcert
    -keystore ORACLE_INSTANCE/config/OVD/ovd_component_
  name/keystores/keys.jks
    -storepass OVD_Admin_password -rfc -alias serverselfsigned
   -file ORACLE_INSTANCE/config/OVD/ovd_component_name/keystores/ovdcert.txt
  ```

  e. Add a wallet to the EM Agent:

  ```
  ORACLE_HOME/../oracle_common/bin/orapki wallet add
    -wallet ORACLE_INSTANCE/EMAGENT/EMAGENT/sysman/config/monwallet
    -pwd EM_Agent_Wallet_password -trusted_cert
   -cert ORACLE_INSTANCE/config/OVD/ovd_component_name/keystores/ovdcert.txt
  ```

  f. Stop and start the Oracle Virtual Directory server.

  g. Stop and start the EM Agent.

- The copyConfig operation fails if you are using IPv6 and the Managed Server listen address is not set.

  To work around this problem, set the Listen Address for the Managed Server in the Oracle WebLogic Server Administration Console. Navigate to the server. Then, on the Settings for server page, enter the Listen Address. Restart the Managed Servers.

- When you are moving Oracle Platform Security and you are using an LDAP store, the LDAP store on the source environment must be running and it must be accessible from the target during the pasteConfig operation.
- If you have configured WebGate with Oracle HTTP Server Release 11.1.1.6, you must apply the following patch to Oracle HTTP Server before you use the movement scripts:

  ```
  13897557
  ```

- The movement scripts do not support moving any releases of Oracle Identity Manager prior to *Release 11.1.2.1* to another environment, either through the movement scripts or manual steps. In addition, if any releases of Oracle Identity Manager prior to *Release 11.1.2.1* is part of the source environment of other components, the movement scripts for that environment will fail.
- When you are moving Oracle Entitlements Server from a source to a target environment, the `copyConfig` step may fail and display an exception similar to the following in the log file:

  ```
  javax.management.InstanceNotFoundException: java.lang:type=Runtime
  at weblogic.rjvm.ResponseImpl.unmarshalReturn(ResponseImpl.java:237)
  at
  weblogic.rmi.internal.BasicRemoteRef.invoke(BasicRemoteRef.java:223)
  ```

  Before running `copyConfig` on the source environment, you must first set the `env` variable in the shell and restart the source environment. Set the `env` variable as follows, for example:

  ```
  setenv JAVA_OPTIONS
  -Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.WLSMBean
  ServerBuilder
  ```

- After you move Oracle Adaptive Access Manager, the database schema user name for Oracle Adaptive Access Manager will be changed only if OPSS data is not migrated as part of the copyConfig operation (specified using the opssdataexport parameter).
- If the copyConfig operation fails for a domain involving Oracle Identity Manager with the following exception trace, there is a problem that the script encountered in getting MBean server connection for the Oracle Identity Manager Managed Server using the host name as `localhost`:

  ```
  INFO : [PLUGIN][OIM] Mar 22, 2013 7:45:23 AM - CLONE-71019  Executing
  Mbean:MBean
  Name:oracle.iam:type=IAMAppRuntimeMBean,name=IDStoreConfigMBean,Application=oi
  m,ApplicationVersion=11.1.2.0.0.
  INFO : [PLUGIN][OIM] null
  oracle.as.t2p.exceptions.FMWT2PCopyConfigException: java.lang.Exception
          at
  oracle.iam.t2p.OIMT2PCopyConfig.doCopyConfig(OIMT2PCopyConfig.java:87)
          at
  oracle.as.clone.cloner.component.J2EEComponentCreateCloner.getMovableCompsFrom

  PluginImpl(J2EEComponentCreateCloner.java:796)
  .
  .
  .
  ```

  In this situation, analyze and correct the network configuration on the machine. Also check the file /etc/hosts for this network configuration.

- If you are moving an integrated Access Manager and Oracle Adaptive Access Manager environment, you may receive the following errors:

  ```
  ####<Mar 23, 2013 4:38:12 AM PDT> <Error> <Security> <slc01age> <AdminServer>
  <[ACTIVE] ExecuteThread: '0' for queue: 'weblogic.kernel.Default
  (self-tuning)'> <<WLS Kernel>> <> <> <1332502692218> <BEA-090870> <The realm
  "myrealm" failed to be loaded:
  weblogic.security.service.SecurityServiceException: java.lang.AssertionError:
  java.lang.reflect.InvocationTargetException.
  ```

```
weblogic.security.service.SecurityServiceException: java.lang.AssertionError:
java.lang.reflect.InvocationTargetException
```

In this case, take the following steps:

1. Remove the access client password of the IAMSuiteAgent from the Access Manager console and the Oracle WebLogic Server Administration Console deployed on the source environment.
2. Execute the copyConfig script on the source environment.
3. Execute the pasteConfig script on the target environment.

- When you execute the pasteConfig script and the archive contains Oracle Platform Security Services, the script may return the following errors:

```
oracle.security.audit.util.StrictValidationEventHandler handleEvent
WARNING: Failed to validate the xml content. Reason: cvc-complex-type.2.4.b:
The content of element '' is not complete. One of
'{"http://xmlns.oracle.com/ias/audit/audit-2.0.xsd":source}' is expected..
Apr 24, 2013 6:28:29 AM
oracle.security.audit.util.StrictValidationEventHandler handleEvent
WARNING: Failed to validate the xml content. Reason: cvc-complex-type.2.4.b:
The content of element '' is not complete. One of
'{"http://xmlns.oracle.com/ias/audit/audit-2.0.xsd":source}' is expected..
```

  You can ignore these errors.

- When you execute the pasteConfig script, you may see the following error messages in the pasteConfig logs:

```
SEVERE: 2013-10-22 01:06:33.432/953.466 Oracle Coherence GE 3.7.1.1 <Error>
(thread=Configuration Store Observer, member=n/a): Error while starting
 cluster: (Wrapped) java.io.FileNotFoundException:
 config/fmwconfig/.cohstore.jks (No such file or directory)
        at com.tangosol.util.Base.ensureRuntimeException(Base.java:288)
        at com.tangosol.util.Base.ensureRuntimeException(Base.java:269)
 at
com.tangosol.net.ssl.SSLSocketProvider.setConfig(SSLSocketProvider.java:444)
  at
com.tangosol.net.SocketProviderFactory.createProvider(SocketProviderFactory.jav
a:77)
 at
com.tangosol.net.SocketProviderFactory.ensureProvider(SocketProviderFactory.jav
a:152)
 at
com.tangosol.coherence.component.net.Cluster.configureSockets(Cluster.CDB:28)
```

  You can ignore these errors.

- The copyConfig script may return the following warnings:

```
 ======================================================================
 WARNING: Unsupported configuration store version detected. Required
 "11.1.2.2.0" but found "11.1.2.1.0".
 Nov 03, 2013 10:16:41 PM
 oracle.security.am.admin.config.BasicFileConfigurationStore loadConfiguration
 WARNING: Unsupported configuration store version detected. Required
 "11.1.2.2.0" but found "11.1.2.1.0".
 Nov 03, 2013 10:16:42 PM
 oracle.security.am.admin.config.BasicFileConfigurationStore loadConfiguration
 WARNING: Unsupported configuration store version detected. Required
 "11.1.2.2.0" but found "11.1.2.1.0".
```

```
=====================================================================
```

You can ignore these warnings.

- In an environment that contains Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager, the target environment may contain incorrect values for the following data source properties:

  ```
  portNumber
  SID
  serverName
  ```

  These are redundant properties, present in all data sources in the domain, and there is no functional loss from these properties carrying the wrong values.

4.2 Configuration Issues and Workarounds

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

- Section 4.2.1, "Configuring Fusion Middleware Control for Windows Native Authentication"

4.2.1 Configuring Fusion Middleware Control for Windows Native Authentication

To use Windows Native Authentication (WNA) as the single sign-on mechanism between Fusion Middleware Control and Oracle WebLogic Server Administration Console, you must make changes to the following files:

- web.xml
- weblogic.xml

These files are located in the em.ear file. You must explode the em.ear file, edit the files, then rearchive the em.ear file. Take the following steps (which assume that while the front end is on Windows, the em.ear file is on UNIX):

1. Set the JAVA_HOME environment variable. For example:

   ```
   setenv JAVA_HOME /scratch/Oracle/Middleware/jrockit_160_05_R27.6.2-20
   ```

2. Change to the directory containing the em.ear, and explode the file. For example:

   ```
   cd /scratch/Oracle/Middleware/user_projects/applications/domain_name
   JAVA_HOME/bin/jar xvf em.ear em.war
   JAVA_HOME/bin/jar xvf em.war WEB-INF/web.xml
   JAVA_HOME/bin/jar xvf em.war WEB-INF/weblogic.xml
   ```

3. Edit web.xml, commenting out the first login-config block and uncommenting the login-config block for WNA. (The file contains information about which block to comment and uncomment.) When you have done this, the portion of the file will appear as in the following example:

   ```
   <!--<login-config>
        <auth-method>CLIENT-CERT</auth-method>
     </login-config>
   -->
    <!--
     the following block is for Windows Native Authentication, if you are using
    WNA, do the following:
       1. uncomment the following block
       2. comment out the previous <login-config> section.
   ```

```
   3. you also need to uncomment a block in weblogic.xml
-->
  <login-config>
    <auth-method>CLIENT-CERT,FORM</auth-method>
    <form-login-config>
      <form-login-page>/faces/targetauth/emasLogin</form-login-page>
      <form-error-page>/login/LoginError.jsp</form-error-page>
    </form-login-config>
  </login-config>
  <security-constraint>
.
.
.
  <security-role>
    <role-name>Monitor</role-name>
  </security-role>
```

4. Edit weblogic.xml, uncommenting the following block. (The file contains information about which block to uncomment.) When you have done this, the portion of the file will appear as in the following example:

```
<!--
the following block is for Windows Native Authentication, if you are using
WNA, uncomment the following block.
-->
 <security-role-assignment>
    <role-name>Admin</role-name>
    <externally-defined/>
  </security-role-assignment>
.
.
.
  <security-role-assignment>
    <role-name>Deployer</role-name>
    <externally-defined/>
  </security-role-assignment>
```

5. Rearchive the em.ear file. For example:

```
JAVA_HOME/bin/jar uvf em.war WEB-INF/web.xml
JAVA_HOME/bin/jar uvf em.war WEB-INF/weblogic.xml
JAVA_HOME/bin/jar uvf em.ear em.war
```

4.3 Documentation Errata

This section contains the following documentation errata for the *Oracle Fusion Middleware Administrator's Guide* and the *Oracle Fusion Middleware High Availability Guide*:

- Section 4.3.1, "Documentation Errata for the Oracle Fusion Middleware Administrator's Guide"
- Section 4.3.2, "Documentation Errata for the Oracle Fusion Middleware High Availability Guide"

4.3.1 Documentation Errata for the *Oracle Fusion Middleware Administrator's Guide*

There are no documentation errata for the *Oracle Fusion Middleware Administrator's Guide* at this time.

4.3.2 Documentation Errata for the *Oracle Fusion Middleware High Availability Guide*

This section contains the following documentation errata for the *Oracle Fusion Middleware High Availability Guide* for 11g Release 2 (11.1.2.1.0), Part Number E28391-04:

4.3.2.1 JRockit SDK Not Certified for IDM

In section 8.3.3.1.1, "Install Oracle WebLogic Server", step 5., On the Choose Products and Components screen, select only Oracle JRockit SDK and click Next, is incorrect. It should state "On the Choose Products and Components screen, select a certified JDK. Refer to the Oracle certification matrix for the appropriate JDK to select. See `http://www.oracle.com/technetwork/middleware/downloads/fmw-11gr1certmatrix.xls`.

5 Oracle Access Management

This chapter describes issues associated with Oracle Access Management. It includes the following topics:

Note: For late-breaking changes and information, see My Oracle Support document ID 1537796.1.

5.1 General Issues and Workarounds

This section describes general issues and workarounds organized by specific Access Manager services. If you do not find a service-related topic (Access Portal, for example), there are no general issues at this time.

The following topics are included:

5.1.1 General Issues and Workarounds: Access Manager

This topic describes general issues and workarounds for Oracle Access Management Access Manager (Access Manager). It includes the following topics:

- Section 5.1.1.36, "Authentication Fails: WNA Challenge, Active Directory, Users with Non-ASCII Characters."
- Section 5.1.1.37, "Simple Mode is Not Supported for JDK 1.6 and AIX."
- Section 5.1.1.38, "User Might Need to Supply Credentials Twice with DCC-Enabled WebGate."

5.1.1.1 BasicScheme Does Not Redirect to Failure URL when Using Internet Explorer Browser

When using Internet Explorer (version 8 and above) and the authentication scheme is set to "BasicScheme" with a failure URL configured at the Application Domain, the user is not redirected to the failure URL after the maximum number of failed attempts is reached. An error is displayed without redirecting to the failure URL or the OAM system error page.

To workaround, set the MaxRetryLimit on the OAM side to a value less than or equal to 3 and set the OverrideRetryLimit challenge parameter to 1, 2 or 3. The user is then prompted only the number of times configured and on failure, redirection to the configured failure URL occurs.

5.1.1.2 Error During Federation Configuration After Upgrade From PS1 to PS2

IAM Suite is the OOTB Application Domain created when OAM 11.1.2 is installed. This Application Domain can be renamed after installation but when upgrading OAM to 11.1.2.2.0, it must be renamed back to **IAM Suite** otherwise the upgrade operation will fail with the following error seen in the WLS admin logs.

```
java.lang.NullPointerException
at
oracle.security.am.common.policy.tools.upgrade.r2ps2.bootstrap.FedR2PS2Bootstr
apHandler.createFedAuthnResource(FedR2PS2BootstrapHandler.java:505)
at
oracle.security.am.common.policy.tools.upgrade.r2ps2.bootstrap.FedR2PS2Bootstr
apHandler.doBootstrap(FedR2PS2BootstrapHandler.java:151)
at
oracle.security.am.common.policy.tools.upgrade.r2ps2.bootstrap.R2PS2BootstrapH
elper.doBootstrap(R2PS2BootstrapHelper.java:70)
at
oracle.security.am.common.policy.tools.PolicyComponentLifecycle.initialize(Pol
.
icyComponentLifecycle.java:99)
```

If the **IAM Suite** Application Domain has been renamed after installation, it is required to rename it back to its original **IAM Suite** name prior to beginning the upgrade process. After the upgrade process is complete, the name can be changed back to its custom name.

5.1.1.3 Time Between Access Manager and Mobile Device Must Be Synced

Time sync is not supported between mobile devices and the Access Manager server therefore the OTP code generated by the mobile device will not be validated by Access Manager if the time is not synced.

5.1.1.4 User Account Not Locked After Invalid Attempts

In an integrated Access Manager-Identity Manager environment in which Active Directory is the back-end identity store, a user account will not be locked after the configured number of authentication attempts with invalid credentials.

5.1.1.5 UseCaseInsensitiveResourceMatch Doesn't Work in PS2

The UseCaseInsensitiveResourceMatch flag (which controls case sensitive resource pattern matching) does not work. To workaround this issue, change the configuration key name from "UseCaseInsensitiveResourceMatch" to "USE_CASE_INSENSITIVE_RESOURCE_MATCH".

5.1.1.6 Additional Setting Required for Case Insensitive Policy Resource Matching

A setting must be added to oam-config.xml and configured in order to workaround an iussue with the "Case Insensitive Policy Resource Matching" option. The additional setting that must be added under PolicyService -> OAMPolicyProvider -> properties is:

```
<Setting Name="USE_CASE_INSENSITIVE_RESOURCE_MATCH
  "Type="xsd:boolean">true</Setting>
```

5.1.1.7 Cookie Based Session Management Available Only for 11g WebGates

Client-side session management (also referred to as cookie-based session management) is available only for 11g WebGate agents.

5.1.1.8 Logout URL Value in DCC Profile Doesn't Clear Browser Session

If the DCC WebGate profile for an 11g APACHE WebGate contains the default value for the Logout URL (/logout.html), DCC cookies are not cleared when logging out; thus the session still exists within the browser. If the default value of Logout URL is removed from the DCC WebGate profile, log out works as expected.

5.1.1.9 Automated Policy Synchronization Not Enabled and Supports Only Policy Artifacts

Multi-Data Center and the Automated Policy Synchronization feature only supports policy aritifacts and not system artifacts. Additionally, Automated Policy Synchronization is disabled out of the box. To enable, set the Java system property as -DENABLE_ENTITY_JOURNAL=true.

5.1.1.10 Not All User Attributes Are Available For Post Authentication Rules

Not all user attributes can be used when writing Post Authentication Rules. For this release, only userId, userDN and guid are available.

5.1.1.11 Partner Registration Fails When Using WebSphere Application Server

If deployed in the Websphere Application Server, partner registration using the Access Manager Console or rreg fails when an offline wsadmin command (for example, Oam.createUserIdentityStore) is executed with the AdminServer and the oam_server running. To rectify, restart the servers after the execution of any offline wsadmin command.

5.1.1.12 Attributes That Have No Value Defined Substituted With NULL

If an attribute is defined in the Identity Store with no value, a NULL is substituted for the parameter in responses that refer to it. For example, if parameter ${user.deptname} has no defined value in the Identity Store for the specified user, the response at runtime will be NULL. (In R1, NONE was used.)

5.1.1.13 Access Denied When LDAP Authentication Module Changed to OID

To workaround this error, use idmConfigTool.sh to provision values for the WebLogic administration server host, port and WebLogic user (including password) into the OAM config-store as a post-installation step. Use these values while accessing IDS MBeans instead of the user/password of the subject that is logged in.

5.1.1.14 SHA2 Support Limitations

The following are known limitations of SHA-2 support per design.

- WebGate will not work in simple mode when using SHA-2 certificates.
- SHA-2 support is not provided for 32-bit platform.
- SHA-224 certificates are not supported.

5.1.1.15 Granular Timeout Doesn't Work If Cookie-based SME Enabled

The granular timeout functionality does not work when Cookie-based SME is enabled (set to `true`). This is expected behavior.

5.1.1.16 OCSP Not Available for x509 Plugin on WAS

OCSP is not available for x509 Plugin when Access Manager 11g is deployed on WebSphere Application Server containers.

5.1.1.17 upgradeConfig() Fails On WebSphere Application Server

upgradeConfig() fails on WebSphere Application Server when used in some shells. For example, when using the tcsh shell, the wsadmin.sh script on WebSphere does not export ORACLE_HOME. Thus, it fails and prints a "Could not identify correct ORACLE_HOME location" error message. The following procedure can be used to workaround this issue.

1. Use the bash shell to launch $ORACLE_HOME/common/bin/wsadmin.sh.

   This is not an issue when using the bash shell.

2. Explicitly export the value of ORACLE_HOME.

   ```
   export ORACLE_HOME
   ```

3. Modify $ORACLE_HOME/common/bin/wsadmin.sh to export ORACLE_HOME.

5.1.1.18 JDK7 Required for OAM 10g/OAM 11g Coexistence

Configuring OAM10g and OAM11g (coexistence is a new feature of R2PS2), JDK7 is required for two security JARs that it contains.

5.1.1.19 X.509 Minimum Keylength Increases with JDK 7u 40

JDK 7u40 increases the minimum keylength for X.509 from 512 bits to 1024 bits. (This change has been made to discourage use of key length that are considered weak by current standards.) To change this default behavior, consult the JDK documentation.

5.1.1.20 LDR_PRELOAD64 Flag Required For 64-bit Platform Non-OHS WebGate Agents on IBM Power AIX 6.1 & 7.1

Support for 64-bit platform Non-OHS WebGate agents on IBM Power AIX 5.3, 6.1 and 7.1 has been added. The Apache Server will not start or work with AIX 6.1 and 7.1 unless the LDR_PRELOAD64 flag is set using the following command:

```
export LDR_PRELOAD64=libclntsh.so
```

5.1.1.21 ASDK Returns Incorrect Version Details

The 11gR2 PS1 ASDK has incorrect version details:

- The `getSDKVersion()` API returns a 11.1.2.0.0 value instead of a 11.1.2.1.0 value.
- The name of the `ofm_oam_sdk_generic_11.1.2.1.0_disk1_1of1.zip` disk might be `ofm_oam_sdk_generic_11.1.2.0.0_disk1_1of1.zip`.

5.1.1.22 Benign Exceptions Observed

The following benign exception might be seen on the Administration and Managed servers. It can be ignored.

```
java.lang.NoClassDefFoundError:
oracle/security/am/engines/rreg/common/RegistrationRequest
  at java.lang.Class.getDeclaredMethods0(Native Method)
  at java.lang.Class.privateGetDeclaredMethods(Class.java:2427)
  at java.lang.Class.privateGetPublicMethods(Class.java:2547)
  at java.lang.Class.getMethods(Class.java:1410)
  at oracle.security.am.admin.config.mgmt.beanimpl.AMBootstrap.
    isBootstrapCandidate (AMBootstrap.java:191)
  at oracle.security.am.admin.config.mgmt.beanimpl.AMBootstrap.
    invokeBootstrapMethods(AMBootstrap.java:146)
  at oracle.security.am.admin.config.mgmt.beanimpl.AMBootstrap.
    doServerBootstrap(AMBootstrap.java:106)
  at oracle.security.am.admin.config.mgmt.beanimpl.AMBootstrap
    load(AMBootstrap.java:247)
```

The following benign exception is seen in the AdminServer-diagnostic.log file. It does not impact the Administration Console functionality and can be ignored.

```
oracle.mds.exception.ReadOnlyStoreException: MDS-01273:
  The operation on the resource /oracle/oam/ui/adfm/DataBindings.cpx failed
  because source metadata store mapped to the namespace / DEFAULT is read only.
  at
oracle.mds.core.MDSSession.checkAndSetWriteStoreInUse(MDSSession.java:2495)
  at
oracle.mds.core.MDSSession.checkAndSetWriteStoreInUse(MDSSession.java:2548)
  at oracle.mds.core.MDSSession.getMutableMO(MDSSession.java:3493)
  at oracle.mds.core.MDSSession.getMutableMO(MDSSession.java:1660)
  at oracle.mds.core.MDSSession.getMutableMO(MDSSession.java:1546)
  at oracle.adfdt.model.mds.MDSApplicationService.findApplication
     (MDSApplicationService.java:57)
  at oracle.adfdt.model.mds.MDSModelDesignTimeContext.initServices
     (MDSModelDesignTimeContext.java:232)
  at oracle.adfdt.model.mds.MDSModelDesignTimeContext.<init>
     (MDSModelDesignTimeContext.java:82)
  at oracle.adfdt.mds.MDSDesignTimeContext.<init>
     (MDSDesignTimeContext.java:66)
  at oracle.adf.view.rich.dt.DtAtRtContext.<init>
     (DtAtRtContext.java:22)
  at oracle.adf.view.rich.dt.Page.<init>(Page.java:535)
  at oracle.adf.view.rich.dt.Page.getInstance(Page.java:80)
  at oracle.adf.view.page.editor.customize.ComposerPageResolver.getPageObject
     (ComposerPageResolver.java:200)
  at oracle.adfinternal.view.page.editor.contextual.event.ContextualResolver.
     getPageDefinition(ContextualResolver.java:1229)
  at oracle.adfinternal.view.page.editor.contextual.event.ContextualResolver.
     <init>(ContextualResolver.java:129)
```

5.1.1.23 Can't Use WLST Commands For Federated SSO Password Policy

WLST commands cannot be used for adding, editing or deleting the federated SSO password policy profile until the following modifications have been made to the oam-config.xml file manually.

1. Back up the existing oam-config.xml file.
2. Find Setting Name="UserProfileInstance" in the file and add the following entry as a child of the "UserProfileInstance" setting.

```
<Setting Name=""NEW_PROFILE" Type="htf:map">
  <Setting Name="PasswordPolicyAttributes" Type="htf:map">
   <Setting Name="FORCED_PASSWORD_CHANGE" Type="xsd:boolean">true</Setting>
   <Setting Name="USER_ACCOUNT_DISABLED" Type="xsd:boolean">true</Setting>
   <Setting Name="PASSWORD_EXPIRED" Type="xsd:boolean">true</Setting>
   <Setting Name="TENANT_DISABLED" Type="xsd:boolean">true</Setting>
   <Setting Name="USER_ACCOUNT_LOCKED" Type="xsd:boolean">true</Setting>
  </Setting>
</Setting>
```

   For edit and delete, the changes should be made on the existing profile entry in oam-config.xml.

3. Increment the oam-config.xml "Version" setting and persist the changes.

5.1.1.24 Exception Logged on Accessing Resource

A CertPathValidatorException is seen in the Access Manager diagnostic log when accessing a Resource. For example:

```
[2013-03-12T21:39:09.281-07:00] [oam_server1] [ERROR] [OAMSSA-12117]
[oracle.oam.engine.authn] [tid: WebContainer : 3] [ecid: disabled,0]
[APP: oam_server_11.1.2.0.0] Cannot validate the user certificate.[[
java.security.cert.CertPathValidatorException: The certificate issued
by O=My Company Ltd, L=Newbury, ST=Berkshire, C=GB is not trusted;
internal cause is:
  java.security.cert.CertPathValidatorException: Certificate chaining error
  at
com.ibm.security.cert.BasicChecker.<init>(BasicChecker.java:111) at
```

5.1.1.25 Can't Get Static Method UserSession.getSessionAttributes()

The static getSessionAttributes() method does not retrieve all Session attributes for a user - only those which have been set using the ASDK.

5.1.1.26 Consecutive Logins in Multiple Tabs Doesn't Work for WebGate

FORM Cache Mode should be used to support multi-tab browser behavior. By default, it is set to COOKIE Mode.

5.1.1.27 Unsupported Items in WebSphere Trust Association Interceptor

The following items are unsupported in the Access Manager WebSphere Trust Association Interceptor (TAI) when compared to the Access Manager WebLogic Server Id Asserter.

- Access Manager WAS TAI does not support SAML assertions based on the OAM_IDENTITY_ASSERTION header.

- OAM WAS TAI does not support the Identity Context. Identity Context is supported based on the OAM_IDENTITY_ASSERTION header by Access Manager WebLogic Server Identity Asserter.

5.1.1.28 Logged Error During OAM Server Configuration Test

After running `idmConfigTool.sh -configOAM`, two WebGate profiles are created: `Webgate_IDM` and `Webgate_IDM_11g`; both are 11g. When validating each Access Manager server configuration using the `oamtest` tool, the Administration Console displays the connection status correctly but a long error/exception for each WebGate is logged. This error log is expected and can be ignored.

5.1.1.29 Simple Policy Not Migrated After Complete Migration

When performing a fresh incremental migration or a delta incremental migration after a complete migration, Simple Policy are not migrated. This issue is due to a Maximum Session Time lapse. Either restart the Administration Server or change the value of Maximum Session Time to more than 120 minutes.

5.1.1.30 Available Services Page Won't Open In Localized Internet Explorer 9

When accessing the OAM Administration Console localized for `cn` or `jp` using Internet Explorer 9, double-clicking the Available Services text will not open the related page. Clicking the folder icon as opposed to the text will work. Or use Internet Explorer 8 or Firefox to workaround. If it works when using Internet Explorer 7, you can force OAM to run in Explorer 7 compatibility mode. See the PDF called **Run ADF Faces applications with IE 9 in IE 8 compatibility mode** at Oracle Technology Network.

5.1.1.31 RSA Plugin Removed From System

The RSA plugin has been removed as a system plugin. The functionality can still be accessed by installing and using a custom RSA plugin.

5.1.1.32 Create Provider Manually When Extending OIM Domain

If extending the Oracle Identity Manager domain by adding Oracle Access Management Access Manager, the 'OIMAuthenticationProvider' will be deleted. When integrating OIM and OAM using idmConfigTool -configOIM, providers are automatically reordered as required. If not using idmConfigTool -configOIM, the provider needs to be created manually.

5.1.1.33 Unable to Access "/" Context Root if Protected by OSSO Agent for 11g OHS

mod_osso agents shipped with 11g OHS cannot be configured to protect the @ context root '/'.

5.1.1.34 Starting Access Manager When Protected by Oracle Entitlements Server Throws Exception

You will get a runtime exception when starting an instance of Access Manager protected by Oracle Entitlements Server. The exception can be ignored.

5.1.1.35 Access Tester Does Not Work with Non-ASCII Agent Names

Register a WebGate with Access Manager using a non-ASCII name. In the Access Tester, enter the valid IP Address, Port, and Agent ID (non-ASCII name), then click Connect.

Connection testing fails.

5.1.1.36 Authentication Fails: WNA Challenge, Active Directory, Users with Non-ASCII Characters

Configure Access Manager to use Kerberos Authentication Scheme with WNA challenge method, and create a non-ASCII user in Microsoft Active Directory.

Problem

An exception occurs when trying to get user details to populate the subject with the user DN and GUID attributes. Authentication fails and an error is recorded in the OAM Server log when a non-ASCII user in Active Directory attempts to access an Access Manager-protected resource:

```
... Failure getting users by attribute : cn, value ....
```

Cause

The username in the attribute is passed without modification as a java string.

Solution

Non-ASCII users can access the resource protected by Kerberos WNA scheme by applying the following JVM system property in the startManagedWeblogic.sh script in $*DOMAIN_HOME*/bin:

```
-Dsun.security.krb5.msinterop.kstring=true
```

5.1.1.37 Simple Mode is Not Supported for JDK 1.6 and AIX

Simple mode is not supported with JDK 1.6 and on AIX platforms. Use Open or Cert mode instead.

5.1.1.38 User Might Need to Supply Credentials Twice with DCC-Enabled WebGate

Problem

When you have a Detached Credential Collector-enabled WebGate combined with a resource WebGate, the user might have to provide credentials twice. This can occur when login is triggered with a URL that results in an internal forward by Oracle HTTP Server.

Workaround

To resolve this issue, you can use following workaround:

1. Edit the httpd.conf file to add rewrite rules that redirect the browser for directory access (before WebGate configuration include) For example:

   ```
   RewriteEngine On
   RewriteRule     ^(.*)/$         "$1/welcome-index.html"      [R]
   ```

2. SSL-enabled Web server: Repeat these rules under SSL configuration.

5.1.2 General Issues and Workarounds: Security Token Service

This topic describes general issues and workarounds for Oracle Access Management Security Token Service (Security Token Service). It includes the following topics:

- Section 5.1.2.1, "STS Does Not Honor The Lifetime Sent In RequestSecurityToken."

- Section 5.1.2.2, "Click On Security Token Service Column Throws Exception."
- Section 5.1.2.3, "Issues with Searches and Non-English Browser Settings."

5.1.2.1 STS Does Not Honor The Lifetime Sent In RequestSecurityToken

Security Token Service does not process the Lifetime sent in the WS-Trust RequestSecurityToken message. Rather, the WS-Trust RequestSecurityTokenResponse contains the Lifetime per the configured token validity time in the Oracle Security Token Service Issuance Template.

5.1.2.2 Click On Security Token Service Column Throws Exception

When adding a new Attribute Name Mapping during the creation of a New Requester Profile in the Security Token Service section of the Access Manager Administration Console, an error message indicating an Unsupported Operation Exception can be displayed when clicking twice on a column titled **Row No.**

5.1.2.3 Issues with Searches and Non-English Browser Settings

Security Token Service searches might not return the expected result when the browser language is set to a non-English language. For example, this occurs when setting the:

- Partner Type field to **`Requester`**, **`Relying Party`** or **`Issuing Authority`** in the Requesters, Relying Party or Issuing Authorities screens
- **`Token Type`** to **`Username`** on the Token Issuance Templates screen when the Oracle Access Manager Administration Console browser setting is non-English
- **`Token Type`** to **`Username`** on the Token Validation Templates screen when the Oracle Access Manager Administration Console browser setting is non-English

When the browser language is English, the search returns expected results.

5.1.3 General Issues and Workarounds: Identity Federation

This topic describes general issues and workarounds for Oracle Access Management Identity Federation (Identity Federation). It includes the following topic:

- Section 5.1.3.1, "Errors when WebGate has Credential Collector Option Enabled"

5.1.3.1 Errors when WebGate has Credential Collector Option Enabled

This problem is seen in the following situation:

- WebGate fronts a resource.
- The "Allow Credential Collector Operations" option is checked for that WebGate.
- The resource is protected by a policy using FederationScheme.

Due to this issue, when requesting access to the resource, the server returns a 200 with a URL where the browser will post the request to that URL using the POST, while the browser should have been redirected through a 302.

To resolve this issue, for WebGate agents fronting resources protected with the FederationScheme, disable the "Allow Credential Collector Operations" option.

5.1.4 General Issues and Workarounds: OAuth Services, and Mobile and Social

This topic describes general issue and workarounds for Oracle Access Management Mobile and Social. It includes the following topics:

5.1.4.1 Mobile and Social Does not Support the Native Android OS Browser

Mobile and Social supports the Mozilla Firefox and Google Chrome browsers on Android devices. The following issues are known to occur if the native Android OS browser is used.

- The login web page rendered by the native browser does not allow the user to enter a username or password.
- If a mobile single sign-on app is not installed on the mobile client, the native Android browser is unable to redirect the user to a page where the user can authenticate. This is due to a limitation in the native browser's JavaScript support.

5.1.4.2 Internet Explorer Users Need to Enable Protected Mode

Internet Explorer users who do not enable Protected Mode cannot sign in with a Social Identity Provider. Instead, an empty page will display.

To work around this issue in Internet Explorer versions 8 and 9, enable Protected Mode:

1. From the Internet Explorer menu choose **Tools > Internet Options > Security**.
2. Select **Enable Protected Mode** and restart the browser.

5.1.4.3 Google Language Menu can Cause the Sign-in Page Flow to Display in Multiple Languages

If a user who signs in with Google selects a different language from the on-screen menu, Google redirects the page request outside of the request flow managed by Mobile and Social. Consequently, the log-in pages that Google generates may be in a different language than the pages generated by Mobile and Social. Mobile and Social provides translated pages based on the browser's language settings. To avoid having pages display in different languages, users should only use their browser's preferred language settings to make changes.

5.1.4.4 The Mobile and Social Settings Pane can be Dragged out of View

In the Oracle Access Management console, when viewing the "Mobile and Social Settings" tree in the navigation pane, it is possible to click and drag the contents of this pane out of view.

To workaround this issue refresh the page or logout and login again.

5.1.4.5 The White Pages App Requires at Least Version 11.1.2.2.2 of Oracle Access Management

A bug that prevents user profile attributes from displaying in the White Pages app is fixed as of Bundle Patch 2.

5.1.5 General Issues and Workarounds: Access Portal Service

This topic describes general issue and workarounds for Oracle Access Management Access Portal Service. It includes the following topics:

- Section 5.1.5.1, "Credentials Not Captured In Basic Authentication (Modal) Dialogs"

5.1.5.1 Credentials Not Captured In Basic Authentication (Modal) Dialogs

In a clean browser session in which the JavaScript client has not yet set the partner ID cookie, credentials entered into a basic authentication (modal) dialog are not captured.

There is currently no workaround for this issue.

5.2 Configuration Issues and Workarounds

This section describes configuration issues and their workarounds organized around specific services. To streamline your experience, only services with an issue are included. For example, Identity Context has no known issues at this time and is not included. The following topics are included:

- Section 5.2.1, "Configuration Issues and Workarounds: Access Manager"
- Section 5.2.2, "Configuration Issues and Workarounds: Security Token Service"
- Section 5.2.3, "Configuration Issues and Workarounds: Identity Federation"
- Section 5.2.4, "Configuration Issues and Workarounds: OAuth Services, and Mobile and Social"

5.2.1 Configuration Issues and Workarounds: Access Manager

This topic describes configuration issues and workarounds for Oracle Access Management Access Manager (Access Manager). It includes the following topics:

- Section 5.2.1.1, "OAM Migration Doesn't Create All Data Sources"
- Section 5.2.1.2, "Password Validation Scheme Defaults to LDAP after Upgrade"
- Section 5.2.1.3, "Using Plugins Between IBM HTTP Server and WebSphere"
- Section 5.2.1.4, "Using ObAccessClient Results in SDK Initialization Failure"
- Section 5.2.1.5, "Configuring oamtai.xml for Multiple WebGates"
- Section 5.2.1.6, "obLockedOn Attribute Missing From Oracle Internet Directory"
- Section 5.2.1.7, "OAM 10g WebGates Used with OAM 11g Need JavaScript"
- Section 5.2.1.8, "Enabling OpenSSO Agent Configuration Hotswap"

5.2.1.1 OAM Migration Doesn't Create All Data Sources

If the OAM 10g environment that is being migrated to 11g has multiple database instances configured in a Directory Server Profile and some of them share the same `displayName` value, the migration process does not convert all of the database instances in Data Sources to the new environment. To workaround, rename the 10g environment database instances such that no two instances in the Directory Server Profile have the same `displayName` value.

5.2.1.2 Password Validation Scheme Defaults to LDAP after Upgrade

After upgrading Access Manager to version 11gR2 PS1, the Password Validation Scheme is not set to the Password Policy Validation Module. Use the Console to set the Password Validation Scheme to the Password Policy Validation Module.

5.2.1.3 Using Plugins Between IBM HTTP Server and WebSphere

Communication between the IBM HTTP Server (IHS) and WebSphere Application Server (WAS) is made possible by installing and configuring plugins that are available with IHS. The following steps describe the installation and configuration process.

1. During IHS installation, install the out-of-the-box plugin.
2. After installation, navigate to the IHS plugin directory at (for example, *$IHS_HOME*\Plugins\config\webserver1) and verify that the `plugin-cfg.xml` configuration file is available.
3. Modify `plugin-cfg.xml` as follows and save the file.
   a. Add the virtual host ports from which IHS can be accessed.

```
<VirtualHostGroup Name="default_host">
<!-- Include active IHS port details required for connecting to OAM on WAS
-->
<!--  <VirtualHost Name="*:9004"/> -->
  <VirtualHost Name="*:8080"/>
    <VirtualHost Name="*:17777"/>
</VirtualHostGroup>
```

   b. Add <ServerCluster> with the appropriate details comprising of the respective server entries where the resource is deployed.
   c. Add <UriGroup> tag for the respective serverclusters.

```
<UriGroup Name="oamserver1_Cluster_URIs">
    <Uri Name="/oam/*"/>
</UriGroup>
```

   d. Add the corresponding <Route> tag for the respective <UriGroup> tag.

```
<Route ServerCluster="oamserver1_Cluster"
  UriGroup="oamserver1_Cluster_URIs" VirtualHostGroup="default_host"/>
```

4. Add the respective VirtualHost entries in WebSphere by navigating to Environment ->Virtual Hosts -> default_hosts -> Host Alias using the IBM console.

5.2.1.4 Using ObAccessClient Results in SDK Initialization Failure

Using an ObAccessClient (created with the 11.1.1.5.0 Access Manager Console) to create the AccessClient for the 11g ASDK (11.1.1.7.0, 11.1.2.0.0 and above) results in the following error because the older `ObAccessClient.xml` file has Boolean settings expressed as `true/false` rather than numeric:

```
oracle.security.am.asdk.AccessClient initialize SEVERE:
    Oracle Access SDK initialization failed.
```

To workaround, copy the original (older) `ObAccessClient.xml` from *DOMAIN_HOME*/output/*AGENT_NAME* to the ASDK configuration directory (configLocation). You may also manually edit the newer `ObAccessClient.xml` to change the Boolean values ("true/false") to numeric values (0/1).

5.2.1.5 Configuring oamtai.xml for Multiple WebGates

There is only one `oamtai.xml` file for a single WebSphere instance. In a case where the deployment contains multiple WebGate profiles protecting applications deployed on the same WebSphere application server - for example, a mix of 10g and 11g WebGates - the OAM Trust Association Interceptor is required to be configured as below.

- Irrespective of the number of WebGates in the deployment, the agent profile defined in the file should be an OAM10g type.
- The assertion type should be defined as HeaderBasedAssertion.

5.2.1.6 obLockedOn Attribute Missing From Oracle Internet Directory

After upgrading Access Manager from 11gR2 to 11gR2 PS1, the `obLockedOn` attribute will be missing from the Oracle Internet Directory. Use the following steps to add this attribute back to the OID.

1. Manually add the obLockedOn attribute to the schema.
2. Import the LDIF to OID using the ldapmodify command.
3. Edit the `oam_user_write_acl_users_oblockedon_template.ldif` to give oamSoftwareUser permission to modify obLockedOn.

   Replace %s_UsersContainerDN% with User Search Base and replace %s_ GroupsContainerDN% with Group Search Base.
4. Import the modified `oam_user_write_acl_users_oblockedon_template.ldif`.

5.2.1.7 OAM 10g WebGates Used with OAM 11g Need JavaScript

When Oracle Access Manager 10g WebGates are used with Oracle Access Management 11g, the *`webgate_install_directory`*`/oamsso/logout.html` page needs JavaScript code to initiate redirection to the Oracle Access Management 11g server logout page. This page, after logging out with the WebGate cookie also clears the 11g session. When migrating Oracle Access Manager 10g WebGates, follow the procedure documented in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

5.2.1.8 Enabling OpenSSO Agent Configuration Hotswap

To enable OpenSSO Agent configuration hotswap, make sure the opensso agents have the following properties in the `Miscellaneous` properties section of the agent's registration in the OpenSSO Proxy on OAM Server, and the agent servers are restarted:

J2ee Agents: `com.sun.identity.client.notification.url =http://<`*`AGENT_SERVER_HOST`*`>:<`*`AGENT_SERVER_PORT`*`>/agentapp/notification`

Web Agents:

`com.sun.identity.client.notification.url=http://<`*`AGENT_SERVER_HOST`*`>:<`*`AGENT_SERVER_PORT`*`>/UpdateAgentCacheServlet?shortcircuit=false`

Not Supported for Web Agents:
`com.sun.identity.agents.config.change.notification.enable=true`

Restart the OAM Server hosting the agent.

5.2.2 Configuration Issues and Workarounds: Security Token Service

This topic describes configuration issues and their workarounds for Oracle Access Management Security Token Service (Security Token Service). It includes the following topics:

- Section 5.2.2.1, "Create Like (Duplicate) Does Not Copy All Properties of Original Template"
- Section 5.2.2.2, "No Console Support Removing Partner Encryption or Signing Certificates"

5.2.2.1 Create Like (Duplicate) Does Not Copy All Properties of Original Template

Security Token Service Create Like (duplicate) button does not copy some properties on the original Issuing Authority Profile template (the Security and Attribute Mapping sections, for instance).

The Administrator must manually enter the necessary configuration items into the newly created Issuing Authority Profile:

1. From the Oracle Access Management Console Launch Pad, click **Token Issuance Templates** under **Security Token Service**.
2. Select an existing Issuance Template
3. Click the Create Like (duplicate) button.
4. Create the new copied Issuance Template and manually enter the necessary configuration items in the newly created Template.

5.2.2.2 No Console Support Removing Partner Encryption or Signing Certificates

Oracle Access Management Console does not provide a way to remove a signing or encryption certificate that was set for an Security Token Service Partner.

The Administrator must manually delete these using the following WLST commands:

To delete the signing certificate of an Security Token Service Partner

```
deletePartnerSigningCert
```

To delete the encryption certificate of an Security Token Service Partner

```
deletePartnerEncryptionCert
```

5.2.3 Configuration Issues and Workarounds: Identity Federation

This topic describes configuration issues and their workarounds for Oracle Access Management Identity Federation (Identity Federation). It includes the following topics:

- Section 5.2.3.1, "Provider Search Text Fields do an Exact Match Search"
- Section 5.2.3.2, "Incorrect Error Message when an Invalid Signing Certificate is Uploaded"

5.2.3.1 Provider Search Text Fields do an Exact Match Search

Users should be aware that in the Oracle Access Management Console, the Identity Provider search screen does an exact match (==) for the ProviderId and Partner name fields, rather than a "contains" search.

Although it is an exact match, the user can employ "*" as a wild card in searches.

5.2.3.2 Incorrect Error Message when an Invalid Signing Certificate is Uploaded

While creating/editing an IdP, if you upload an invalid file for a signing certificate, you will see a `Null pointer exception` error message instead of a proper message indicating that the file does not contain a certificate.

5.2.4 Configuration Issues and Workarounds: OAuth Services, and Mobile and Social

This topic describes configuration issues and their workarounds for Oracle Access Management Mobile and Social (Mobile and Social). It includes the following topics:

5.2.4.1 The OAuth 3-Legged Flow With External LDAP Requires a WebGate Proxy

A WebGate proxy is required to use the OAuth 3-Legged authorization flow with an external LDAP directory server. To address this issue, follow the steps in the "Configuring a WebGate to Protect the OAuth Service" section of the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

5.2.4.2 OAuth Scope Supersets Should be Defined Before Subsets

When defining OAuth scopes on the Resource Server Configuration page, add scope supersets (UserProfile.*) before subsets (UserProfile.users). You can only select scope supersets from the dropdown list after you remove scope subsets from the list.

5.2.4.3 Steps Required to Localize the Register Page

Because of a design change, attribute names on the Register page are in English and are not localized to other languages. To translate this page, use the following steps to modify the attribute name values using the Oracle Access Management console.

1. Open the Oracle Access Management console Launch Pad and click **Social Identity** under **Mobile and Social**.

   Open the Application Profile, for example *OAMApplication*.

2. Go to the **User Attribute Display Name** list in the **Registration Service Details with Application User Attribute Mapping** section.

   Replace the values in English with localized values.

3. Save your changes by clicking **Apply** on the *OAMApplication* page.

4. Open the Register page and confirm that the page shows the correct localized values.

5.2.4.4 Mobile Clients do not Translate Error Messages Sent by the Server

The Mobile and Social server sends error messages to the mobile clients in the language that is configured in the server locale language settings. The mobile clients cannot translate server error messages to a different language.

5.2.4.5 Yahoo Identity Provider Does not Return First Name and Last Name

The Yahoo social identity provider does not return `firstname` and `lastname` values following user authentication. To work around this issue, change the following Mobile and Social mappings in the Oracle Access Management console:

1. Open the Application Profile for editing.

   Click Next until the Social Identity Provider configuration page opens.

2. Open the **Application User Attribute Vs Social Identity Provider User Attributes Mapping** section.

3. In the **Attribute Mapping** section, click **Yahoo** to select it in the **Social Identity Provider** list.

4. Configure the values as follows:

   - Locate **firstname** in the **Application User Attribute** column and in the corresponding **Social Identity Provider User Attributes** column, choose **nickname**.
   - Locate **lastname** in the **Application User Attribute** column and in the corresponding **Social Identity Provider User Attributes** column, choose **fullname**.

5. Save the Application Profile.

5.2.4.6 Once Set, Jail Breaking "Max OS Version" Setting Cannot be Empty

Once you assign a value to the Jail Breaking Detection Policy "Max OS Version" setting, you cannot remove the value and leave the field empty. Per the documentation, the Max OS Version field is used to configure the maximum iOS version to which the Jail Breaking policy applies. If the value is empty, a maximum iOS version number is not checked so the policy applies to any iOS version higher than the value specified for Min OS Version. Once set, however, the value cannot go back to being empty. To work around this issue, set a value for the Max OS Version field.

5.3 Oracle Access Management Console Issues

This section documents issues that affect the Oracle Access Management Console. It includes the following topics:

- Section 5.3.1, "Content Missing from Help Screens"
- Section 5.3.2, "Messages Sent From the Server to the Client Can Appear in a Foreign Language"

5.3.1 Content Missing from Help Screens

The Agent Registration Quick Start Wizard Help screen is missing content.

5.3.2 Messages Sent From the Server to the Client Can Appear in a Foreign Language

If the OAM Server and the Oracle Access Management Console client are configured for different locales, the server will report error messages to the client in whichever language the server is configured for.

5.4 Documentation Errata

Oracle manuals describing and showing Oracle Access Management 11.1.2 and related services, including these Release Notes, incorrectly refer to the OAM Server (the former name of the Access Manager Server). However, in the next release of Oracle 11.1.2 books, the term OAM Server will be replaced by AM Server (Access Manager Server).

This section describes documentation errata for Oracle Access Management-specific manuals. It includes the following titles:

- Section 5.4.1, "Oracle Fusion Middleware Administrator's Guide for Oracle Access Management"
- Section 5.4.2, "Oracle Fusion Middleware Developer's Guide for Oracle Access Management"

5.4.1 Oracle Fusion Middleware Administrator's Guide for Oracle Access Management

Documentation errata for Oracle Fusion Middleware Administrator's Guide for Oracle Access Management is organized into the following topics:

- Section 5.4.1.1, "Max Session Time Description Update"
- Section 5.4.1.2, "Creds Parameter Lists 10g and 11g Format Without Specifics"
- Section 5.4.1.3, "Incorrect OpenSSO Agent Configuration Directory Documented"
- Section 5.4.1.4, ""Integrating Microsoft SharePoint Server With Access Manager" Chapter Requires an Update"

5.4.1.1 Max Session Time Description Update

The Max Session Time element description in Chapter 16 Registering and Managing OAM 11g Agents has been updated.

5.4.1.2 Creds Parameter Lists 10g and 11g Format Without Specifics

Format of **creds=** challenge parameter lists 10g format (`creds:source$name`) in an 11g book. The 10g format was removed and text added to explain 11g format.

5.4.1.3 Incorrect OpenSSO Agent Configuration Directory Documented

Replaced the incorrect configuration directory path WebTier_Middleware_Home/Oracle_WT1/instances1/config/OHS/ohs1/config/ with the correct one: PolicyAgent-base/AgentInstance-Dir/config

5.4.1.4 "Integrating Microsoft SharePoint Server With Access Manager" Chapter Requires an Update

This chapter lists support for Microsoft SharePoint Server 2010. As of March 2014, Access Manager with a 10g WebGate supports both Microsoft SharePoint Server 2010 and Microsoft SharePoint Server 2013. Other versions of Microsoft SharePoint Server are not supported in this release.

5.4.2 Oracle Fusion Middleware Developer's Guide for Oracle Access Management

There are no documentation errata for Oracle Fusion Middleware Developer's Guide for Oracle Access Management.

6 Oracle Entitlements Server

This chapter describes issues associated with Oracle Entitlements Server. It includes the following topics:

- Section 6.1, "General Issues and Workarounds"
- Section 6.2, "Configuration Issues and Workarounds"
- Section 6.3, "Documentation Errata"

6.1 General Issues and Workarounds

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

- Section 6.1.1, "Searching for a Resource Created in the Authorization Policy Manager of a Derby Template Domain Gives an Error"
- Section 6.1.2, "Grant Missing Manage and View Permissions for a Delegated Administrator"

6.1.1 Searching for a Resource Created in the Authorization Policy Manager of a Derby Template Domain Gives an Error

If the Oracle Entitlements Server domain was created using Derby template, when you search for a resource created in the Authorization Policy Manager, the console displays an error message:

```
JPS-10000: There was an internal error in the policy store
```

The workaround is to use the search management API.

6.1.2 Grant Missing Manage and View Permissions for a Delegated Administrator

There are issues related to missing `MANAGE - POLICY`, `VIEW - APPLICATION_ROLE` / `RESOURCE` / `RESOURCE_TYPE` / `ENTITLEMENT` permissions that are implicitly "granted" or implied when privileges, such as "view and manage," are granted to the delegated administrator. For example, in order to create a policy as a delegated administrator, the `MANAGE - POLICY` permission is required, and because the delegated administrator must search for an application role, resource, and/or entitlement, he requires the `VIEW - APPLICATION_ROLE` / `RESOURCE` / `RESOURCE_TYPE` / `ENTITLEMENT` permissions.

To work around these issues, grant `ALL` permissions to the delegated administrator. This includes domain delegated permissions as well.

6.2 Configuration Issues and Workarounds

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

- Section 6.2.1, "x.509 Certificates Key Length Limitation for JDK1.7.0_40 and Later"

6.2.1 x.509 Certificates Key Length Limitation for JDK1.7.0_40 and Later

For `JDK1.7.0_40` and later, the use of `x.509` certificates with RSA keys less than 1024 bits in length is restricted.

Because the Oracle Entitlements Server Administration Server key size is 512 bits, if you use `JDK1.7.0_40` and later, you must remove the key size limitation. To do this, modify the default value `jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 1024` to `jdk.certpath.disabledAlgorithms=MD2` in the `java.security` file in the `java_home/jre/lib/security` directory.

If you do not perform this workaround, the following scenarios may fail:

- Creation of all Security Modules except WebLogic Security Module in controlled-push mode
- Controlled-push WebLogic Security Module registration with Oracle Entitlements Server

6.3 Documentation Errata

There is no documentation errata at this time.

7

Oracle Adaptive Access Manager

This chapter describes issues associated with Oracle Adaptive Access Manager.

It includes the following topics:

7.1 OAAM Admin Issues and Workarounds

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

7.1.1 Session Details

This section describes session detail issues and workarounds.

7.1.1.1 Searching for Devices May Not Work Correctly in Some Cases

Searching by "User Friendly Name" Does Not Return Any Results If Device Is Secure

In the Device tab of the User Details and Devices Details pages, searching by **User Friendly Name** does not return any results if the device is secure (`Registered` is `true`).

Searching by "Any Device" as the Device Type Does Not Return Any Results

In the Device tab of the Details pages (for example, User Details: Devices tab, Fingerprint Details: Devices tab, or Alert Details: Device tab) searching by **Any Device** as the Device Type does not return any results even when there are devices.

Searching by "null" as the User Friendly Name Returns All Results

In the Device tab of the User Details and Devices Details pages, searching by **User Friendly Name** with the value of `null` returns all results. The search should return only devices with the name `null`.

7.1.1.2 Sorting by "Last Used On Date" Does Not Work for Devices

In the Device tab of the Session Details pages, sorting by **Last Used On Dates** does not work. The devices remain sorted by the Device ID as default.

7.1.1.3 Session Details Are Not Displayed Correctly

Fingerprint Data Shows Incorrect Number of Fingerprints in the Session in the User Details Page

In the Profile Data section of the User Details page, the number of fingerprints in the session is shown as **0** in Fingerprint Data even when fingerprint data for the session is available and can be displayed in the Fingerprint Data tab.

When Multiple Transactions Are Created the Policy Data Becomes Out of Sync

If multiple transactions are created in a session and corresponding pre- and post-transaction policies are executed, the policy data in the Session Details page becomes out of sync. For example, if in the same session, there were 5 transactions which triggered different rules that in turn generated different types of alerts, the session details page data is not displayed correctly in the corresponding checkpoints.

7.1.1.4 Labeling Issues

Checkpoint and Transaction ID Selection Options Do Not Indicate the Data to be Selected

In the Session Details Transaction and Checkpoint panels, the selection buttons are labeled **`Select Row 1`** instead of more meaningful labels to the user. For example, the labels could be **`Select Row 1`** ***`Checkpoint_name`*** in the Checkpoint panel or **`Select Row 1 Transaction ID`** ***`Transaction_id`*** for the Transaction panel. Currently, the user must traverse the table to know the kind of data he is selecting.

Checkpoint and Transaction Filters Included as Table Column Headers

In the Session Details page, the following tables have filters:

- Checkpoints results table
- Transactions results table

The filters along with the real column header are listed as column headers; as a result, the screen reader (JAWS) reads both when traversing through a table.

7.1.1.5 User Interface Issues

Scrollbar Is Missing from Session Details Page When Screen Resolution is Low

The Session Details page does not display scrollbars which may prevent you from viewing the Alerts summary in the Checkpoint details panel.

High and Medium Alert Level Colors Do Not Meet Minimum Color Contrast Ratio

In the Alert section of Checkpoint Details in the Session Details page, the **High** and **Medium** color coded alerts do not meet the minimum color contrast ratio of 4.5:1.

The **High** text contrast is 4.0:1.

The **Medium** text contrast is 1.97:1.

To work around this issue, enable High Contrast mode in Windows and OAAM.

7.1.2 Bulk Editing for Closing CSR Cases Shows Agent Case Dispositions

Bulk edit for closing CSR cases displays dispositions related to Agent cases.

7.2 OAAM Command Line Tool (CLI) Issues and Limitations

This section describes OAAM Command Line Tool (CLI) issues and workarounds. It includes the following topic:

- Section 7.2.1, "OAAM CLI Scripts Failing If File-Based CSF Is Used"

7.2.1 OAAM CLI Scripts Failing If File-Based CSF Is Used

When running the OAAM command line tool (CLI), you cannot use a file-based CSF (`oaam.csf.useMBeans` is set to `False`). CLI cannot retrieve the credentials required to run the CLI scripts from the CSF and an access control exception is shown.

This is a known issue, and the workaround for this issue is to run CLI using a repository-based CSF with MBeans (`oaam.csf.useMBeans` is set to `True`).

For details about CSF with MBeans, see "Configure OAAM Database Details with CSF with MBeans" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

7.3 Multi-Language Support Issues and Limitations

This section describes multi-language support issues and limitations. It includes the following topics:

- Section 7.3.1, "OAAM Admin Console Contains Garbled Characters When Supplementary Characters are Used"
- Section 7.3.2, "KBA Multi-Language Support Issues"

7.3.1 OAAM Admin Console Contains Garbled Characters When Supplementary Characters are Used

The OAAM Admin Console may contain garbled characters when supplementary characters are used.

7.3.2 KBA Multi-Language Support Issues

This section describes issues associated with multi-language support in KBA.

Duplicate Entries in the List of Categories

The **Category** drop-down list in the New Questions page may display multiple entries of the same categories in different languages.

Category Names are Displayed in English Irrespective of How the Category Name Was Entered in the Filter

If the browser language is set to English, the search results in the Question search page display the category name in English irrespective of the language you entered the category name in.

Unable to Search KBA Question by Category in Different Locale

When searching for KBA questions in the OAAM Admin Console, the **Category** and **Locale** filters do not work when used together. Examples are as follows:

- In a browser set for English, if the user searches with "Parejo" as the **Category** and "Spanish" as the **Locale**, the search results display KBA questions, but the category is shown as "Significant Other." The correct locale is not displayed.
- In a browser set for Spanish, the search results display Spanish KBA questions with "Parejo" as the category but the locale is shown as English. If the user searches by the combination of "Parejo" and "Espanol," the search results display no records.

7.4 Test to Production (T2P) Issues and Limitations

This section describes T2P issues and limitations. It includes the following topic:

- Section 7.4.1, "During the OAAM Plug-in Paste Configuration Process an Incorrect Message Is Shown When Steps are Skipped"

7.4.1 During the OAAM Plug-in Paste Configuration Process an Incorrect Message Is Shown When Steps are Skipped

During the OAAM plug-in paste configuration operation if the OAAM domain does not exist, the paste configuration steps are skipped and the following message is displayed:

```
Not valid OAAM Domain. Skipping OAAM-specific copy configuration steps.
```

`copy configuration steps` should be changed to `paste configuration steps`.

7.5 API Issues

This section describes API issues and limitations. It includes the following topics:

- Section 7.5.1, "setUserDevices API Does Not Work Correctly in Some Cases"
- Section 7.5.2, "getUserDevices API Returns Success Status for Invalid User ID"

7.5.1 setUserDevices API Does Not Work Correctly in Some Cases

setUserDevices API Does Not Work When Certain Inputs are Null

`setUserDevices` does not work correctly when certain inputs are null. The issues are as follows:

- When an element in the `UserDevice` array is `null` but the rest are valid elements, `setUserDevices` returns an unexpected error and none of the devices are updated.
- When the Device Map ID is null in the `UserDevice` object, `setUserDevices` returns a status of `Success` and the other valid devices are updated.

setUserDevices API Returns An Empty List When User Friendly Name Contains Special Characters

`setUserDevices` returns a null object when the User Friendly Name contains special characters.

7.5.2 getUserDevices API Returns Success Status for Invalid User ID

`getUserDevices` returns a status of `Success` for an invalid user ID.

7.6 Documentation Errata

There is no documentation errata at this time.

8

Oracle Privileged Account Manager

This chapter describes issues associated with Oracle Privileged Account Manager. It includes the following topics:

- General Issues and Workarounds
- Configuration Issues and Workarounds
- Documentation Errata

8.1 General Issues and Workarounds

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

- Section 8.1.1, "No Translation (Messages or Help) Support for OPAM Command Line Tools"
- Section 8.1.2, "idmconfigtool Does Not Create OPAM Admin Roles in Groups Container"
- Section 8.1.3, "Deprecated Features for Oracle Privileged Account Manager Restful API"
- Section 8.1.4, "Thread Count Continuously Increases During Oracle Privileged Session Manager Session Checkouts"
- Section 8.1.5, "Unlimited Tablespace Privilege Missing When Using Oracle Database 12.1"
- Section 8.1.6, "Session Checkout Does Not Appear In "My Checkouts""
- Section 8.1.7, "Improve User and Group Search Performance"
- Section 8.1.8, "Database Connections Leaked from Oracle Privileged Account Manager Server"

8.1.1 No Translation (Messages or Help) Support for OPAM Command Line Tools

Oracle Privileged Account Manager command-line tool messages and help were not translated in the Oracle Privileged Account Manager 11.1.2.0.0 release.

Translation support for the Oracle Privileged Account Manager command-line tool messages and help will be provided after the 11.1.2.0.0 release.

8.1.2 idmconfigtool Does Not Create OPAM Admin Roles in Groups Container

When you execute the steps to create Oracle Privileged Account Manager Admin Roles, the roles are created under `IDSTORE_SEARCHBASE` instead of `IDSTORE_`

GROUPSEARCHBASE in the properties file that is passed into the idmConfigTool. This result makes configuring an authenticator against that identity store more complex, and it diverges from the process that is documented in the "Preparing the Identity Store" section of the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.

Workaround: To address this issue, apply BLR patch #16570348. You can download this patch from My Oracle Support at the following location:

http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info

After applying this patch, the idmConfigTool will work as documented in the Administrator's Guide.

8.1.3 Deprecated Features for Oracle Privileged Account Manager Restful API

The following table lists the Oracle Privileged Account Manager RESTful APIs that were available in the Oracle Fusion Middleware 11g Release 2 (11.1.2.1.0) release and have been deprecated in 11g Release 2 (11.1.2.2.0). In addition, this table lists the new, equivalent APIs and provides links to topics in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager* that describe how to use the new APIs.

Deprecated API (11gr2 11.1.2.1.0)	New API (11gr2 11.1.2.2.0)	Refer to This Topic
Show Service Account Password in the Target Resource	Show Service Account Password in the Target Resource	"Show Service Account Password" in the "Target Resource" section.
Show Password in the Account Resource	Show Password in Account Resource	"Show Password" in the "Account Resource" section.
Show Password History in the Account Resource	Show Password History in Account Resource	"Show Password History" in the "Account Resource" section.
Search Accounts in the UI Resource	Search Accounts in Account Resource	"Search Accounts" in the "Account Resource" section.
Search Assigned Accounts in the UI Resource	Search Assigned Accounts in Account Resource	"Search Assigned Accounts" in the "Account Resource" section.
Get All Checked Out Accounts in the UI Resource	Get All Checked Out Accounts in Account Resource	"Get All Checked Out Accounts" in the "Account Resource" section.

8.1.4 Thread Count Continuously Increases During Oracle Privileged Session Manager Session Checkouts

To prevent thread counts from continuously increasing as Oracle Privileged Session Manager session checkouts progress, you must implement the following idle connection timeouts for each Unix target node so that when a connection has been idle for 20 minutes, it will be closed:

```
ClientAliveInterval 600
ClientAliveCountMax 2
```

Where the ClientAliveInterval value is in seconds.

For example, on Linux, you must edit the /etc/ssh/sshd_config file to add these parameters.

Note: For more information about the `ClientAliveInterval` and `ClientAliveCountMax` keywords, refer to the `sshd_config` UNIX man page.

8.1.5 Unlimited Tablespace Privilege Missing When Using Oracle Database 12.1

Oracle Privileged Account Manager operations fail with a database error when you use Oracle Database 12.1.0.1 or higher. This error is displayed in the Oracle Privileged Account Manager server logs and is similar to the following:

```
<Error> <oracle.idm.opam> <BEA-000000>
<OPAMSQLManager.executeUpdateStatementSQLException occurred SQLErrorCode=1950
SQLErrorMesg=ORA-01950: no privileges on tablespace 'DEV_OPAM_BINSTORE'>
```

Oracle Database removed the `Unlimited Tablespace` privilege that was assigned to the `Resource` DB role, starting with the 12.1 release. The removal of this privilege has caused issues for Oracle Privileged Account Manager operations. For a description of the Oracle Database 12.1 release changes, refer to the following:

http://docs.oracle.com/cd/E16655_01/network.121/e17607/release_changes.htm#DBSEG941

Workaround: Login to Oracle Database using SQLPLUS as the `SYS` user. Run the following SQL command to grant unlimited tablespace to the Oracle Privileged Account Manager schema user:

```
grant unlimited tablespace to <opam_schema>;
```

For example, if the Oracle Privileged Account Manager schema name is *dev_opam*, then you would run the following command:

```
grant unlimited tablespace to dev_opam;
```

8.1.6 Session Checkout Does Not Appear In "My Checkouts"

Session Checkouts will not appear in My Checkouts unless the same (case sensitive) username used to log in to the Oracle Privileged Account Manager GUI Console is also used to initiate the session.

8.1.7 Improve User and Group Search Performance

Oracle Privileged Account Manager's identity store searches may not perform well when searching large user bases.

Oracle Privileged Account Manager performs a `contains` search when looking up users and groups in the identity store. A `contains` search can be expensive for some identity stores because the `contains` indexes may not be present or may not perform well. Also, when performing user searches, Oracle Privileged Account Manager looks for the given search keyword in the user's login ID, mail, firstname, and lastname. Looking for multiple attributes in a user search may also cause performance issues, which can manifest themselves as timeout issues when searching in the identity store.

Workaround: To address this issue, apply BLR patch #18621722.

This patch changes the default search behavior for identity store searches. After applying this patch, Oracle Privileged Account Manager performs a "`beginswith`" search for both user and group lookups by default. However, this search behavior is configurable through the Oracle Privileged Account Manager Console. The Server

Configuration page now has an **Identity Store search filter** configuration parameter. The allowed values for this parameter are, `beginswith` or `contains`.

Also, user attribute searches are now limited to just one attribute — the login ID.

You can download BLR patch #18621722 from My Oracle Support at the following location:

`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info`

8.1.8 Database Connections Leaked from Oracle Privileged Account Manager Server

Oracle Privileged Account Manager server operations can fail with an error message similar to the following:

```
<Reached maximum capacity of pool "opamDS", making "0" new resource instances
instead of "1".>
```

This error happens when the Oracle Privileged Account Manager server runs out of database connections. If the WebLogic connection pool max size is set to a very low value, such as 15, then concurrent usage frequently exceeds this limit and causes this issue. You can fix this issue by increasing the connection pool max size. In rare cases, the background threads that Oracle Privileged Account Manager uses to enforce Password Policies and Usage Policies can leak database connections. This situation happens inconsistently because the leak only occurs in race conditions.

Workaround: To address this issue, apply BLR patch #18347777. You can download this patch from My Oracle Support at the following location:

`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info`

8.2 Configuration Issues and Workarounds

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

- Section 8.2.1, "Use Absolute Paths While Running configureSecurityStore.py With -m Join"
- Section 8.2.2, "Upgrade: CSF Mapping Does Not Get Imported"

8.2.1 Use Absolute Paths While Running configureSecurityStore.py With -m Join

The Config Security Store fails to create the policy store object when using variables such as `ORACLE_HOME` and `MW_HOME` while running `wlst.sh` using `configureSecurityStore.py` with `-m join`.

Always use absolute paths for `ORACLE_HOME` and `MW_HOME` while running the command for `-m join`.

8.2.2 Upgrade: CSF Mapping Does Not Get Imported

Oracle Privileged Account Manager privileged accounts can optionally contain CSF mappings to synchronize account credentials with the Oracle Credential Store Framework (see "Adding CSF Mappings" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*).

The Oracle Privileged Account Manager command line tool (CLI) `export` command does not export these optionally configured CSF mappings to the exported XML file.

As a result, if you export Oracle Privileged Account Manager data to XML and import the data back from the exported XML, then the CSF mappings will be missing.

Workaround: You must manually update the CSF mappings as follows:

1. Use the CLI `retrieveaccount` command to retrieve the account details, including the CSF mappings. (See "`retrieveaccount` Command" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.)
2. Use the `retrieveaccount` command to fetch and save details about the relevant accounts.
3. Export the data by using the `export` command.
4. Import the data by using the `import` command.
5. Use the saved account details to manually update the CSF mappings for relevant accounts. (See "Adding CSF Mappings" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*).

8.3 Documentation Errata

This section contains documentation errata for the following publications:

- *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Patching Guide for Identity and Access Management*

8.3.1 *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*

Currently, there are no documentation issues to note for the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.

8.3.2 *Oracle Fusion Middleware High Availability Guide*

This section contains documentation errata for the *Oracle Fusion Middleware High Availability Guide*.

In the *Oracle Fusion Middleware High Availability Guide* for 11g Release 2 (11.1.2.1.0), Part Number E28391-04, update the following:

- In sections 9.8.5.3 and 9.8.5.4.1, the *Installing and Configuring Oracle Identity and Access Management* guide release number should read "11.1.2.1.0".
- In section 9.8.5.4.1, Configuring Oracle Identity Management on OPAMHOST1, after Item 2 (Install the Oracle Identity and Access Management software), add the following step: "Optionally, Oracle Privileged Account Manager can operate with Oracle Database TDE (Transparent Data Encryption) mode. For more information, see Section 9.4, Optional: Enabling TDE in Oracle Privileged Account Manager Data Store in the guide *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
- At the end of section 9.8.5.4.5, Starting Oracle Privileged Account Manager on OPAMHOST1, add the following item: "For more information, see sections 9.9, Assigning the Application Configurator Role to a User and 9.10, Optional: Setting Up Non-TDE Mode in the guide *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. Section 9.10 Optional: Setting Up Non-TDE

Mode is required only if you did not set up TDE as section 9.8.4.1 explains in the guide *Installing and Configuring Oracle Identity and Access Management*.

8.3.3 *Oracle Fusion Middleware Patching Guide for Identity and Access Management*

This section contains documentation errata for the *Oracle Fusion Middleware Patching Guide for Identity and Access Management* 11g Release 2 (11.1.2.1.0), Part Number E36789-02.

The order of sections provided for patching Oracle Privileged Account Manager in the *Oracle Fusion Middleware Patching Guide for Identity and Access Management* must be corrected. When patching Oracle Privileged Account Manager you must perform the steps in the following order:

1. Enable TDE in Oracle Privileged Account Manager Data Store ***or***
   Configure Non-TDE Mode
2. Import Pre-Upgrade OPAM Data

Consequently, the sections provided in the *Oracle Fusion Middleware Patching Guide for Identity and Access Management* must be rearranged as follows:

- 3.7.5 "Optional: Enabling TDE in Oracle Privileged Account Manager Data Store"
- 3.7.6. "Optional: Configuring Non-TDE Mode"
- 3.7.7 "Importing Pre-Upgrade OPAM Data"

9

Oracle Identity Navigator

This chapter describes issues associated with Oracle Identity Navigator. There are no known issues at this time.

10 Oracle Identity Manager

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

10.1 Patch Requirements

This section describes patch requirements for Oracle Identity Manager 11*g* Release 2 (11.1.2.2). It includes the following sections:

> **Note:** For information about any additional patches that you must apply, see Section 1.5, "Downloading and Applying Required Patches"

10.1.1 Obtaining Patches From My Oracle Support (Formerly OracleMetaLink)

To obtain a patch from My Oracle Support (formerly OracleMetaLink), go to following URL, click **Patches and Updates**, and search for the patch number:

https://support.oracle.com/

10.1.2 Patch Requirements for Oracle Database 11g (11.1.0.7)

Table 10–1 lists patches required for Oracle Identity Manager 11*g* Release 2 (11.1.2) configurations that use Oracle Database 11*g* (11.1.0.7). Before you configure Oracle Identity Manager 11*g*, be sure to apply the patches to your Oracle Database 11*g* (11.1.0.7) database.

Table 10–1 Required Patches for Oracle Database 11g (11.1.0.7)

Platform	Patch Number and Description on My Oracle Support
UNIX / Linux	7614692: BULK FEATURE WITH 'SAVE EXCEPTIONS' DOES NOT WORK IN ORACLE 11G
	7000281: DIFFERENCE IN FOR ALL STATEMENT BEHAVIOR IN 11G
	8327137: WRONG RESULTS WITH INLINE VIEW AND AGGREGATION FUNCTION
	8617824: MERGE LABEL REQUEST ON TOP OF 11.1.0.7 FOR BUGS 7628358 7598314
Linux x86 64-bit	8545377: ORA-1780 RAISED WHEN CURSOR_SHARING=FORCE
Windows 32 bit	8689191: ORACLE 11G 11.1.0.7 PATCH 16 BUG FOR WINDOWS 32 BIT
Windows 64 bit	8689199: ORACLE 11G 11.1.0.7 PATCH 16 BUG FOR WINDOWS (64-BIT AMD64 AND INTEL EM64T)
Oracle Solaris on SPARC 64-bit	8545377: ORA-1780 RAISED WHEN CURSOR_SHARING=FORCE

Note: The patches listed for UNIX/Linux in Table 10–1 are also available by the same names for Solaris SPARC 64 bit.

10.1.3 Patch Requirements for Oracle Database 11*g* (11.2.0.1.0)

Table 10–2 lists the required patch for Oracle Identity Manager 11*g* Release 2 (11.1.2.2) configurations that use Oracle Database 11*g* (11.2.0.1.0).

Table 10–2 Required Patch for Oracle Database 11g (11.2.0.1.0)

Platform	Patch Number and Description on My Oracle Support
Linux x86 64-bit	8545377: ORA-1780 RAISED WHEN CURSOR_ SHARING=FORCE

10.1.4 Patch Requirements for Oracle Database 11*g* (11.2.0.2.0)

If you are using Oracle Database 11*g* (11.2.0.2.0), make sure that you download and install the appropriate version (based on the platform) for the RDBMS Patch Number 9776940. This is a prerequisite for installing the Oracle Identity Manager schemas.

Table 10–3 lists the patches required for Oracle Identity Manager 11*g* Release 2 (11.1.2) configurations that use Oracle Database 11*g* Release 2 (11.2.0.2.0). Make sure that you

download and install the following patches before creating Oracle Identity Manager schemas.

Table 10–3 Required Patches for Oracle Database 11g (11.2.0.2.0)

Platform	Patch Number and Description on My Oracle Support
Linux x86 (32-bit) Linux x86 (64-bit) Oracle Solaris on SPARC (64-bit) Oracle Solaris on x86-64 (64-bit)	RDBMS Patch#13004894.
Microsoft Windows x86 (32-bit)	Bundle Patch 2 [Patch#11669994] or later. The latest Bundle Patch is 4 [Patch# 11896290].
Microsoft Windows x86 (64-bit)	Bundle Patch 2 [Patch# 11669995] or later. The latest Bundle Patch is 4 [Patch# 11896292].
All platforms	Patch 12419331: Database PSU 11.2.0.2.3 on top of 11.2.0.2.0 Base Release.

If this patch is not applied, then problems might occur in user and role search and manager lookup. In addition, search results might return empty result.

10.1.5 Patch Requirements for Oracle Database 11*g* (11.2.0.3.0)

Table 10–4 lists the patches required for Oracle Identity Manager 11*g* Release 2 (11.1.2.2) configurations that use Oracle Database 11g (11.2.0.3.0).

Table 10–4 Required Patches for Oracle Database 11g (11.2.0.3.0)

Platform	Patch Number and Description on My Oracle Support
Linux x86, 32-bit, and 64-bit	14019600: MERGE REQUEST ON TOP OF 11.2.0.3.0 FOR BUGS 13004894 13370330 13743357
Solaris, HP-UX, IBM AIX:	14019600: MERGE REQUEST ON TOP OF 11.2.0.3.0 FOR BUGS 13004894 13370330 13743357
Microsoft Windows 32-bit	13783452: ORACLE 11G 11.2.0.3 PATCH 4 BUG FOR WINDOWS 32 BIT
Microsoft Windows 64-bit	13783453: ORACLE 11G 11.2.0.3 PATCH 4 BUG FOR WINDOWS (64-BIT AMD64 AND INTEL EM64)

10.1.6 Patch Requirements for Oracle Database 11*g* (11.2.0.4.0)

Table 10–5 lists the patch required for Oracle Identity Manager 11*g* Release 2 (11.1.2.2) configurations that use Oracle Database 11*g* (11.2.0.4.0).

Table 10–5 Required Patch for Oracle Database 11g (11.2.0.4.0)

Platform	Patch Number and Description on My Oracle Support
All platforms	17501296: UNABLE TO DELETE ROWS FROM TABLE WITH TEXT INDEX AFTER UPGRADE TO 11.2.0.4

10.1.7 Patch Requirements for Oracle Database 10*g* (10.2.0.3, 10.2.0.4, and 10.2.0.5)

In Oracle Database 10*g*, problems are encountered when creating materialized view using CONNECT_BY_ROOT clause. This is because the CONNECT_BY_ROOT operator is not available in Oracle Database 10*g* (10.2).

To resolve this issue, use the patches listed in Table 10–6:

Table 10–6 Required Patches for Oracle Database 10g (10.2.0.3 and 10.2.0.4)

Oracle Database Release	Patch Number and Description on My Oracle Support
10.2.0.3.0	7012065: BLR BACKPORT OF BUG 6908967 ON TOP OF VERSION 10.2.0.3.0 (BLR #81973)
10.2.0.4.0	8239552: BLR BACKPORT OF BUG 6908967 ON TOP OF 10.2.0.4.0 (BLR #113173)
10.2.0.4 and 10.2.0.5	8545377: ORA-1780 RAISED WHEN CURSOR_ SHARING=FORCE

10.1.8 Patch Upgrade Requirement

While applying the patch provided by Oracle Identity Manager, the following error is generated:

```
ApplySession failed: ApplySession failed to prepare the system.
```

OPatch version 11.1.0.8.1 must be upgraded to version 11.1.0.8.2 to meet the version requirement.

See "Obtaining Patches From My Oracle Support (Formerly OracleMetaLink)" on page 10-2 for information about downloading OPatch from My Oracle Support.

10.1.9 Patch Requirement for BI Publisher 11.1.1.7.1

For information about patch requirement for BI Publisher 11.1.1.7.1, see Section 2.2.2, "Mandatory Patches Required for Installing Oracle Identity Manager".

10.1.10 Patch Requirement for SOA 11.1.1.7.0

For information about patch requirement for SOA 11.1.1.7.0, see Section 2.2.2, "Mandatory Patches Required for Installing Oracle Identity Manager".

10.1.11 Patch Requirement for SSL with JDK 7u40 or Later

In an Oracle Identity Manager environment in which SSL is enabled, JDK 7u40 or later is used, and SSL is configured by using the default setting as described in section "Enabling SSL for Oracle Identity Manager By Using Default Setting" of the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*, apply Oracle WebLogic Server patch 13964737.

10.1.12 Obtaining the Latest Bundle Patch

You must download and apply the latest Bundle Patch for Oracle Identity Manager 11*g* Release 2 (11.1.2.2). To do so:

1. Log in to My Oracle Support web site at the following URL:

   `https://support.oracle.com`

2. Click the **Knowledge** tab.

3. Search the article titled `Master Note on Fusion Middleware Proactive Patching - Patch Set Updates (PSUs) and Bundle Patches (BPs) (Doc ID 1494151.1)`.

4. Download and apply the appropriate Bundle Patch by following the instructions in the article. The row for 'Oracle Identity Manager (OIM) 11gR2' in the Proactive Patch Table provides information about the Bundle Patches for the current release of Oracle Identity Manager.

10.2 What's New in Oracle Identity Manager 11*g* Release 2 (11.1.2.2)

Oracle Identity Manager 11*g* Release 2 (11.1.2.2) has the following key new features:

- Access Policy Harvesting for Reconciled Accounts
- Dynamic Organization Membership
- Hierarchical Entitlements
- Catalog Auditing
- Archiving/Purge Support for Entities
- Draft Request Support
- Additional Information in Requests
- Account and Entitlement Dependency Handling
- Entitlement Form Support
- Sunrise/Sunset of Accounts and Entitlements
- Flexible Certification
- Improved Diagnostic Console via Oracle Enterprise Manager
- Enable Taskflows for Customization
- FVC Utility Enhancements
- BI Publisher Certification for IBM WebSphere Application Server

10.2.1 Access Policy Harvesting for Reconciled Accounts

Oracle Identity Manager enables you to link the reconciled and bulk loaded accounts to pre-existing access policies by running the 'Evaluate User Policies' scheduled task, and therefore, such reconciled and bulk loaded accounts can be managed via access policies. The linking of access policies to reconciled or bulk loaded accounts is also referred to as access policy harvesting.

Only reconciled and bulk loaded accounts are linked with access policy, which means that the direct or request-based provisioned accounts are not considered for access policy harvesting.

10.2.2 Dynamic Organization Membership

A user is associated to the home organization, but can require membership to other organizations to perform related functions. For example, a global help desk user who belongs to the Support organization would require access to view and perform certain functions, such as password reset, on other organizations, say Finance or Sales. Oracle Identity Manager has the capability to manually assign the help desk user to an Organization Viewer admin role, which is restrictive and more applicable to permission grants. Dynamic organization membership provides a way to specify a rule that drives the membership of the user to one or more organizations based on their user attributes. The feature introduces the ability to specify a membership rule for organizations similar to how roles are handled. When the user is dynamically

associated to other organizations, the user gets implicit viewer privileges to view users, roles, and privileges made available to those organizations as well. If certain users are required to perform certain functions, such as viewing and performing certain functions on other organizations, the users can still be associated to the corresponding admin role manually. Note that this is dynamic rule-based organization membership, and not virtual organization that must be associated with a physical organization in Oracle Identity Manager.

10.2.3 Hierarchical Entitlements

Business users, requesters, approvers, or access certifiers, require detailed information on what a particular entitlement maps to in the target system. For example, granting an e-Business role or responsibility would grant a user a set of menu/button privileges. Oracle Identity Manager supports such critical hierarchical entitlement metadata to be imported and made available during request, approval, and certification processes.

Users typically have more than one account in a target system. In addition to supporting multiple accounts to be associated with a user, Oracle Identity Manager supports specifying to which account a specific entitlement in a request needs to be associated with during the request checkout process.

10.2.4 Catalog Auditing

Catalog auditing maintains a footprint of changes in the access request catalog. By enabling the catalog auditing feature of Oracle Identity Manager, you can track who changes what and when in the access request catalog through the UI.

10.2.5 Archiving/Purge Support for Entities

The application capabilities in Oracle Identity Manager generate a large volume of data. To meet the standards of performance and scalability, maintaining the data generated for the life cycle management of Oracle Identity Manager entities is a challenge. Oracle Identity Manager meets this challenge by providing a real-time and continuous data purge solution. Request, Reconciliation, Task, and Orchestration entity data can be continuously purged through this based on the options or choices made. The configuration is one time and the purge solution works automatically without any intervention from the administrator.

10.2.6 Draft Request Support

Oracle Identity Manager enables requesters to save the request cart enabling them to validate and submit requests at a later time.

10.2.7 Additional Information in Requests

In many instances, requesters are required to provide additional information during access request for each requested item. For example, in a request that involves multiple entitlements, the requester might be required to specify the start date and end date for each of the entitlements requested. Oracle Identity Manager enables requesters to provide such information during request that can be carried all the way to approval and provisioning processes. Oracle Identity Manager also provides a scheduled task for entitlement grant and revoke based on the start and end dates specified.

10.2.8 Account and Entitlement Dependency Handling

Oracle Identity Manager provides a request catalog to request account entitlements. However, it requires the business user to know any entitlement-related dependencies. For example, the user must know that an e-Business account is required before the user can request for an entitlement that grants privileges to raise a purchase order in e-Business. Oracle Identity Manager can now automatically request the account for a user when a related entitlement is requested, thereby reducing the burden of the business users to know the account-entitlement relationship.

10.2.9 Entitlement Form Support

Oracle Identity Manager enables you to associate a new form with complex entitlements. A complex entitlement is represented by child object having at least two attributes, one of them marked as Entitlement attribute. Using this form, users can provide additional information that might help an approver during the approval process.

10.2.10 Sunrise/Sunset of Accounts and Entitlements

Oracle Identity Manager supports temporal grant of accounts and entitlements, which refers to provisioning accounts or entitlements between a specific start or sunrise date and end or sunset date. You can specify start and end dates for accounts and entitlements in various instances, for example:

- Employee on boarding on a future start date
- Contractor on boarding from a future start date to a specific end date
- Employee termination on a specific end date
- Temporal accounts, which can be requested to be active between a specific start date and end date
- Temporal entitlements, which can be requested to be active between a specific start and end date

10.2.11 Flexible Certification

Oracle Identity Manager introduces the capability of specifying additional levels of reviews in the certification workflow process. For example, Oracle Identity Manager can launch a certification review process whereby the business manager reviews the users that report to the manager, but is then followed by the managers' manager also reviewing the same access rights, while viewing the decisions made by their subordinates.

10.2.12 Improved Diagnostic Console via Oracle Enterprise Manager

Oracle Identity Manager introduces a new operational console in Oracle Enterprise Manager that provides administrators a complete view of all the defined Oracle Identity Manager operations, default and custom event handlers, child processes, workflow processes, and state and error information, without requiring to look into different server logs. This tool does not replace the larger Identity and Access Management pack in Enterprise Manager that provides a suite-wide monitoring capability, but serves as a useful diagnostic tool specifically for Oracle Identity Manager.

10.2.13 Enable Taskflows for Customization

Oracle Identity Manager provides default taskflows for using them in the customized pages of Oracle Identity Self Service and to invoke other taskflows. For example, you can customize the user details page so that the user details of the manager will be displayed if you click the manager login name in the user details page. The default or predefined taskflows are called public taskflows.

10.2.14 FVC Utility Enhancements

The Form Version Control (FVC) Utility facilitates the management of form data changes after a form upgrade operation. Oracle Identity Manager enables you to upgrade the form version and data by using any one of the following:

- The Form Upgrade Job scheduled task: Updates the form version to the latest active version and the form data to the value specified during the field's creation for all accounts.
- The command-line FVC Utility: Supports field mapping and data updates on a provisioning process form and its associated child forms.

10.2.15 BI Publisher Certification for IBM WebSphere Application Server

Oracle Identity Manager is certified to use BI Publisher reports on IBM WebSphere Application Server.

10.3 General Issues and Workarounds

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

10.3.1 Auto-Logged In User is Logged Out After the Cookie Expiry Interval of 120 Seconds

In an Oracle Identity Manager deployment integrated with Oracle Access Manager (OAM), when you log in to Oracle Identity Self Service for the first time, you are redirected to reset the password and answer challenge questions. After successfully resetting the password and answering challenge questions, you are automatically logged in to the Oracle Identity Self Service without requiring to authenticate again. However, the login session ends in 120 seconds and you are redirected to the login page.

To workaround this issue, the cookieExpiryInterval configuration property of the ssoConfig tag in the oim-config.xml file must be set as -1.

Note: The oim-config.xml file is stored in MDS. To edit this file, you can either use WebLogic export/import utilities, or use MBeans from the Enterprise Manager console.

10.3.2 Localized Display Name Not Reconciled in Oracle Identity Manager Via User/Role Incremental Reconciliation

When a user attribute with subtype, such as displayname;lang-jp, is modified in iPlanet DS/ODSEE, then reconciliation does not bring that change into Oracle Identity Manager. Unlike other directory servers, such as OID or AD, which bring in all subtype attributes (displayname, displayname;lang-jp, ...), iPlanet DS/ODSEE only logs the updated subtype attribute. Because of this iPlanet DS/ODSEE limitation, the subtype update is not reconciled.

The workaround is to update all the other subtype attributes with existing values, in addition to the subtype being updated in a single modify command. For example, if you have displayName;lang-zh-tw, ;lang-fr, and ;lang-ja, then to update displayName;lang-ja, the ldif shown in Example 10–1 must be used.

Example 10–1 Sample ldif File

```
dn: cn=Role 001,cn=Groups,dc=example,dc=com
changetype: modify
replace: displayName
displayName: Roles 001
-
replace: displayName;lang-zh-tw
displayName;lang-zh-tw: Roles 001-Chinese
-
replace: displayName;lang-fr
displayName;lang-fr: Roles 001-French
-
replace: displayName;lang-ja
displayName;lang-ja: Roles 001-Japanese_update1
```

10.3.3 Organizations Not Created Because of AD Organization Reconciliation Run

When the scheduled job for AD organization reconciliation is run, AD organizations are not created in Oracle Identity Manager.

To workaround this issue:

1. Create a reconciliation rule for the Xellerate Organization resource object by using the Design Console. To do so:
   a. In the Design Console, open the Reconciliation Rules form.
   b. In the Name field, enter `AD Organization Recon Rule`.
   c. In the Object field, select **Xellerate Organization**.
   d. In the Description field, enter **AD Organization Recon Rule**.
   e. Save the reconciliation rule.
   f. Click **Add Rule Element**. The Add Rule Element dialog box is displayed.
   g. In the Rule Elements tab, select the following:

      - For Organization Data, select **Organization Name**.

      - For operator, select **Equals**.

      - For attribute, select **Organization.Organzation Name**.

      - For transform, select **none**.

h. Click **Save**, and then close the dialog box.

i. In the Reconciliation Rules form, select **Active**.

j. Click **Save**.

2. Create a reconciliation profile for the Xellerate Organization resource object. To do so:

   a. In the Resource Objects form, search and select **Xellerate Organization**.

   b. In the Object Reconciliation tab, click **Create Reconciliation Profile**.

3. Run the AD Organization Recon scheduler to create AD organizations as OIM Organizations.

10.3.4 The SodCheckViolation Field of the Process Form is Not Updated for Request Provisioning

For request provisioning of the PSFT resource with conflicting entitlements, the SodCheckViolation field in the process form is not updated. The entitlement violation is mapped to the field with the SoDCheckEntitlementViolation label, while the PSFT resource has the field with the SoDCheckViolation label. Therefore, the mapping does not occur. Direct provisioning and provisioning through access policy successfully takes place with the SoDCheckViolation field label.

To workaround this issue for request provisioning, change the SoDCheckViolation field label to SoDCheckEntitlementViolation in the PSFT form by using the Design Console.

10.3.5 Blank Page Displayed for Approval Details

Blank page is displayed for approval details when the host and port to access identity application and the host and port to access task details are different.

The task details URL configuration can be checked from Oracle Enterprise Manager in the following way:

1. Login to Oracle Enterprise Manager by using WebLogic administrator username and password.
2. On the left navigation menu, click **SOA**. Expand **soa-infra**, **default**.
3. Click the required SOA composite under the default menu.
4. On the right pane, click the approval task in the Component Metrics section.
5. Click the **Administration** tab.

   The host and port used to access identity and task details must match for task details to work.

Notice that host and port has been set by using OIMExternalFrontEndURL in the DiscoveryConfigMBean. If OIMExternalFrontEndURL is empty, then OIMFrontEndURL can be used. If there has been a change in frontend host or port, then correct it or perform the steps described in "Oracle Identity Manager Host and Port Changes" of the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

10.3.6 Modification of Disabled Account and Requesting Entitlement for the Account is Allowed

Oracle Identity Manager allows modification of an account and requesting of its entitlement, although the account is in disabled state.

This is a known issue, and a workaround is currently not available.

10.3.7 The Refresh Button is Truncated in Some Pages of the Oracle Identity Self Service

When you open Oracle Identity Self Service by using Google Chrome 15.0.x web browser, the Refresh button on the toolbar is displayed as truncated in some pages.

To workaround this issue, upgrade Google Chrome 15.0.x to Google Chrome 18.0.1025.162 or higher version.

10.3.8 Provisioning of Application Instance with AD User Resource Object Does not Work

When you create an application instance for AD with appropriate details and request to provision the application instance as System Administrator, the resource is in provisioning state, and the following message is logged:

```
<Warning> <XELLERATE.SERVER> <BEA-000000> <No fields having ITResouce property
found in form with sdk_key=11>
<Warning> <XELLERATE.SERVER> <BEA-000000> <More than fields of type
ITResourceLookupField found on form with sdk_key=11>
<Warning> <XELLERATE.SERVER> <BEA-000000>
<Cannot figure out the ITResource field uniquely>
```

To workaround this issue, add the ITResource=true property for AD Server process form field in the process form.

10.3.9 Some Attestation Pages Do Not Work in Mozilla Firefox and Google Chrome

In Oracle Identity Manager User and Administrative Console, some pages related to attestation do not work when you use Mozilla Firefox or Google Chrome web browsers. These include pages for creating attestation processes and submitting attestation requests.

To workaround this problem, use Microsoft Internet Explorer web browser.

10.3.10 Custom Scheduled Jobs Fail Because of Dependency on Legacy APIs

Custom scheduled jobs, which use APIs available in legacy versions of Oracle Identity Manager but is not available in the current release, fail at run time. For example, a custom scheduled job, which calls com.thortech.xl.client.mail.tcSendMail to send emails, fails with the java.lang.NoClassDefFoundError error message. This is because com.thortech.xl.client.mail.tcSendMail is available in Oracle Identity Manager release 9.x and earlier releases, but is not available in 11g releases.

To avoid this issue, use only APIs published with the current release instead of using individual unsupported APIs, such as tcAdapterUtilities or tcClient. In addition, you must migrate any custom code to use the new APIs if the old APIs have been deprecated. For information about APIs in Oracle Identity Manager 11*g* Release 2 (11.1.2.0), see *Oracle Fusion Middleware Java API Reference for Oracle Identity Manager*.

10.3.11 Catalog Tag Cannot Store More Than 256 Characters

When you create a role, entitlement, or application instance with maximum possible values for name, display name, and description attributes, only the first 256 characters of the entity are displayed in the request catalog. For example, when you create a role with name=2000 characters, role display name=3000 characters, and description=1024 characters, and search for the role in the request catalog, the first 256 characters of the corresponding entry for the role is displayed. The user must search for the entity in the catalog by using the words present in the first 256 characters of the entity name, display name, or description.

This is a known issue, and a workaround is currently not available.

10.3.12 Self Registration Request Fails After Request Approval

When the task assignee of Self registration request tries to approve the task from the pending approvals page, the task is approved but the request moves to Request Failed status.

For self registration requests, Organization is a mandatory attribute that must be provided by the approver before approving the task. If the task is approved from the pending approvals page, the task is completed but since approver has not updated the Organization for the user, the request fails. The following workaround is available for the approver:

1. Provide a value for the Organization attribute for the user in the task details page.
2. Update the user information by clicking Update in the task details page.
3. Approve the task from the task details page.

Oracle Identity Manager validates if mandatory attribute values are provided in the task details page and that all the changes to the page are saved before approving the task.

10.3.13 Soft-Deleted Entitlement is Provisioned by Access Policy-Based Provisioning

When performing access policy-based entitlement provisioning where the entitlement is already soft-deleted, the entitlement can still be provisioned to the user.

This a known issue, and a workaround is currently not available.

10.3.14 Interrupted Scheduled Job Run Fails on Restarting

When a scheduled job runs for a considerable time and the job is interrupted by clicking the stop button, the job status changes to Interrupted, and a message is displayed stating that the job is stopped.

However, depending on the implementation of stop check on the execute methods of the individual scheduled jobs, the processing is made to stop with due checking only after a specified time. If the checking is delayed, then there is a similar delay in the actual stopping of the job in the backend. Till the execute method of the job verifies that the job is stopped, the status of the job continues to show as Interrupted and not Stopped. After the result of the verification is returned, the job status changes to Stopped. Only after this change in status of the job, the next run of the job can be rescheduled.

10.3.15 Bulk Request for Multiple Entities Fails After Approval

When a request for multiple entities, such as application instance, roles, or entitlements, is created for a user who does not have the viewer admin role for the entities, no error is generated during request submission. However, the request fails after approval. This is because bulk request checks only the requester's permissions. The beneficiary permissions are used to determine the child requests to be created after request-level approval is done.

This is a known issue, and a workaround is currently not available.

10.3.16 Import of Disconnected Application Instance Fails

When you export an application instance, the Deployment Manager shows the IT Resource and Resource as dependent objects in the Select Dependencies window. In the final export window at the end of all the dependency selection, Deployment Manager shows IT Resource Defn in the Unselected Dependencies list. To avoid import failure, add the dependency for IT Resource Def from the Unselected Dependencies list.

10.3.17 Existing Data for Administrators Role Grant Does Not Sync After Applying Patch 14591093

In an environment, in which the Administrators role has already been granted to the system administrator or any user before applying patch 14591093, this role grant is not reflected in LDAP after applying the patch. The patch takes care of new grants made to the users for the Administrators role.

To workaround this issue, perform any one of the following:

- Retry the role grant with a newly created user or a user who does not have Administrators role granted through the Oracle Identity Manager User and Administrative Console.
- Include the user's DN in the Administrators unique member in Oracle Directory Services Manager (ODSM). To do so:
  1. Login to ODSM.
  2. Find the 'cn=Administrators,cn=Groups,dc=us,dc=example,dc=com' role.
  3. Add the uniquemember field.
  4. Specify the DN of the user. For example, for the oim_admin user, the dn is 'cn=oim_admin,cn=Users,dc=us,dc=example,dc=com'.
  5. Click **Save/Apply**.
  6. Retry the role grant.

10.3.18 The Reset Button in the Resource Object Lookup Redirects to Basic Search

In the Create Application Instance page, when you search for a resource object by using Advance Search, if you click on the Reset button, then instead of resetting the values in the same page, the search is redirected to Basic Search. This is because the Reset button resets the QueryDescriptor object in Application Development Framework (ADF), which defines the Simple or Advanced display mode. For details about the QueryDescriptor object, refer to ADF documentation.

10.3.19 IT Resource Definition Not Displayed in Dependency List

When exporting an application instance by using the Deployment Manager, IT resource definition is not displayed the dependency selection list. This is because the Deployment Manager shows only one level of dependencies in the Select Dependency page of the Export wizard. Other dependent objects are displayed in the Unselected Dependencies pane in the Export wizard before the export. To avoid missing dependencies at the time of import, select the dependency object from the Unselected Dependencies pane.

10.3.20 Error in Entitlement Provisioning for Manually Created Resource Object

When you create a resource object by using the Design Console, create the provisioning process, parent and child forms with entitlement, change the lookup code with the correct ITResource key, populate the ent-list table, and then try to provision the entitlement, the following error is generated:

```
IAM-4060021 : An error occurred while validating whether entitlement with key 2151
is already provisioned to user with key 31 and the cause of error is
oracle.iam.provisioning.exception.GenericProvisioningException: Entitlement
attribute not marked as key in reconciliation field mapping for UD_TESTC.
```

This means that the key attribute in reconciliation field mapping is not defined for the child form attribute. Here, in the UD_TESTC child form, the value of the entitlement property is set to true in the UD_TESTC_LKP child form attribute, but reconciliation mapping is not defined.

To workaround this issue, define the reconciliation field mapping. See "Reconciliation Field Mappings Tab" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about reconciliation field mapping.

10.3.21 QBE Returns No Result When User Has No Permission on Organization of the Requester

User is allowed to search for a request in the Track Requests page even though the user does not have permissions on the requester's organization. But when the user filters the records for the requester in the Track Requests page by using Query By Example (QBE) without permissions on the requester's organization, no results are returned.

This is a known issue, and a workaround is currently not available.

10.3.22 Checkbox UDF Displayed as Boolean Field

When you create a UDF of type checkbox in the User form, customize the Create User, Modify User, and User Details pages to add the UDF, and then create a user by selecting the checkbox, it is displayed as a Boolean field with values as true and false.

To workaround this issue, add the field on the User Details pages as a check box, and mark the field as read-only.

10.3.23 Lookup for Entitlements Must Be Searchable and Searchable Lookup

When creating a child table with a lookup field for entitlement, the following options must be selected so that the Entitlement=true property is set and the field type is lookup:

- **Searchable**
- **Entitlement**

- **Searchable Picklist**

There is scope for error when you do not select the **Searchable** option in the Constraints section and/or the **Searchable Picklist** from the Advanced section. As a result, the field type of the form field will be a Combo box instead of a LookupField.

To workaround this issue, perform any one of the following:

- If the **Searchable** option in the Constraints section is not selected, then open the form attribute again, and select the **Searchable** option to mark the attribute to be of searchable type. Then, create a new form for the application instance or select **Regenerate View** in the parent form view.
- If the **Searchable Picklist** option in the Advanced section is not selected, then a Combo box type field is created. There is no way to edit the Searchable Picklist option. There are two ways to fix this. The first method is:
  a. Open the Form Designer form in the Design Console, and open the child form.
  b. Create a new version of the child form, and change the field type from ComboBox to LookupField. Then, activate the child form.
  c. Create a new version of the parent form, associate the new version of the child form, and then activate the parent form.
  d. Create a new form for the application instance or regenerate the view of the existing parent form.

  Otherwise, create another form field attribute with the correct options selected. Then, customize the parent form page, and hide the form field with the incorrect attribute values.

10.3.24 Dependent Lookup Does Not Work With Pick List Component

When you have a dependent lookup with a pick list (a lookup with glass icon to search for the values) and select a value in the parent lookup, the correct values in the dependent combo box are not displayed. This is because Oracle Identity Manager does not support dependent lookup for the pick list component.

This is a known issue, and a workaround is currently not available.

10.3.25 Cascading Lookups Display Limited Number of Values

When you create a cascading lookup as a LOV or as a combo box, only 25 values are displayed in the lookup search irrespective of the number of values.

To workaround this issue:

- Do not use cascading lookup as a combo box, and instruct users to narrow the searches.
- Implement cascading lookups by using the Managed Bean approach, as described in "Implementing Custom Cascading LOVs" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

10.3.26 Catalog Search With Special Characters Fail

If catalog search contains special characters, the search fails with error that has IAM-7130125 and DRG code in the message, such as:

```
IAM-7130125 : Search token caused Oracle text DRG issue, DB exception is
:ORA-20000: Oracle Text error: DRG-50943: query token too long on line 1 on column
40 20000
```

```
IAM-7130125 : Search token caused Oracle text DRG issue, DB exception is
:ORA-20000: Oracle Text error: DRG-50901: text query parser syntax error on line
1, column 5 20000
```

In the request catalog, search keywords that include all the commonly used special characters, such as #, $, and -, in requestable entities work correctly and return desired results. However, search keywords with few special characters, such as double quote ("), colon (:), or brackets do not return the desired results.

To avoid the issue, escape the special characters with the back slash character (\) in the search query string. For example, replace special characters **(**, **)**, and **"** with **\(**, **\)** and **\"** respectively.

10.3.27 Lookup Search Does Not Support Asterisk Wildcard Character

Searching for lookup definitions with the asterisk character (*). For example, searching lookup definitions with * or (a*) do not return any result.

To workaround this issue, search the percentage character, **%** or (**a%**).

10.3.28 Errors Not Displayed in Form Designer

When you add a UDF to a form by using the Form Designer, if you mark the UDF as Searchable and Encrypted at the same time, then no error message is displayed although this combination in not valid.

This is a known issue, and a workaround is currently not available.

10.3.29 User Creation Fails if Default Password Policy is Removed

User creation depends on default password policy. User creation fails if there is no default password policy. Therefore, default password policy must not be deleted.

To avoid failure of user creation because of default password policy removal, Oracle recommends the following:

- Default password policy is the only one used for user creation and is not recommended to be deleted.
- The default password policy constraints can be modified if the password is expected to meet different criteria.
- If the default policy is deleted or a different password policy is required to be considered as the default password policy, which would be used for user creation, then the desired default policy must be associated with the TOP organization.

10.3.30 Exception Displayed Intermittently

The following error message might be displayed intermittently:

```
too many objects match the primary key oracle.jbo.key[ua0902 ]. with npe
```

For example, when you try to reassign a task in Oracle Identity Self Service, this error message might be displayed intermittently.

Whenever this error message is displayed, log out of Oracle Identity Self Service and log in again.

10.3.31 Benign unknownplatformexception Error

When logging in by using any client in Oracle Identity Manager, for example while logging in to the Design Console, the logging is successful. However, some times a benign `unknownplatformexception` error is displayed.

This does not result in any loss of functionality.

10.3.32 Error in Searching for Data Components

When you search for data controls from the catalog in the Data Components dialog box, the search is only performed for the data controls at the top level and not for the fields. An error is logged when you search for the fields in the Data Components dialog box for customization purpose, and the search does not return any result.

This is a known issue, and a workaround is currently not available.

10.3.33 Retry Provisioning Task Fails

When a provisioning task is assigned to a role and the role member is able to view the task, and when the role member tries to retry the provisioning task, the following error message is displayed:

```
Error JBO-29000: Unexpected exception caught: Thor.API.Exceptions.tcBulkException,
msg=null
Error Localized message not available. Error returned is: null
```

To workaround this issue, assign the provisioning task to the System Administrator role.

10.3.34 Multiple Entries Displayed for the Same Provisioning Task

When a user opens the Provisioning Tasks page in Oracle Identity Self Service and clicks **Search**, multiple entries for the same provisioning task that is assigned to the user are displayed.

To workaround this issue, close the Open Tasks page and reopen it.

10.3.35 Length of Attribute Value Changes on Updating the Form Field

The following issues are encountered if you update a field in an existing form:

- If you update the Organization Name existing field in the AD User form, save and close the form, regenerate view, and provision and provide the lookup value for the Organization Name in the Catalog, the following error message is displayed:

  ```
  IAM-2050099 : The length of the attribute value Organization Name is greater
  than the maximum allowed length 40.
  ```

  Even if you try to provision for single user and select the Organization Name, the same error is displayed.

  To workaround this issue, create a new form for AD User and attach it to the application instance.

- For child table, if you edit the existing lookup field, for example the GroupName field in AD User form, add Entitlement and Searchable option, and view the child form in the Design Console, one more field adds with entitlement = true, and the length of the field changes.

To workaround this issue, perform the changes from the Design Console when configuring resources for entitlement for the first time.

10.3.36 Input Data Lost in Request Catalog

When you add an application instance in the request catalog, enter some data in the parent form, remove the user, and then add another user, the data entered to the parent form is lost.

This is a known issue, and a workaround is currently not available.

10.3.37 Error on Publishing Sandbox

If two users log in to Oracle Identity Self Service by using the same System Administrator login credentials, perform some operations on sandbox by using the same sandbox, and try to publish the sandbox, then the following error is displayed and the sandbox does not get published:

```
Publish Sandbox Failed
oracle.mds.sandbox.RefreshFailedException: MDS-00001: exception in Metadata
Services layer MDS-00165: metadata Object
"/persdef/oracle/iam/ui/catalog/model/am/CatalogAM.xml" has changed
MDS-00164: There is a concurrent "UPDATE" operation on the document
"/persdef/oracle/iam/ui/catalog/model/am/mdssys/cust/site/site/CatalogAM.xml.x
ml". MDS-00165: metadata Object
"/persdef/oracle/iam/ui/catalog/model/am/CatalogAM.xml" has changed
MDS-00164: There is a concurrent "CREATE" operation on the document
"/persdef/oracle/iam/ui/catalog/model/am/mdssys/cust/site/site/CatalogAM.xml.x
ml". MDS-00165: metadata Object
"/persdef/oracle/iam/ui/catalog/model/am/CatalogAM.xml" has changed
MDS-00164: There is a concurrent "UPDATE" operation on the document
"/persdef/oracle/iam/ui/catalog/model/am/mdssys/cust/site/site/CatalogAM.xml.x
ml". MDS-00165: metadata Object
"/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf" has changed
MDS-00164: There is a concurrent "UPDATE" operation on the document
```

This is a known issue, and a workaround is currently not available.

10.3.38 Import/Export of Organization and Role Without UDFs

Organization and role entities are imported and exported via the Deployment Manager without any related UDFs and UDF values. The related UDFs are imported and exported separately via the Deployment Manager because Role Metadata and Organization Metadata options are available under the drop-down list of exportable entities in the Deployment Manager.

Only default value of UDFs are imported and exported. The value assigned to UDFs at creation of Organization and Role entities are not import and exported.

10.3.39 Possible Suboptimal SQL in Target Resource Reconciliation Run

When you add a resource object and run target resource reconciliation for bulk accounts using DBUM connector, the following SQL might report suboptimal performance:

Note:

- The exact SQL structure may vary because of matching rule predicates in an environment.
- This SQL may show suboptimal performance in very few environments. It may function properly in almost all environments. All setups have their own uniqueness in terms of data volume, distribution, and selectivity.

```
INSERT
INTO    RECON_ACCOUNT_MATCH
(
   RE_KEY  ,
   ORC_KEY ,
   SDK_KEY ,
   RAM_ROWVER
)

(
   SELECT re.re_key           ,
          ud_db_ora_u.orc_key ,
          :"sys_b_0"          ,
          :"sys_b_1"
   FROM   UD_DB_ORA_U UD_DB_ORA_U                        ,
          ra_oracledbuser725eedcb ra_oracledbuser725eedcb,
          ost ost                                        ,
          oiu oiu                                        ,
          recon_events re
   WHERE  re.rb_key =:"SYS_B_2"
          AND re.re_status = :"SYS_B_3"
          AND re.re_key = ra_oracledbuser725eedcb.re_key
          AND
          (
            ud_db_ora_u.ud_db_ora_u_itres=ra_oracledbuser725eedcb.ra_
itresource15641f83
            AND
            ud_db_ora_u.ud_db_ora_u_username=ra_oracledbuser725eedcb.ra_
username8825b9c0
          )

          AND oiu.orc_key = ud_db_ora_u.orc_key
          AND ost.ost_key = OIU.ost_key
          AND ost.ost_status <> :"SYS_B_4"
)
```

To workaround this issue, use the Plan Stability feature of the Oracle Database for this rare behavior of this particular SQL. Oracle Database as a RDBMS feature provides for SQL Plan stability via Stored Outlines. It can be used by DBAs to prevent certain database environment changes from affecting the performance characteristics of applications. This feature helps optimize database performance when the optimizer, in normal mode, does not pick up an execution plan that is tuned for performance. Therefore, the SQL Profiles feature can be used to potentially lock a better SQL plan for this SQL in the Oracle Identity Manager database environment (by using the SQL Tuning Advisor and subsequent usage of SQL Profiles, or any suitable mechanism of choice by the DBAs).

More on this feature usage as a workaround for this or similar situations can be found in section "Using Plan Stability" of the *Oracle Performance Tuning Guide*.

10.3.40 Multiple Child Tables Cannot Be Used in Requests

Although a connector has more than one child table, only one child table can be used in requests.

To workaround this issue, use entitlement requests.

10.3.41 Session Failover Issues

Active-Active session fail over does not work properly with Oracle Identity Manager. These issues are mostly displayed in Oracle Identity System Administration.

This is a known issue, and a workaround is currently not available.

10.3.42 Error in Adding Data for Process Instance to Child Form

When a new UDF is added to the application instance form and the UDF is updated for already provisioned users, it is not displayed in the UI but is available in the database.

If there are any changes to the application instances form, such as adding new fields, adding new children forms, or adding fields to children forms, then the form versions of all existing users must be updated to the latest version by using the Form Version Control Utility. This utility is available in the design console directory. Update the properties file as follows, and execute the utility:

- Resource Object Name: roname
- Process Form Name: UD_PFORM
- From Version: <fromversion>
- To Version: <toversion>

10.3.43 Last Entitlement Not Removed

Oracle Identity Manager does not remove the last entitlement during a modify account request.

To workaround this issue, remove the existing entitlement by using a revoke entitlement request instead of a modify account request.

10.3.44 Manual Fulfillment Task Not Initiated for Entitlement Provisioning

An entitlement request for a disconnected resource does not initiate the manual fulfillment task but marks the request as completed.

To workaround this issue, using the Design Console, open the corresponding provisioning process for the disconnected application and add a manual provisioning task for entitlement provisioning so that this manual task gets initiated after the approval is complete.

10.3.45 Form Fields Displayed For Disable/Enable/Revoke Manual Provisioning Task

The form associated to a disconnected application instance is displayed even when the request type is disable, enable, or revoke. There is no functionality loss in displaying

the form during the disable, enable, or revoke requests. Ignore the form field display and submit the request.

10.3.46 Duplicate Rows in Request Tracking

Request tracking might display duplicate rows for the same request when searching by beneficiary. Ignore the duplicate rows.

10.3.47 Help Desk Cannot Use Request Tracking

Request tracking for help desk role mandates to specify the beneficiary of the request, even when searching by request ID.

To workaround this issue, issue a full search of the request without specifying any search filters.

10.3.48 Use Request Details to Approve Requests That Require Mandatory Information

For requests that require mandatory additional information to be provided, such as Organization, when approving a self-registration request, do not act upon the request directly from the Pending task list. Open the request, provide the required information in the Request Details page, and then approve the request. This is a SOA tasklist limitation.

10.3.49 Benign Error Messages

Although Oracle Identity Manager handles all validations, some of the error messages are not detailed enough. Benign exceptions and error messages might be displayed in the server logs during server startup, which can be ignored as long as the system is up and running.

10.3.50 Accessibility Compliance

Currently, the system is not compliant completely with Accessibility guidelines and the Accessibility link provided does not function.

10.3.51 Password Policy Not Enforced

Password policy attached to a resource does not get enforced properly during request to a connected resource. However, when you try to change the password of a provisioned resource from the My Information page, the policy is enforced.

10.3.52 Form Designer Failure Not Displayed

Form designer failure in the backend is not displayed in the UI. If the change you are expecting is not successful, then abandon the sandbox. Oracle recommends creating and using short-lived sandboxes (for example separate sandbox with a detailed description for UI customization, form creation, and UDF addition) so that conflicts can be avoided.

10.3.53 Request for Application Instance Fails If Related Sandbox is Not Published

If the sandbox, in which an application instance is created, is not published, then the request for that application instance will fail during request checkout process. Best practice is to create a sandbox for an application instance and immediately publish it.

10.3.54 Application Instance Administrator Cannot Create Forms

Only System Administrators or System Configurators can create forms and attach it to application instances.

10.3.55 Delete Reconciliation Does Not Work With libOVD and ODSEE

Delete reconciliation does not work with libOVD and ODSEE combination.

This is a known issue, and a workaround is currently not available.

10.3.56 Lookup Values Not Saved on the My Information Page

Oracle Identity Manager does not support a UDF of type Lookup to be created for the My Information page.

10.3.57 Benign Error for Missing Matching Rule Data

When running reconciliation, matching rule transformation fails with the following error message if all the fields that are part of the matching rule are not provided as input while invoking the ignoreEvent API:

```
<BEA-000000> <Generic Information: {0}
oracle.iam.reconciliation.exception.DBAccessException: Failed SQL:: select
USR_KEY from usr where USR_FIRST_NAME=? and USR_LAST_NAME=? and USR_LOGIN=?
and USR_TYPE is null and USR_EMAIL is null and USR_MIDDLE_NAME is null and
USR.USR_STATUS != 'Deleted' AND ((UPPER(USR.USR_LOGIN)=UPPER(?)) OR
(UPPER(USR.USR_UDF_OBGUID)=UPPER(RA_EZCUSERTRUSTED49EC4A54.RA_OBJECTGUID)))
=>PARAMS:: [John, Doe, J.DOE, J.DOE]
Caused By: java.sql.SQLSyntaxErrorException: ORA-00904:
"RA_EZCUSERTRUSTED49EC4A54"."RA_OBJECTGUID": invalid identifier
```

This is a benign error, and there is no functional loss because of this. The event is not ignored. It is created and processed normally without causing any data corruption.

10.3.58 User Type Attribute Value Not Populated

When you perform customization on the User Type attribute in the My Information page, for example display the User Type attribute as read-only, then the value in the User Type attribute does not populate.

Here, the attribute name is User Type in the My Information page, but from customization VO, you must select **role** to populate the correct values in the User Type attribute. Therefore, to workaround this issue:

1. In customization mode, select the Panel Form Layout Component.
2. Open the Resource Catalog.
3. Select **Data Component**, **My Information**, **UserVO1**, and then select **role**.
4. Drop the field with Output Text with a label.

10.3.59 Approval Page Customization Not Supported

Approval page customization is not supported through WebCenter Composer.

To customize the approval details page, see "Developing Workflows: Vision Request Tutorial" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

10.3.60 Enable, Sequence, and Description for Lookup Values Not Supported

The Enable, Sequence, and Description attributes are not supported for lookup values. Therefore, do not include a value in the Description field for searching lookups. Also, the Enabled, Sequence, and Description columns are displayed without any values.

10.3.61 Cannot Add Radio Button

When you try to add a radio button to a form, for example organization form, a forward-only range paging error is generated. This is because adding a radio button through drop handlers is not supported. However, radio buttons can be added to forms through view layer customization with custom code.

10.3.62 Indirect Role Membership Error

Clicking the **Roles** tab in the My Access section or the Users section of the Oracle Identity Self Service generates an error when the logged-in user has indirect role relationship.

10.3.63 Created UDFs Not Listed in Customization View

When you create a UDF in an active sandbox, the UDF is not listed in the customization view (catalog of the Data Component).

To avoid this issue, create the UDF, and then create the sandbox and activate it. Newly created UDFs are displayed in customization view in the sandboxes created after the UDF creation.

10.3.64 Attributes Cannot Be Marked Required Using Form Designer

Attributes cannot be marked as required or mandatory from the Form Designer. However, mandatory attributes can be specified by customizing the page by using Oracle Web Center.

10.3.65 Cascading LOV Not Working

When you setup cascading LOVs, the values in the dependent LOV are not displayed based on the selection of the parent LOV.

To workaround this issue:

1. Set up the cascading LOV by using two UDFs.
2. Add both the Select One Choice components.
3. Setup the partial rendering of the component.

10.3.66 Number Type Lookup Code Not Supported

Oracle Identity Manager does not support number type lookup code in this release.

10.3.67 Customizing the Self Registration Page Does Not Work

When you try to customize the self registration page of Oracle Identity Manager by selecting View, Source, validation error messages are displayed stating that input for the form fields are missing.

To avoid this issue, provide values for the input fields in the self registration page. The complete steps to customize the self registration page are the following:

1. Login to Oracle Identity Self Service.
2. Activate a sandbox.
3. Click **Customize**.
4. Navigate to the Oracle Identity Manager login page, and click **New User Registration**. Alternatively, navigate to /identity/faces/register directly.
5. Enter values for the required input fields.
6. Select **View**, **Source**.
7. Customize the page.

10.3.68 Some Help Links Do Not Work

When you access Help Topics for Oracle Identity Manager from Oracle Identity Self Service and Oracle Identity System Administration, some links do not work. The following are the navigation paths where the links are not active:

From Oracle Identity System Administration:

- Help link from Identity System Administration, Using Oracle Identity System Administration, Lookups
- Help link from Identity System Administration, Using Oracle Identity Self Service, Approval Details, Request for Information

From Oracle Identity Self Service:

- Help link from Identity Self Service, Using Oracle Identity Self Service, Approval Details, Request for Information
- Help link from Identity Self Service, Using Oracle Identity Self Service, Manage Sandboxes
- Help link from Identity Self Service, Using Oracle Identity Self Service, Customize Oracle Identity Self Service
- Help link from Identity Self Service, Using Oracle Identity System Administration, Manage Reconciliation Events
- Help link from Identity Self Service, Using Oracle Identity System Administration - Manage Policies:

  - Create Access Policies

  - Manage Access Policies

  - Create Attestation Configuration
- Help link from Identity Self Service, Using Oracle Identity System Administration, Approval Policies
- Help link from Identity Self Service, Using Oracle Identity System Administration, Manage Attestation Configuration
- Help link from Identity Self Service, Using Oracle Identity System Administration, Password Policy
- Help link from Identity Self Service, Using Oracle Identity System Administration, Perform Configuration Tasks: Create IT Resource

  - Manage IT Resource

  - Create Generic Connector

- Manage Generic Connector

- Help link from Identity Self Service, Using Oracle Identity System Administration, Form Designer
- Help link from Identity Self Service, Using Oracle Identity System Administration, Application Instances:

  - Search Application Instances

  - Create Application Instances

  - Delete Application Instances
- Help link from Identity Self Service, Using Oracle Identity System Administration, Modify Application Instances, The How links
- Help link from Identity Self Service, Using Oracle Identity System Administration, Lookups
- Help link from Identity Self Service, Using Oracle Identity System Administration, Perform System Management Tasks:

  - Import

  - Export
- Help link from Identity Self Service, Using Oracle Identity System Administration, Scheduler
- Help link from Identity Self Service, Using Oracle Identity System Administration, Notification
- Help link from Identity Self Service, Using Oracle Identity System Administration, System Management
- Help link from Identity Self Service, Using Oracle Identity System Administration, Manage Connector
- Help link from Identity Self Service, Using Oracle Identity System Administration, Manage Sandboxes

View the Help topics from the relevant section of the interface. For example, to view the Help topic for System Management or Sandboxes, navigate to the Help topics from Identity System Administration. For any topic that is not displayed, refer to Oracle Fusion Middleware Identity Management 11*g* Release 2 (11.1.2) Documentation Library.

10.3.69 Unpublished Entities Provisioned Via Access Policies

Entitlements and accounts can be granted via access policies. When entitlements and accounts are granted via access policies, organization scoping does not apply, and therefore, the entitlements and accounts that are not published to the target user's organization are also provisioned.

Although an entitlement is not published to an organization, an access policy can still provision the entitlement to the user of that organization. This is because access policies are not aware of the publishing and scoping security model of Oracle Identity Manager.

This is a known issue, and a workaround is currently not available.

10.3.70 Certificate-Based Digital Signatures Not Supported

For task approvals, Oracle Identity Manager does not support digital signatures based on certificates. However, Oracle Identity Manager supports password-based digital signatures. See "How to Specify a Workflow Digital Signature Policy" in the *Oracle Fusion Middleware Developer's Guide for Oracle SOA Suite*.

10.3.71 Entitlements Provisioned to Users Not Displayed After Upgrade

In an upgraded deployment of Oracle Identity Manager 11*g* Release 2 (11.1.2.2), the entitlements provisioned to the users before the upgrade are not displayed in the Entitlements tab.

To display the entitlements in the Entitlements tab after the upgrade, login to Oracle Identity System Administration, and run the Entitlement Assignments scheduled job.

10.3.72 Labels in Query Panel Cannot be Customized

By default, labels in query panels are not customizable. For example, the Beneficiary label in the Track Requests search page cannot be customized, but the column names in the Track Requests search results table can be changed.

10.3.73 UMS Fails to Send Notification While Provisioning Account

Notification in provisioning workflow does not use the notification model in Oracle Identity Manager 11*g*. Therefore, if UMS notification provider is configured and notification is assigned to a provisioning task, then while provisioning an account for OIM user, a notification message is not sent. In addition, a NullPointerException error message is logged.

To configure and use notification in provisioning workflow, see "Specifying the E-Mail Server" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

10.3.74 Error on Creating Subtask

When the requester tries to create a subtask by selecting Create Subtask from the Actions menu in the Inbox, NullPointerException is generated. Creating subtasks is not supported for certification tasks.

10.3.75 Running the pasteConfig Script Displays Incorrect Error Message

While running the pasteConfig script in the target host, if the jdk location specified does not exist, then an incorrect error message is displayed, as shown:

```
The JDK wasn't found in directory /scratch/aime1/jrockit-jdk1.6.0_
37-R28.2.5-4.1.0.
Please edit the startWebLogic.sh script so that the JAVA_HOME variable points to
the location of your JDK.
```

You can ignore this error message because it does not result in any loss of functionality.

> **Note:** If the source Middleware home uses a JDK that is external to the Middleware home, then the pasteBinary operation must also use an external JDK. The JDK provided to run FMW T2P utility must be accessible to the source as well as target.

10.3.76 Error Logged While Exporting Metadata of oracle.security.apm Application

The following error is logged on running the FMW T2P copyConfig utility in the source computer:

```
Exporting metadata of application -  oracle.security.apm
.
Metadata transfer operation started
Exporting metadata from repository . . . . . .
. . . . . .
Metadata tranfer operation failed
.
Cause: main.WLSTException : MDS-00503: The metadata path "../mds" does not contain
any valid directories.MDS-91009: Operation "exportMetadata" failure.
Use dumpStack() to view the full stacktrace.
.
Unable to export Application data from Oracle Metadata Repository. The Application
"oracle.security.apm" may not have any data in Oracle Metadata Repository or it
may not be in "ACTIVE" state.
```

This is a benign error and can be ignored because it does not cause any loss of functionality in Oracle Identity Manager.

10.3.77 Error Logged While Exporting Metadata of oim Application

The following error is logged on running the FMW T2P copyConfig utility in the source computer:

```
Exporting metadata of application -  oim
.
.
Cause: main.WLSTException : MDSAppRuntimeMBean is not available for
oracle.mds.lcm:name=MDSAppRuntime,type=MDSAppRuntime,Application=oim,Location=oim_
server1,*MDS-91009: Operation "exportMetadata" failure. Use dumpStack() to view
the full stacktrace.
.
.
Unable to export Application data from Oracle Metadata Repository. The Application
"oim" may not have any data in Oracle Metadata Repository or it may not be in
"ACTIVE" state.
```

This is a benign error and can be ignored because it does not cause any loss of functionality in Oracle Identity Manager.

10.3.78 Benign ApplicationDB Connection Pool Errors

Errors related to the ApplicationDB data source connection pool might be logged. This data source is used internally by ADF for reading MDS artifacts for Oracle Identity Self Service. These errors cause no functional loss. Frequency of these exceptions can be reduced by tuning the Data Source `Inactive Connection Timeout` property and JVM parameters, such as `jbo.ampool.timetolive` and `jbo.ampool.maxinactiveage`.

The following exception might be logged:

```
<Warning> <JDBC> <BEA-001153>
<Forcibly releasing inactive/harvested connection
weblogic.jdbc.wrapper.PoolConnection_oracle_jdbc_driver_T4CConnection back
into the data source connection pool "ApplicationDB"
```

Immediately followed by:

```
java.sql.SQLException: Connection has already been closed.
```

10.3.79 Reconciliation Archival Utility Throws Errors

When you install an Active Directory Release 9.x connector and run the reconciliation archival utility, then uninstall AD 9x connector and install AD 11*g* connector, and try to run reconciliation archival utility, errors are generated and the utility does not run. The following is a sample error message:

```
ERROR ==> Error/warning occurred while executing ./oim_create_recon_arch_
tables.sql
For Details check log file ./logs/oim_create_recon_arch_tables.log
Exiting Utility
```

The errors are generated because old Reconciliation Archival tables related to the uninstalled connector still exist in the database. Therefore, to avoid this issue, after uninstalling a connector, drop the RA tables related to the connector.

10.3.80 Latency in Auto Closing the Tab After Acting on the Task

When you act on a task from the details page, the tab closes automatically, but after a delay of few seconds. This is a known issue, and there is no workaround for this.

10.3.81 Filters on Some Columns Not Supported

Oracle Identity Manager does not support filters or Query by Example (QBE) on some columns in the search result table. Examples of such columns are Date Added and Hierarchy Aware.

10.3.82 Disconnected Resource Child Table Tasks Not Autocreated

Disconnected resource child table insert/delete trigger tasks are not autocreated when the child table with an Entitlement field is created by using the Design Console.

10.3.83 Field Added to a Page Might Not Be Displayed

During UI customization, when you try to add a field to a page for the first time, the field might not be displayed on the page. The field is displayed on the page when you retry to add the field by clicking the Add action.

10.3.84 Auto-Unlock Feature Does Not Work

The auto-unlock feature between Oracle Identity Manager and Oracle Access Manager (OAM) does not work. User is not unlocked on running the Automatically Unlock User scheduled task.

Working of the auto-unlock feature between Oracle Identity Manager and OAM is dependent on the fixes of the following bugs on top of Oracle Virtual Directory 11*g* Release 1 (11.1.1) Patch Set 5:

- Bug# 13503440: OVD: REDUCE TRANSACTION SEND TO BACKEND WHEN USING USERMANAGEMENT PLUGIN
- Bug# 14464394: NEW MAPPING FOR ORCLUSERLOCKEDON FOR CHANGELOG AND USERMANAGEMENT PLUGIN

10.3.85 Self Registration Request Fails

In an Oracle Identity Manager deployment on Microsoft Windows with OUD as the LDAP server, self registration request fails. Successful self registration request is dependent of the fix of the following libOVD bug:

Bug# 16523164: OIM/LIBOVD SHOULD REQUEST 'MODIFIERSNAME' WHEN SEARCHING IN CN=CHANGELOG

10.3.86 Catalog Synchronization Job Overrides Certifier/Approver/Fulfillment User

For role processing, run the Catalog Synchronization scheduled job one time in Full mode, and run it in Incremental mode from the next time onward. If the job is run again in Full mode, it overrides the current values for certifier, approver, and fulfillment user, and sets them to Role Owner.

10.3.87 Certification Creation Fails With Incorrect SSL Configuration

If SSL is not configured correctly, then certification creation might fail and the following error is displayed in the scheduler page for certification creation:

```
org.springframework.transaction.TransactionSystemException: JTA failure on commit;
nested exception is javax.transaction.SystemException: Could not contact
coordinator at
soa_server1+[2606:b400:2010:4049:216:3eff:fe52:65ba]:8002+RRC4SN130321+t3s+
        at
org.springframework.transaction.jta.JtaTransactionManager.doCommit(JtaTransactionM
anager.java:1044)
        at
```

To avoid this issue, SOA clear port must be opened when starting Oracle Identity Manager. If Oracle Identity Manager has been started with the clear SOA port closed, then re-open it and restart SOA and Oracle Identity Manager.

After the servers are started with clear port open, you can close the clear port. It is only required to be opened for starting the servers.

10.3.88 Role Certification Creation Fails With Only Certify Policy Option Selected

Role certification for only policies does not create certifications. While creating a role certification with content selected to certify only policies, the scheduler jobs fail with the following error:

```
java.lang.Exception: Role certification creation succeeded but with the following
errors: {0}. Role certification creation failed with the following error: null.
```

10.3.89 Duplicate Attribute Labels Displayed

While adding a custom attribute by using the Form Designer, the Add Content dialog box incorrectly displays two labels for the same custom attribute. For example, for the custom attribute Att1, labels Att1 and Att1_C are displayed. The correct label is Att1. If Att1_C is added, then it corrupts the sandbox, and the following error is generated:

```
JBO-25058: Definition Att1__c of type Attribute is not found in UserEO.
```

If the corrupted sandbox is published, then the customized screen is corrupted and does not open for any user. The only solution then is to rollback the sandbox. For information about rolling back the sandbox, search and see the technote "OIM 11gR2:

How to Roll back A Published Sandbox" (ID 1496179.1) by navigating to the following URL:

https://support.oracle.com

10.3.90 Error in Clone Log During PasteConfig Operation

During pasteConfig operation, if the specified target OPSS datasource URL is different than the source OPSS datasource URL, then clone log will have some SQL errors. However, the pasteConfig operation completes successfully. This error can be ignored.

Error in logs:

```
INFO: Found persistence provider
"org.eclipse.persistence.jpa.PersistenceProvider". OpenJPA will not be used.
INFO: Found persistence provider
"org.eclipse.persistence.jpa.PersistenceProvider". OpenJPA will not be used.
[EL Severe]: --ServerSession(515759393)--Exception
[EclipseLink-4002] (Eclipse Persistence Services - 2.3.1.v20111018-r10243):
org.eclipse.persistence.exceptions.DatabaseException
Internal Exception: java.sql.SQLException: ORA-01017: invalid
username/password; logon denied

Error Code: 1017
oracle.security.jps.internal.credstore.ldap.LdapCredentialStore <init>
WARNING: Could not create credential store instance. Reason
oracle.security.jps.service.policystore.PolicyStoreException:
javax.persistence.PersistenceException: Exception [EclipseLink-4002] (Eclipse
Persistence Services - 2.3.1.v20111018-r10243):
org.eclipse.persistence.exceptions.DatabaseException
Internal Exception: java.sql.SQLException: ORA-01017: invalid
username/password; logon denied

Error Code: 1017
opss-DBDS:oracle.jdbc.OracleDriver:t2pp_
OPSS:jdbc:oracle:thin:@example.com:1521/orcl.example.com
```

10.3.91 Slow Database Connection

You may encounter the following error message due to slow database connection:

```
<Error> <oracle.iam.oimdataproviders.impl>
<BEA-000000> <java.sql.SQLException: Internal error: Cannot obtain
XAConnection weblogic.common.resourcepool.ResourceDisabledException: Pool
oimOperationsDB is Suspended, cannot allocate resources to applications..
oracle.iam.platform.entitymgr.vo.ConnectivityException:
```

If you come across such error messages, perform the following steps:

1. Open the *DOMAIN_HOME*\bin\setSOADomainEnv.cmd file.
2. Uncomment the following lines:

   ```
   EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES}
   -Dweblogic.resourcepool.max_test_wait_secs=30"
   export EXTRA_JAVA_PROPERTIES
   ```

3. Save your changes and restart the Oracle Identity Manager managed Oracle WebLogic Server.

10.3.92 Scheduled Job Does Not Run

If any scheduled job does not run as scheduled, then perform any of the following:

- Restart Oracle Identity Manager server.
- Manually run the scheduled job from the UI by clicking Run Now.

10.3.93 QBE and User Membership Rule Work for Lookup Fields Only for Encoded Values

User membership rule for organizations and Query by example (QBE) work for custom lookup fields if the encoded lookup values are used instead of the display strings. For example, Account Status is a lookup with display values 'Locked' and 'Unlocked', but QBE and user membership rule work with Account Status if their encoded values are used, which are 1 and 0 respectively.

To workaround this issue, use simple or advanced search for searching custom lookup fields.

10.3.94 Role Name Displayed as Null

When creating a role certification with reviewer as Role Certifier, if a role has no certifier, then the certification job shows the following warning message:

```
java.lang.Exception: Role certification creation succeeded but with the following
errors: Role certification will not contain role "null": Role has no role owner
assigned to it.
```

The role name is displayed as 'null' in the warning message if the role does not contain a description.

10.3.95 Empty Results Displayed in the Organization Hierarchy and Management Hierarchy Tabs

If a user certification reviewer is in a different organization from the certifier, then empty results for the certifier are displayed in the organization hierarchy and management hierarchy tabs. This is because a reviewer cannot view the direct reports and organization hierarchy details of the certifier if the reviewer and certifier are members of different organizations, and are not related through the management hierarchy.

10.3.96 Request Approval Tasks Not Displayed in the Inbox With SSL Enabled

In a SSL-enabled Oracle Identity Manager setup with JDK 7u40 or later, request approval tasks are not displayed, and the following exception might be found in SOA logs:

```
Unable to invoke endpoint URI
"https://oimhost:oimport/workflowservice/CallbackService" successfully due to:
javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Message send
failed:
sun.security.validator.ValidatorException: PKIX path validation failed:
java.security.cert.CertPathValidatorException: Algorithm constraints check failed:
MD5withRSA
```

To workaround this issue, refer to the following sections in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*, and validate if the SSL setup has been configured correctly:

- "Generating Keys"
- "Enabling SSL for Oracle Identity Manager By Using Default Setting"
- "Enabling SSL for Oracle Identity Manager By Using Custom Keystore"

10.3.97 Error Logged for Some OUD Operations When LDAP Synchronization is Enabled

In an environment in which LDAP synchronization is enabled, certain operations against OUD fail with one of the following errors in OUD logs:

```
The request control with Object Identifier (OID) "1.2.840.113556.1.4.319" cannot
be used due to insufficient access rights
```

OR:

```
The request control with Object Identifier (OID) "1.3.6.1.4.1.26027.1.5.4" cannot
be used due to insufficient access rights
```

To workaround this issue:

1. Change the ACIs on control 1.2.840.113556.1.4.319 from ldap://all to ldap://anyone in OUD config file *OUD_INSTANCE*/config/config.ldif file, as shown:

   Change:

   ```
   ds-cfg-global-aci: (targetcontrol="1.3.6.1.1.12 || 1.3.6.1.1.13.1 ||
   1.3.6.1.1.13.2 || 1.2.840.113556.1.4.319 || 1.2.826.0.1.3344810.2.3 ||
   2.16.840.1.113730.3.4.18 || 2.16.840.1.113730.3.4.9 || 1.2.840.113556.1.4.473
   || 1.3.6.1.4.1.42.2.27.9.5.9") (version 3.0; acl "Authenticated users control
   access"; allow(read) userdn="ldap:///all";)
   ```

   To:

   ```
   ds-cfg-global-aci: (targetcontrol="2.16.840.1.113730.3.4.2 ||
   2.16.840.1.113730.3.4.17 || 2.16.840.1.113730.3.4.19 || 1.3.6.1.4.1.4203.1.10.2
   || 1.3.6.1.4.1.42.2.27.8.5.1 || 2.16.840.1.113730.3.4.16 ||
   2.16.840.1.113894.1.8.31 || 1.2.840.113556.1.4.319" ||
   1.3.6.1.4.1.26027.1.5.4 ) (version 3.0; acl "Anonymous control access";
   allow(read) userdn="ldap:///anyone";)
   ```

2. Restart OUD and Oracle Identity Manager servers.

10.3.98 Error Thrown When Oracle Identity Manager Uses Database in Oracle Enterprise Linux 6

When Oracle Identity Manager instance points to the database, which is running on Oracle Enterprise Linux 6, OutOfMemoryError might be thrown.

To avoid this issue, perform the following steps in Oracle Enterprise Linux 6 host on which the database is installed:

1. To fix any memory issue while starting database instances, add the following in the /etc/sysctl.conf file:

   ```
   kernel.shmmax = 12737418240 / kernel.shmall = 3109721
   ```

2. To fix any java.lang.OutOfMemoryError while starting Oracle Identity Manager Managed Servers:

a. Check `ulimit -u` or `sudo cat /proc/PROCESS_ID/limits`.

b. Change soft and hard limit in the /etc/security/limits.conf file to 327680.

c. Change soft limit in the /etc/security/limits.d/90-nproc.conf file to 327680.

10.3.99 The Design Console Hangs Intermittently

When Oracle Identity Manager is deployed on Microsoft Windows 2008 or 2012, the Design Console hangs intermittently while creating an adapter. After it hangs, there is no other way to kill the process and start a new session.

10.3.100 Lookup UDF Created with Maximum Length of 4000 Characters

New lookup UDFs are created with maximum length of 4000 characters although the default value is 100. Only the EO attribute (UI artifact) has the length constraint of 4000; backend database column has the correct length.

To workaround this issue, edit the UDF, set the correct length, and save the UDF.

10.3.101 UDF Not Removed From the Add Fields List

If a UDF is searchable, then it is displayed in the Add Fields drop down on the Search Users page. If you later mark the UDF as non-searchable by editing the UDF properties in the Form Designer, then the UDF is not automatically removed from the Add Fields drop down on the Search Users page.

To workaround this issue:

1. Extract the sandbox ZIP file that was used for editing the attributes to make the UDF non-searchable.
2. In a text editor, open the /persdef/oracle/iam/ui/common/model/user/view/mdssys/cust/site/site/UserVO.xml file.
3. For all such attributes that did not get removed from Add Fields drop down, add the `IsQueriable="false"` attribute in the corresponding <ViewAttribute Name="attrName"> tag. For example:

```
<ViewAttribute Name="UserTextUDF__c" EntityUsage="UserEO"
EntityAttrName="UserTextUDF__c" AliasName="UserTextUDF__c" IsPersistent="false"
xmlns="http://xmlns.oracle.com/bc4j" IsQueriable="false">
```

4. Save, re-zip, and import the sandbox. Test the changes in activated sandbox state. Publish the sandbox.

10.3.102 Deployment Manager Does Not Open After Updating to Java 7 Update 51

The Deployment Manager does not open after updating to Java 7 update 51 because of security-related attribute permission not being present in the JAR manifest, which can be bypassed by updating the security information in the Java Console. To do so:

1. Open the Java Console.
2. Click the Security tab.
3. Add the site name, which is in the following format:

```
http://HOST:PORT/xlWebApp/DeploymentManager/loadDU.do
```

10.3.103 Periodic Scheduled Job Throws NullPointerException

While running any periodic scheduled job, a NullPointerException is thrown. This is because the job parameter key is null during job creation.

To workaround this issue, delete the scheduled job, create a similar job as non-periodic, and then change it to a periodic job.

10.3.104 Notification Sent Although Notification Template Status is Disabled

If an end user, who does not have the System Configuration Administrator admin role in Top organization, is used to send notification, then the notification is sent although the status of the notification template is Disabled.

To workaround this issue, provide the System Configuration Administrator admin role in the Top organization to the user.

10.3.105 OUD Changlelogs Purged Before Incremental Reconciliation Runs

In an integrated deployment of Oracle Unified Directory (OUD) and Oracle Identity Manager, OUD changelogs might be purged before the Oracle Identity Manager incremental reconciliation runs. This can cause the following error:

```
Caused By: oracle.ods.virtualization.service.VirtualizationException:
oracle.ods.virtualization.engine.util.DirectoryException: LDAP Error 53 :
[LDAP: error code 53 - Full resync required. Reason: The provided cookie is older
than the start of historical in the server for the replicated domain :
dc=hsgbu,dc=oracle,dc=com]
```

The cause of this error is that OUD purges its replication store according to the interval specified by OUD's replication-purge-delay. This resets OUD's external changelog cookie. The cookie contains the value used by Oracle Identity Manager when comparing against its own stored last changelog number. Consequently, if the value is reset before Oracle Identity Manager can reset it by processing new changelog events, then the last changelog number for Oracle Identity Manager will be out of date, and the error will be generated.

To workaround this issue, re-synchronize the integration between OUD and Oracle Identity Manager. To do so:

1. Increase the changelog retention period in OUD as follows:
   a. (Optional) Display the current value of the replication purge delay by running the following command:

      ```
      $ dsconfig -h localhost -p 4444 -D "cn=directory manager" -w password -n \
        get-replication-server-prop \
        --provider-name "Multimaster Synchronization" --advanced \
        --property replication-purge-delay
      ```

   b. Change the purge delay by running the following sample command that changes the purge delay to one week:

      ```
      $ dsconfig -h localhost -p 4444 -D "cn=directory manager" -w password -n \
        set-replication-server-prop \
        --provider-name "Multimaster Synchronization" --set
      replication-purge-delay:1w
      ```

2. Disable all the incremental jobs, if not already disabled. There is a total of six incremental jobs.
3. Run the following full reconciliation jobs:

- LDAP Role Delete Full Reconciliation
- LDAP User Delete Full Reconciliation
- LDAP Role Create and Update Full Reconciliation
- LDAP Role Hierarchy Full Reconciliation
- LDAP User Create and Update Full Reconciliation
- LDAP Role Membership Full Reconciliation

4. Get the latest changelog from OUD by running the following command:

```
ldapsearch -h OUD_HOST -p OUD_PORT -D "cn=Directory Manager" -w PASSWORD -b ""
-s base "objectclass=*" lastExternalChangelogCookie
```

5. Update all six incremental jobs with the value obtained in step 4, and enable the incremental jobs.

10.3.106 Icon Not Displayed in Internet Explorer 11

When you open the Expression Builder to add or edit a rule in the Members tab for roles or organizations using Windows Internet Explorer 11, the icons to select AND, OR, and Remove are not displayed properly.

10.3.107 Offline Certification Not Supported in Internet Explorer 11

User certification in offline mode is not supported when Windows Internet Explorer 11 web browser is used.

10.3.108 Deployment Manager Fails to Import or Export

While using the Deployment Manager to import/export, the XML file generated while exporting cannot be saved, and the XML file cannot be read while importing. No error message is logged for this issue, but it is displayed that Java 1.3 or 1.4 is not letting I/O operations.

To grant permissions for I/O operations, add the following to the JRE/lib/security/java.policy:

```
grant {
    permission java.io.FilePermission "<<ALL FILES>>", "write";
};
```

This issue can occur with any Oracle Identity Manager version or Java version. Therefore, Java settings must be verified if Deployment Manager is throwing an error in reading the XML file during import when it prompts to select the XML file in the final step of exporting the file.

10.3.109 Error Message Logged When Creating a Disconnected Application Instance

When creating a disconnected application instance, the following error message is logged:

```
<Error> <oracle.iam.request.impl> <BEA-000000> <Failed to get the request data set
APP_INSTANCE_NAME from MDS with the error data set not found.>
```

This error is benign and can be safely ignored.

10.3.110 Error When Exporting Artifact Using Deployment Manager

While exporting any artifact using the Deployment Manager, the following error message is sometimes displayed:

```
Population can only be done in DBCREATED mode
```

The possible reason for this error is because the cache retains certain elements when the import operation is performed, and the export operation picks up the elements from the cache, which are not in the DBCREATED mode.

Completing any export or import wizard clears the cache, and therefore, resolves the issue. Therefore, export any unrelated independent artifact via the Deployment Manager, for example a system property, and then try the specific operation for which the issue was faced.

10.4 Configuration Issues and Workarounds

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

- Benign Connection Error From OIA For SoD Check
- Use Absolute Paths While Running configureSecurityStore.py With -m Join
- Oracle Identity Manager Fails to Find orclPwdExpirationDate
- Design Console Login Failure With SSL Enabled
- Create User Event Fails in Integrated Environment
- Insufficient Memory Causes Server Startup Failure
- OIMSignatureAuthenticator Not Configured for Oracle Identity Manager Domain Security Realm

10.4.1 Benign Connection Error From OIA For SoD Check

A connection error stating `Argument(s) "type" can't be null` is displayed intermittently when Oracle Identity Analytics (OIA) is configured for SoD Check, and an SoD Check is initiated. The error is as shown:

```
Caused By: oracle.iam.grc.sod.exception.SILServiceComponentException:
oracle.iam.grc.sod.scomp.impl.oia.analysis.SoDAnalysisExecutionOperOIA :
initializeUnable to connect to OIA Server : Argument(s) "type" can't be null.
```

This is a benign error and causes no functional loss.

10.4.2 Use Absolute Paths While Running configureSecurityStore.py With -m Join

The Config Security Store fails to create the policy store object when using variables, such as *ORACLE_HOME* and *MW_HOME*, while running wlst.sh using configureSecurityStore.py with -m join. Always use absolute paths for *ORACLE_HOME* and *MW_HOME* while running the command for -m join.

10.4.3 Oracle Identity Manager Fails to Find orclPwdExpirationDate

When OAM integration is enabled in Oracle Identity Manager that is configured with libOVD/OID, ODSEE, OUD, or AD, Oracle Identity Manager reset user password fails, and the `Attribute orclpwdexpirationdate is not supported in schema` error message is generated.

To workaround this issue, change the backend IDStore schema. To do so:

1. Create new attributetypes: `( 2.16.840.1.113894.200.1.7 NAME 'orclPwdExpirationDate' EQUALITY caseIgnoreMatch SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' SINGLE-VALUE USAGE userApplications ).`
2. Modify the orclIDXPerson objectclass to include orclPwdExpirationDate as an optional attribute.

10.4.4 Design Console Login Failure With SSL Enabled

If SSL is enabled on the Design Console, then login to the Design Console might fail with the following 'Invalid Login' error:

```
Error Keyword: DAE.LOGON_DENIED
Description: Invalid Login.
Remedy: Contact your system administrator.
Action: E
Severity: H
Help URL:
Detail:
javax.security.auth.login.LoginException: java.lang.NoClassDefFoundError:
com/rsa/jsafe/JSAFE_InvalidUseException
    at
weblogic.security.SSL.SSLClientInfo.getSSLSocketFactory(SSLClientInfo.java:101
)
    at
weblogic.socket.ChannelSSLSocketFactory.getSocketFactory(ChannelSSLSocketFactory.j
ava:185)
```

To workaround this issue, copy the *MIDDLEWARE_HOME*/modules/cryptoj.jar file to $*OIM_HOME*/designconsole/ext/ directory and login again.

10.4.5 Create User Event Fails in Integrated Environment

In an integrated environment of Oracle Access Manager, Oracle Identity Manager, and libOVD, for the Oracle Identity Manager create user event, the oblockedon attribute is not populated with the current date and time when orclAccountlocked=true. The attribute is populated with 0 value when orclAccountLocked=false.

To workaround this issue, apply the patch for the following OVD bug:

Bug# 16482350: OIM-OAM-LIBOVD:OUD: IAM-205024 FOR CREATING OIM USER

10.4.6 Insufficient Memory Causes Server Startup Failure

If Oracle Identity Manager server fails to start because of insufficient native memory for Java, then make sure to set memory settings to accommodate heap size.

When Oracle Identity Manager is installed on Microsoft Windows with Jrocket Java (for example jrockit-jdk1.6.0_37-R28.2.5-4.1.0), Java/JVM gets terminated when servers are started. This is caused by the -Xmx2048m memory settings for the CUSTOM_MEM_ARGS_64BIT environment variable in the setDomainEnv script. To avoid this issue, this memory setting must be changed to the recommended value. Here setting it to a value of -Xmx1538m resolves the issue. To do so:

1. In a text editor, open the $*DOMAIN_HOME*/bin/setDomainEnv.cmd file.
2. In the following snippet:

```
if "%JAVA_VENDOR%"=="Oracle" (
```

```
set CUSTOM_MEM_ARGS_64BIT=-Xms1024m -Xmx2048m -XX:PermSize=512m
-XX:MaxPermSize=1024m
set CUSTOM_MEM_ARGS_32BIT=-Xms1024m -Xmx2048m -XX:PermSize=512m
-XX:MaxPermSize=1024m
) else (
set CUSTOM_MEM_ARGS_64BIT=-Xms1024m -Xmx2048m -XX:PermSize=512m
-XX:MaxPermSize=1024m -XX:ReservedCodeCacheSize=256m
set CUSTOM_MEM_ARGS_32BIT=-Xms1024m -Xmx2048m -XX:PermSize=512m
-XX:MaxPermSize=1024m -XX:ReservedCodeCacheSize=256m
)
```

Modify the lines with CUSTOM_MEM_ARGS_64BIT within the If condition to the following for 64-bit host. Otherwise, modify CUSTOM_MEM_ARGS_32BIT.

```
set CUSTOM_MEM_ARGS_64BIT=-Xms1024m -Xmx1538m -XX:PermSize=512m
-XX:MaxPermSize=1024m
```

3. Save the setDomainEnv.cmd file and restart the servers.

10.4.7 OIMSignatureAuthenticator Not Configured for Oracle Identity Manager Domain Security Realm

In a Oracle Identity Manager deployment that is integrated with Access Manager (OAM), OIMSignatureAuthenticator is not configured in the Oracle Identity Manager domain's security realm. As a result, the following error can occur on the Oracle Identity Manager server:

```
<Error> <XELLERATE.ACCOUNTMANAGEMENT> <BEA-000000> <Class/Method:
tcUtilityFactory/tcUtilityFactory(Hashtable env, tcSignatureMessage
poUserIDMessage) encounter some problems:
javax.security.auth.login.LoginException: java.lang.SecurityException:
[Security:090304]Authentication Failed: User xelsysadm
javax.security.auth.login.FailedLoginException: [Security:090302]Authentication
Failed: User xelsysadm denied
javax.security.auth.login.LoginException:
javax.security.auth.login.LoginException: java.lang.SecurityException:
[Security:090304]Authentication Failed: User xelsysadm
javax.security.auth.login.FailedLoginException: [Security:090302]Authentication
Failed: User xelsysadm denied
        at
weblogic.security.auth.login.UsernamePasswordLoginModule.login(UsernamePasswordLog
inModule.java:199)
```

This exception can occur in any one of the following scenarios:

- You are using a 9.x connector, which performs signature-based login to Oracle Identity Manager. To perform signature-based client login in an Oracle Identity Manager deployment integrated with OAM, the following configuration must be performed:

  1. Login to the WebLogic Administrative Console.
  2. Go to **Security realms**, **myrealm**, **Providers**, **Authentication**.
  3. Click **New**, add OIMSignatureAuthenticator, and provide a name, such as `OIMSignatureAuthenticator`.
  4. Click **OIMSignatureAuthenticator** that you added in step 3, and set the control flag as **SUFFICIENT** from the drop down. Save the changes.
  5. Click **Reorder**, and re-order the existing authentication providers as follows:

  - OAMIDAsserter
  - OIMSignatureAuthenticator
  - LDAPAuthenticator (such as OID/OUD, depending on the directory type)
  - DefaultAuthenticator
  - DefaultIdentityAsserter

6. Save and activate the changes done so far.
7. Restart all the servers running in the Oracle Identity Manager WebLogic domain.

- You have custom Oracle Identity Manager client code, which performs signature-based login by using the tcUtilityFactory or OIMClient APIs. For this scenario, resolve the issue by referring to "Using OIMClient and tcUtilityFactory in Integrated Deployments" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

10.5 Multi-Language Support Issues and Limitations

This section describes multi-language issues and limitations. It includes the following topics:

10.5.1 UI Components are Displayed in English on non-English Web Browsers

On the Lookups or Form Details pages in Oracle Identity System Administration, UI components are displayed in English on non-English web browsers.

This is known issue, and a workaround is currently not available.

10.5.2 BI Publisher 11g Reports Displayed in English Although Translation Files Are Available

Oracle Identity Manager 11*g* Release 2(11.1.2) supports BI Publisher 11*g* for Oracle Identity Manager reports. The translations for these Oracle Identity Manager reports must be manually imported. Oracle Identity Manager has centralized translations, each locale has a XLIFF (.xlf) file for all the Oracle Identity Manager reports.

By default, all BI Publisher 11*g* reports are displayed in English. Import the translations files to BI Publisher.

To import a XLIFF file:

1. In Oracle BI Publisher Enterprise, select the Oracle Identity Manager folder in the catalog.
2. Click the Translation toolbar button, and then select **Import XLIFF**.
3. Click **Browse** to locate the translated file, and then select the appropriate locale from the list.
4. Click **Upload**.

First, upload all the transaction files in the catalog for each report. Select the report, and then change the report locale and UI language locale to run the report in different locale.

10.5.3 Date Format in BI Publisher Report Not Displayed Per Report Locale Setting

The date format in the content and footer of the BI Publisher report is not displayed according to the value specified in Report Locale setting for the logged-in user.

This is a known issue, and a workaround is currently not available.

10.5.4 Translated Values Not Displayed for User Type and Locale

In the Create User and Modify pages, values of the following attributes are displayed in English irrespective of the browser language setting:

- User Type, in the Basic Information section
- Locale, in the Preferences section

This is a known issue, and a workaround is currently not available.

10.5.5 Catalog Search With Special Non-ASCII Characters Do Not Work Correctly

If catalog items, such as roles, application instances, and entitlements, contain special non-ASCII characters, such as some German, Greek, or Turkish characters, then the search pattern with these characters do not return correct results.

This is a known issue, and a workaround is currently not available.

10.5.6 Polish Translation of BI Publisher Files Do Not Work

BI Publisher 11.1.1.6.0 and 11.1.1.7.0 cannot handle the string colon(:). Therefore, Polish translation of BI Publisher files do not work correctly.

This is a known issue, and a workaround is currently not available.

10.5.7 Localized String for Cart is Truncated in the Catalog Search Results Page

In the Catalog Search Results page, the localized string for Cart on the top right of the page is displayed as truncated text.

This is a known issue, and a workaround is currently not available.

10.5.8 Values Not Displayed Per Browser Language Setting

Some fields with drop-down list are displayed in English instead of the browser language setting. For example:

- The following option values of the SortBy list on the Catalog Search page:
  - Type
  - Display Name
- The following option values of the Risk Level list on the Detailed Information panel of the Catalog search result page:
  - High Risk
  - Medium Risk
  - Low Risk
- The following Task Status option values in the Search panel, and values under Task Status column of Search Results table on the Provisioning Tasks page:
  - Pending
  - Rejected
- Values in the Type list on the Form Designer page.

This is a known issue, and a workaround is currently not available.

10.5.9 Challenge Questions and Password Policy Messages Displayed in Server Locale

After restarting Oracle Identity Manager and navigating to the self registration or Forgot Password pages when no user is logged in, the Challenge Questions and Password Policy messages are intermittently displayed in server locale instead of browser locale.

To workaround this issue, login to Oracle Identity Self Service by using any available user login credentials after Oracle Identity Manager is started or restarted.

10.5.10 Values for Organization Type and Status Displayed in English

The values in the Organization Type or Status lists in some pages are displayed in English although the browser is set with a non-English locale. For example:

- The values in the Organization Type or Status lists in the Admin Roles tab of the My Access page in Oracle Identity Self Service.

- The values in the Organization Type or Status lists for any selected admin role in the Admin Roles tab of User Details page in Oracle Identity Self Service.
- The values in the Organization Type or Status lists in the Organizations tab of Role Details page in Oracle Identity Self Service.
- The values in the Organization Type or Status lists for any selected suborganization in the Children tab of Organization Details page in Oracle Identity Self Service.
- The values in the Organization Type or Status lists in the Search Parent Organization dialog box when creating new organization in Oracle Identity Self Service.
- The Type column of the Organizations tab of the Application Instances page in Oracle Identity System Administration.

This is a known issue, and a workaround is currently not available.

10.5.11 MLS and MR Support Not Available

Multi-Language Support (MLS) and Multi-Representation (MR) support are not available for Role Display Name and User Display Name in Oracle Identity Self Service.

10.5.12 Error Displayed If User Login Contains Special Character

If user login name contains a special character, such as German Esszet character or Turkish dotted I character, then the following error message is displayed on clicking Inbox on the left navigation pane in Oracle Identity Self Service:

```
An internal error has occurred. Please contact the administrator or Oracle support
for help
```

10.5.13 Task Stage Name and Task Assignee Label Displayed in English

When you open the request details in the Track Requests page and navigate to the History Panel in the Approval Details tab, the task stage name and task assignee label are displayed in English instead of the translated language.

10.5.14 Escalating Request Displayed Warning in Server Locale

If a request assignee has no manager, then escalating this request displays a warning message. The warning message is displayed in server locale instead of browser locale.

10.5.15 Some Predefined View Names Cannot Be Translated

The following predefined view names in the Inbox are hard coded in English and cannot be translated:

- Pending Approvals
- Pending Certifications
- Manual Provisioning

10.5.16 Request Task Details Displayed in Server Locale

From the Home page or Inbox in Oracle Identity Self Service, when you open a task, the task detail is displayed in server locale instead of browser locale.

10.5.17 Oracle Identity Manager Operation Names Not Translated in Enterprise Manager

In Oracle Identity Manger Administration pages of Oracle Enterprise Manager that provides business operation diagnostic capabilities, there is no translation for the operation names. The following operation names are not translated:

- Modify an Account by Access Policy
- Revoke an Account by Access Policy
- Disable an Account by Access Policy
- Enable an Account by Access Policy
- Provision an Account by Access Policy
- Modify Account
- Revoke Entitlement
- Assign Role Membership
- Delete Role Membership
- Create User
- Change Password
- Reset Password
- Enable User
- Disable User
- Delete User
- Modify User
- Modify Role Membership
- Lock User
- Unlock User
- Add Proxy
- Update Proxy
- Remove Proxy
- Remove All Proxies
- Set Challenge Question Answers
- Password Expired
- Provision Account
- Grant Entitlement
- Modify Entitlement
- Disable Account

- Enable Account
- Revoke Account
- Change Account Password
- Evaluate Policies
- Bulk Request
- Associate Application Instance with reconciled account
- Update Application Instance with reconciled account
- Delete Application Instance with reconciled account
- Create Role
- Modify Role
- Delete Role
- Modify Role Auto group membership rule

10.5.18 Display Label Not Shown Correctly When Browser Language is Switched

When the resource type form, such as form for AD User, is created with browser language XX-YY, Display Label is shown correctly in the browser language XX-YY. However, when the browser language is switched to others, for example XX or MM-NN, and the same form is opened, Display Label is shown incorrectly as UD_ XXXXX similar to the Name value.

To workaround this issue:

1. Create the resource type form with browser language as XX.
2. Apply the new create resource type form to application instance. Then, you can view the form with the correct browser language XX and XX-NN.

For example, for Japanese language, create the resource type form with browser language ja. Then, the form is displayed correctly with browser language of both ja and ja-JP.

10.5.19 User Type Values Not Translated

The following values of the User Type list are displayed in English on the Create User page irrespective of the browser language setting:

- Employee
- Contingent Worker
- Non Worker
- Other

To workaround this issue:

1. Navigate to the $*ORACLE_HOME*/server/apps/oim.ear/APP-INF/classes/ directory.
2. Open the xlWebAdmin_*LANG*.properties file for your locale. For example, open the xlWebAdmin_ja.properties file for Japanese language.
3. Add following lines with unicode text and save the file.

```
global.Lookup.Users.Role.EMP=\u5F93\u696D\u54E1
```

```
global.Lookup.Users.Role.CWK=\u6D3E\u9063\u5C31\u696D\u8005
global.Lookup.Users.Role.NONW=\u975E\u5C31\u52B4\u8005
global.Lookup.Users.Role.OTHER=\u305D\u306E\u4ED6
```

The lines of code are translations for Employee, Contingent Worker, Non Worker, and Other respectively.

4. Restart Oracle Identity Manager.

10.5.20 Online Help Translated in Nine Languages

Oracle Identity Manager online help is not translated in all supported languages. It is translated in the following languages:

- Brazilian Portuguese
- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese
- Spanish
- Traditional Chinese

10.6 Documentation Errata

Currently, there are no documentation issues to note.

11

Oracle Identity Management Integration

This chapter describes issues associated with Oracle Identity Management integrations. It contains the following topics:

11.1 Integrating Access Manager and Oracle Adaptive Access Manager

This section contains issues related to the integration of Oracle Access Management Access Manager with Oracle Adaptive Access Manager. It contains the following topics:

11.1.1 The setupOAMTAPIntegration Script Fails with Permissions Issues

During the integration of Access Manager and Oracle Adaptive Access Manager, you must provide the WebLogic/WebSphere Admin user name and password when running the `setupOAMTAPIntegration` script to configure Access Manager for TAP integration. If you provide the OAAM Admin user name and password, the script fails because the OAAM Admin user does not have the permissions required to run the script.

Also, the following incorrect `FileNotFoundException` error message is displayed, which does not inform you that you have entered an incorrect user name and password:

```
java.io.FileNotFoundException: .\config\jps-config.xml
```

If valid data is provided, the script works as expected.

11.1.2 Login to a Protected Resource May Fail in an Access Manager Release 2 PS2 and Oracle Adaptive Access Manager Release 2 TAP Integrated Environment

Login to a protected resource may fail with an invalid class exception in an Access Manager Release 2 PS2 and Oracle Adaptive Access Manager Release 2 TAP integrated environment if a user session is still active prior to the Access Manager upgrade from Release 2 to Release 2 PS2 and the pre-upgrade session information is used post-upgrade. For the integration to work properly, before shutting down or starting the servers prior to the upgrade, you must stop all existing stale pre-upgrade sessions by clicking **Delete All User Sessions** in the Session Management page. For more information about session management, refer to the "About the Session Management Page" section in the "Managing Sessions" chapter of the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management* 11g Release 2.

11.1.3 Lock User is Unable to Unlock Self in an Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager Integrated Environment

In an Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager integrated environment, when an end user is locked in OIM and LDAP by providing multiple incorrect passwords, and he provides valid credentials in the OAAM login page, the user is denied access and an error message similar to the following is displayed:

```
User account is disabled. Please contact customer service
```

The locked user is not redirected to an account locked page with the **Forgot your password** link that enables him to use the Forgot Password flow to unlock himself. In an Access Manager and Oracle Identity Manager integrated environment, the locked user is redirected to an account locked page with the **Forgot your password** link available to him.

11.1.4 Invalid Class Exception When Password Policy Fails

In an OAAM 11g Release 1 PS2 (11.1.1.3) and OIM 11g Release 2 PS1 (11.1.2.1) or OAAM Release 2 PS1 (11.1.2.1) and OIM Release 1 PS2 (11.1.1.3) integrated environment, when the end user enters a password that violates the default password policy in the Expired, Forgot, or Change Password flow, the following message is displayed:

```
An error occurred while attempting to change your password. Please try again
```

An invalid class exception similar to the following is shown in error log file:

```
<Apr 13, 2013 5:06:09 AM CST> <Error> <oracle.oaam> <BEA-000000>
<failed to changePassword(john.doe@example.com)
javax.ejb.EJBException: Problem deserializing error response; nested
exception is:
java.io.InvalidClassException:
oracle.iam.identity.exception.IdentityException; local class incompatible:
stream classdesc serialVersionUID = 1935467088360363654, local class
```

```
serialVersionUID = -7391301560574640548; nested exception is:
java.io.InvalidClassException:
oracle.iam.identity.exception.IdentityException; local class incompatible:
stream classdesc serialVersionUID = 1935467088360363654, local class
serialVersionUID = -7391301560574640548
at weblogic.ejb.container.internal.RemoteBusinessIntfProxy.unwrapRemoteException(
RemoteBusinessIntfProxy.java:121)
at weblogic.ejb.container.internal.RemoteBusinessIntfProxy.invoke(RemoteBusinessI
ntfProxy.java:96)
at $Proxy163.changePasswordx(Unknown Source)
at oracle.iam.identity.usermgmt.api.UserManagerDelegate.changePassword(Unknown
Source)
...etc
Caused By: java.io.InvalidClassException:
oracle.iam.identity.exception.IdentityException; local class incompatible:
stream classdesc serialVersionUID = 1935467088360363654, local class
serialVersionUID = -7391301560574640548
        at java.io.ObjectStreamClass.initNonProxy(ObjectStreamClass.java:562)
        at
java.io.ObjectInputStream.readNonProxyDesc(ObjectInputStream.java:1582)
...etc
```

The password related flows work if a valid password that adheres to the defined password policy is provided. The error does not affect the flow.

11.1.5 User Unlock Exception Occurs in Change Password/Forgot Password Flow

In an Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager integrated environment, during the Change Password/Forgot Password flow, an `UserUnlockException` error is shown even though the flow is successful.

11.1.6 ChangePassword.credentials.enum Not Found Error Occurs in Change Password Flow

In an Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager integrated environment, during the Change Password flow, a `ChangePassword.credentials.enum not found` error is shown even though the flow is successful.

11.1.7 Access Manager and Oracle Adaptive Access Manager Integrations Using OAAMBasic and OAAMAdvanced Schemes Deprecated

Oracle Access Management Access Manager and Oracle Adaptive Access Manager integrations using OAAMBasic and OAAMAdvanced authentication schemes are deprecated starting with 11.1.2.2 and will be desupported in 12.1.4 and future releases. The recommendation is to use the Oracle Access Management Access Manager and Oracle Adaptive Access Manager integration using Trusted Authentication Protocol (TAP) instead of OAAMBasic and OAAMAdvanced integrations. For information about Access Manager and Oracle Adaptive Access Manager integration using TAP, see *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

11.1.8 Multiple Sessions Created Instead of Unified Session for an Access Manager - OAAM TAP Integrated Environment

In an Access Manager and OAAM integrated environment multiple sessions were created instead of a unified session for a particular user. As result session count

increased for the user and reached its maximum limit. Over a period of time, this resulted in orphaned sessions. To work around this issue, set the following OAAM property:

```
oaam.uio.oam.authenticate.withoutsession=false
```

11.2 Natively Integrating Oracle Adaptive Access Manager

This section contains issues related to OAAM native integration. It contains the following topic:

- Section 11.2.1, "generateOTP() API Has Been Deprecated"

11.2.1 generateOTP() API Has Been Deprecated

The `generateOTP()` API has been deprecated in the OAAM JAVA and SOAP APIs. Please use the `getOTPCode()` API instead when writing your production code. For details on how to use the `getOTPCode()` API, see the *Oracle Fusion Middleware Java API Reference for Oracle Adaptive Access Manager*.

11.3 Documentation Errata

This section contains the following documentation errata for the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

11.3.1 Remove oaam.oim.passwordflow.unlockuser Property from the Documentation

In the Access Manager-OAAM-OIM integration, the `oaam.oim.passwordflow.unlockuser` property is no longer needed and should be removed from Section 3.8.2, Table 3-7 of the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

11.3.2 The oaam.uio.oam.authenticate.withoutsession Property Setting

In Section C.7.4.4, change "For Access Management 11g Release 1 (11.1.1) and earlier: `oaam.uio.oam.authenticate.withoutsession = false`" to "For Access Management 11g: `oaam.uio.oam.authenticate.withoutsession = false`." This setting applies to all 11g releases.

12

Oracle Fusion Middleware on IBM WebSphere

This chapter describes issues you might encounter when you install and configure supported Oracle Fusion Middleware products on IBM WebSphere. It includes the following topics:

12.1 General Issues and Workarounds

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

12.1.1 Additional Debug/TRACE Details in Exception Message

If a runtime exception is thrown by an EJB, IBM WebSphere adds additional debug details to the exception message. This can result in incorrect error messages on the UI.

To fix this issue, add the com.ibm.CORBA.ShortExceptionDetails JVM property to the Oracle Identity Manager server by using the WebSphere Console, and set its value to `true`. Make this change on all relevant application servers, save the configuration, and restart all the relevant servers.

For information about adding the JVM property, refer to IBM WebSphere Application Server documentation by navigating to the following URL:

http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fxrun_jvm.html

12.1.2 Cell Creation Fails When Multiple Templates are Selected With Oracle Identity Manager in the Same Session

As part of Oracle Identity Manager cell creation using was_config.sh or was_config.bat, if you select additional templates, such as Oracle Entitlements Server (OES) template, then cell creation fails.

To avoid this issue, first create the cell with Oracle Identity Manager template only, and then extend the cell with additional templates as required.

12.1.3 Opening Identity Directory Service Profile Displays Warning Popup in Oracle Entitlements Server

When configuring the Identity Directory Service Profile in Oracle Entitlement Server Administration Console (System Configuration tab > IDS Profile > Open), a warning popup may display. For example: `Cannot acquire a read-write connection; using a read-only connection instead`.

This can occur when Identity Directory Service is attempting to connect to the Mbean Server. When connecting to the Mbean Server, an exception may be thrown indicating the attempt to create a listener failed. In this case, check the standard output (for example, SystemOut.log) of the corresponding server. Before the exception stack trace the cause of the failure will be mentioned. For example:

```
[9/17/12 4:58:16:286 PDT] 00000020 ORBRas        E
com.ibm.ws.orbimpl.transport.WSTransport createServerSocket WebContainer : 0
ORBX0390E: Cannot create listener thread. Exception=[ org.omg.CORBA.INTERNAL:
CAUGHT_EXCEPTION_WHILE_CONFIGURING_SSL_SERVER_SOCKET,
Exception=org.omg.CORBA.INTERNAL: UNABLE_TO_CREATE_SSL_SERVER_SOCKET
Exception=java.net.BindException: Address already in use
vmcid: 0x49421000  minor code: 76  completed: No  vmcid: 0x49421000  minor code:
77  completed: No
- received while attempting to open server socket on port 9404 ]
```

The problem is a port conflict exists when trying to open a socket on a port that is already in use. For more information about this issue, see the following IBM technical note at: http://www-01.ibm.com/support/docview.wss?uid=swg21248645.

To workaround this issue, change the port settings to be dynamic (by specifying port="0" for specific endpoints in serverindex.xml) as discussed in the IBM technical note.

12.1.4 Cannot Create CSF Mapping in IBM WebSphere with Target Domain in WebLogic Server

When Oracle Privileged Account Manager is running on IBM WebSphere, you cannot add CSF mappings corresponding to a Oracle WebLogic Server domain.

Similarly, when Oracle Privileged Account Manager is running on Oracle WebLogic Server, you cannot add CSF mappings corresponding to a IBM WebSphere cell.

12.1.5 OIMAdmin Keys Credential Might Be Lost

In an Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) deployment that has been upgraded from Release 9.x, OIMAdmin Keys Credential might be lost if SOA communication issues for authentication are found in the logs. There errors can occur if the user in the first run has not set .xldatabasekey, which is a prerequisite for running MT in PRE_CONFIG_MODE.

The following is an example of logged error:

```
[oim_server1] [ERROR] [] [oracle.soa.services.workflow.worklist] [tid:
WebContainer : 5] [ecid: disabled,0] [APP:
oracle.iam.console.identity.self-service.ear] <Fatal Error occurred while
authenticating with EJB identity propagation. Unable to get the workflow
context using authenticate.getWorkflowContextFromSession>
oracle.bpel.worklistapp.util.WorklistUtil
```

To workaround this issue:

1. Login to Oracle Enterprise Manager.
2. Right click **Cell_Websphere**, and select **Security**, **Credentials**.
3. Expand oracle.wsm.security.
4. Select **OIMAdmin key**, and click **Edit**. If OIMAdmin key does not exist, then create it by clicking **Create Key** in the oracle.wsm.security map.
5. In the Edit Key dialog box, enter the xelsysadm credentials.
6. Stop Oracle Identity Manager Server, SOA Server, and Admin Server in respective sequence. Stop node, and stop Manager.
7. Start Manager, sync node, and start node. Start Admin Server, SOA Server, and Oracle Identity Manager Server in respective sequence.

12.1.6 Warnings, Errors and Stack Traces Appear in oaam_admin Log File of OAAM Configured on IBM WebSphere

The following warnings, errors, and stack traces often appear in the `oaam_admin` log of OAAM on IBM WebSphere Application Servers, but do not have any effect on functionality:

- Failed to register connection type (`WARNING`)
- Could not load properties file `bharosa_server.properties` (`ERROR`)
- Could not load properties file `oaam_custom.properties` (`ERROR`)

- Unable to customize `Oracle`, `OAAM`, `view`, or `DataBindings.cpx`. Empty or null value for tip customization layer user (stack trace)
- The operation on the resource, pages, or `loginPageDef.xml` failed because the source metadata store mapped to the namespace or `BASE DEFAULT` is read only (stack trace)
- Exception while querying the `ExalogicOptimizationsEnabled` attribute (`WARNING`)

12.1.7 Task Details Page Might Throw ADFC-12000 Errors

In an Oracle Identity Manager deployment on IBM WebSphere Application Server, performing any action on the Task Details page of the Inbox might throw ADFC-12000 errors.

To workaround this issue, close the browser session, and access the Task Details page in a new session.

12.1.8 Oracle Identity Federation Audit Records Not Moved to Database

Problem

When you configure the audit service to move audit records to the database, the Oracle Identity Federation busstop file at: `%DOMAIN_HOME%/servers/%INSTANCE_NAME%/logs/auditlogs/OIF` is updated. However these audit records are not populated in the database.

Workaround

To resolve this, enter the `wsadmin` scripting environment and run the following command:

```
wsadmin>sts_
commands.putStringProperty("/notifierconfig/CommonAuditListenerConfig/auditbusstop
","%DOMAIN_HOME%/logs/%INSTANCE_NAME%/auditlogs")
```

This action should result in a "Command was successful." message.

12.1.9 All Channels Cannot be SSL Enabled between OIM and Database Server on Websphere

All channels can not be SSL enabled between OIM and Database server on Websphere.

OIM application has three different channels to the database:

- Data Sources
- Direct DB for DDL operations
- Custom registry

Of the three listed above, only the Data Source channel can be SSL enabled. To do so, add the following custom property on each data source:

```
Name: connectionProperties
```

```
Value:javax.net.ssl.trustStore=TRUST_STORE_
LOCATION;javax.net.ssl.trustStoreType=JKS;javax.net.ssl.trustStorePassword
=TRUST_STORE_PASSWORD;oracle.net.ssl_version=3.0
```

replace `TRUST_STORE_LOCATION` and `TRUST_STORE_PASSWORD` with appropriate values.

12.1.10 Enterprise Manager Does Not Reflect the State of WebSphere Cell

Oracle Enterprise Manager is accessible, but it does not reflect the exact state of the WebSphere cell. Although all the servers are running, they are shown as DOWN.

To workaround this issue, copy the dmsapp.jar file to both the DMS Application locations. To do so:

1. Locate the dmsapp.jar file inside was-dms.ear by unzipping new was-dms.ear to a directory.
2. Replace dmsapp.jar inside both the DMS Application locations with the new dmsapp.jar. The directory paths for both DMS Application locations are:
   - ./was5012/profiles/Dmgr01/installedApps/DefaultCell01/Dmgr DMS Application_11.1.1.1.0.ear/dms.war/WEB-INF/lib/dmsapp.jar
   - ./was5012/profiles/Custom01/installedApps/DefaultCell01/DMS Application_11.1.1.1.0.ear/dms.war/WEB-INF/lib/dmsapp.jar
3. Restart all servers including the Node Manager and the Deployment Manager.

12.1.11 End User Names with Character "#" Created in Oracle Identity Manager Cannot Login to Oracle Privileged Account Manager

If you create an end user name in Oracle Identity Manager that contains a pound symbol (**#**) character, that user will not be able to log into Oracle Privileged Account Manager.

To workaround this issue, avoid using the pound symbol (**#**) character in end user names that will be logging into Oracle Privileged Account Manager.

12.1.12 Error Generated When Launching Patch Set Assistant on Solaris 10 Machines Configured with WebSphere

The following error is generated when launching the Patch Set Assistant from `ORACLE_HOME/bin` of Oracle Identity and Access Management installs on Solaris 10 machines configured with WebSphere:

```
WAS_HOME=<PATH to WAS_HOME>: is not an identifier
```

To workaround this issue:

Before invoking the PSA for patching on Solaris, apply Patch:16270302 from My Oracle Support (MOS) to the Oracle Identity and Access Management install location.

12.1.13 Provisioning of GTC-Based Connector Fails with Error

After upgrading Oracle Identity Manager Release 9.x to 11*g* Release 2 (11.1.2.2) on WebSphere, the provisioning of GTC-based connector fails with the following error:

```
Response: org.apache.commons.pool.ObjectPool
Response Description: Unknown response received
Setting task status... "org.apache.commons.pool.ObjectPool" does not correspond to
a known Response Code. Using "UNKNOWN".
```

To workaround this issue:

1. Stop IBM WebSphere Application Server.
2. Copy the commons-pool-1.2.jar file from oim.ear/xlWebApp.war/WEB-INF/lib/ directory to the oim.ear/APP-INF/lib directory.

3. Restart IBM WebSphere Application Server.

12.1.14 Error on Closing the Request Tab When Inbox is Open

In a single-node or clustered deployment of Oracle Identity Manager 11*g* Release 2 (11.1.2.2), when the Inbox tab is open, after the request submission if you close the Catalog Request tab or click the Back to Catalog button, then the following error is displayed:

```
ADF_FACES-60096:Server Exception during PPR, #1[[
com.ibm.websphere.servlet.error.ServletErrorReport:
java.lang.ClassCastException: [Ljava.lang.Object&#59; incompatible
with org.apache.myfaces.trinidad.component.StampState$RowState
```

This error does not have an impact on any functionality of Oracle Identity Manager. To avoid this error, close the Inbox before closing the Request tab. Also, the error disappears on refreshing the page.

12.1.15 Identity and Access Option Not Available in EM After Upgrade

After upgrading Oracle Identity Manager 11*g* Release 2 (11.1.2.1) to 11*g* Release 2 (11.1.2.2), the **Identity and Access** option is not available in Oracle Enterprise Manager. This issue is applicable to single-node and clustered upgrade.

To workaround this issue:

1. Stop all servers including the Deployment Manager.
2. Create a directory called `oim` under the $*WAS_HOME*/profiles/DmgrProfileName/config/cells/DefaultCellName/fmwconfig/mbeans/ directory, if it is not already present.
3. Copy the following file:

   $*MW_HOME*/Oracle_IDM1/server/setup/templates/was/oim-mbeans.xml

   To the following directory:

   $*WAS_HOME*/profiles/DmgrProfileName/config/cells/DefaultCellName/fmwconfig/mbeans/
4. Next, copy the following file:

   $*MW_HOME*/Oracle_IDM1/server/setup/templates/was/oim-clustermbean.jar

   To the following directory:

   $*WAS_HOME*/profiles/DmgrProfileName/config/cells/DefaultCellName/fmwconfig/mbeans/oim/
5. Verify that patch 17894163 is applied on *ORACLE_COMMON*. If the patch is not applied, then apply it on *ORACLE_COMMON* by downloading it from My Oracle Support web site at:

   https://support.oracle.com
6. Start all servers.
7. Redeploy Oracle Enterprise Manager. To do so:
   a. Login to IBM WebSphere Administrative Console.
   b. Select **Applications**, **Application Types**, **Websphere Enterprise Applications**.

c. Select the **em** option from the list, and then click **Update**.

d. Select the **em.ear** file, which is available in the *$MW_HOME*/oracle_common/sysman/archives/fmwctrl/app/ directory. Then, click **Next**.

e. Click **Next**.

f. Click **Next**.

g. Verify that the module maps to OracleAdminServer by default, and then click **Next**.

h. Click **Finish**.

i. After the deployment is done, click **Save** to save the configuration.

8. Restart OracleAdminServer.

You can now login to Oracle Enterprise Manager and verify that the **Identity and Access** option is available along with all the submenu options.

12.2 Configuration Issues and Workarounds

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

12.2.1 SSLHandshakeException Error for Google and Yahoo IdP Partners

When you integrate Access Manager with Identity Federation, and configure a Google or Yahoo IdP partner for federated SSO on IBM WebSphere application server through

the OpenID protocol, you may see an `SSLHandshakeException` error when you attempt to access the resource.

For a Google partner, the error is as follows:

```
oracle.security.fed.controller.library.LibraryException:
oracle.security.fed.controller.frontend.action.exceptions.ResponseHandlerExcep
tion: oracle.security.fed.util.http.HttpException:
javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.j: PKIX path building
failed: java.security.cert.CertPathBuilderException: PKIXCertPathBuilderImpl
could not build a valid CertPath.; internal cause is:
        java.security.cert.CertPathValidatorException: The certificate issued
by OU=XXX Secure Certificate Authority, O=XXX, C=US is not trusted;
...
```

For a Yahoo partner, the error is as follows:

```
[2013-02-15T15:18:58.747-08:00] [oam_server1] [WARNING] [OAM-12001]
[oracle.oam.audit] [tid: WebContainer : 5] [ecid: disabled,0] [APP:
oam_server_11.1.2.0.0] Cannot load audit configuration.
[2013-02-15T15:18:58.749-08:00] [oam_server1] [WARNING] [OAM-12001]
[oracle.oam.audit] [tid: WebContainer : 5] [ecid: disabled,0] [APP:
oam_server_11.1.2.0.0] Cannot load audit configuration.
[2013-02-15T15:18:58.750-08:00] [oam_server1] [WARNING] [OAM-12001]
[oracle.oam.audit] [tid: WebContainer : 5] [ecid: disabled,0] [APP:
oam_server_11.1.2.0.0] Cannot load audit configuration.
[2013-02-15T15:18:59.136-08:00] [oam_server1] [ERROR] [FEDSTS-12078]
[oracle.security.fed.controller.library.api.FedEngineInstance] [tid:
WebContainer : 5] [ecid: disabled,0] [APP: oam_server_11.1.2.0.0] Library
Exception: {0}[[
oracle.security.fed.controller.library.LibraryException:
oracle.security.fed.controller.frontend.action.exceptions.ResponseHandlerExcep
tion: oracle.security.fed.util.http.HttpException:
javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.j: PKIX path building
failed: java.security.cert.CertPathBuilderException: PKIXCertPathBuilderImpl
could not build a valid CertPath.; internal cause is:
        java.security.cert.CertPathValidatorException: The certificate issued
by CN=XXX Root, OU="XXX, Inc.", O=XXX Corporation, C=US is not trusted;
...
```

This error is due to missing Yahoo/Google SSL certificates.

Solution

You need to import the Yahoo/Google SSL certificates into the IBM JSSE Trusted keystore.

First obtain the SSL certificates.

1. Using the Firefox browser, go to the https URL that is being accessed.
2. After viewing the page, right click on the page, then view page info, then details, then view certificate, then details tab.
3. Click export, then save.

Next, import the certificates into the keystore using the instructions provided in the following IBM Technote:

```
http://www-01.ibm.com/support/docview.wss?uid=swg21588087
```

Note: When executing the `keytool` command in Step 6 of the Technote:

- The alias is whatever string you want to use to reference that certificate afterwards.
- If you are not sure which `cacerts` to use, import the certificates to all the `cacerts` keystores.

Note: You may need to download Equifax certification from this URL:

`http://www.geotrust.com/resources/root-certificates/index.html`

Under Root Certificates, download Root1 - Equifax Secure Certificate Authority (.pem file).

Import this certificate using the steps described above.

12.2.2 Controlled-Push Policy Distribution Fails on Oracle Entitlements Server Administration Server

In an Oracle Entitlements Server on IBM WebSphere environment, controlled-push policy distribution fails when the parameter `oracle.security.jps.config` is not configured. The `oracle.security.jps.config` parameter is configured to be the location of the `jps-config.xml` file. If this setting is missing, then policy distribution may fail in an IBM WebSphere environment. The configuration parameter is required for the policy distribution to succeed.

12.2.3 Shell Syntax Error Seen When Configuring Fusion Middleware Products on IBM Websphere Application Server on Solaris SPARC64 5.10 Machines

When you run the *ORACLE_HOME*`/common/bin/wsadmin.sh` script on Solaris Sparc64 5.10 machines, to configure Fusion Middleware products in a cell on IBM Websphere Application Server, the following error is displayed:

```
./wsadmin.sh: test: argument expected
```

Workaround:

Replace the following line in the *ORACLE_HOME*`/common/bin/setWsadminEnv.sh` file

```
if [ ! $WSADMIN_SCRIPT_LIBRARIES ]; then
```

with

```
if [ ! "${WSADMIN_SCRIPT_LIBRARIES}" ]; then
```

After making this change, re-run the *ORACLE_HOME*`/common/bin/wsadmin.sh` script to complete the configuration.

12.2.4 Error Displayed When Accessing DMS Spy for Oracle Access Manager on IBM Websphere

If you have not configured an external LDAP such as OID or OVD, and you try accessing DMS Spy servlet for Oracle Access Manager on IBM Websphere, the following error is displayed:

```
Error 403: AuthorizationFailed
```

If you have not created a user in the external LDAP with Admin roles, then the `wsadmin` user is not allowed to log in to DMS Spy by default. You must manually associate the `wasadmin` user with Admin roles to be able to log in.

Workaround:

Complete the following steps:

1. Log in to the IBM Console.
2. On the left pane, go to **Applications** > **Application Types** > **WebSphere enterprise applications**.
3. On the right pane, click on **Dmgr DMS Application_11.1.1.1.0**.
4. Click on **Security role to user/group mapping**.
5. Select **Admin** role and click on **Map Users...** button.
6. Type `wasadmin` in the search string and click on **Search** button.
7. Select **wasadmin** in the **Available** box and click on **-->** arrow.
8. Click **OK** to return to the previous page.
9. Click **OK** again.
10. Click **Save directly to the master configuration**.
11. Start **Dmgr DMS Application_11.1.1.1.0**.
12. Repeat the above step for **DMS Application_11.1.1.1.0**

12.2.5 Oracle Identity Manager Server Configuration on IBM WebSphere Fails If Sun JDK is Used During Installation

If you provide a Sun JDK as the value for the `-jreLoc` parameter when installing Oracle Identity and Access Management components on IBM WebSphere, the installation is successful. However, when you try to configure Oracle Identity Manager Server, Design Console, and Remote Manager using the Oracle Universal Installer Configuration Assistant, the configuration fails.

Workaround:

1. Open the `orapram.ini` file located in the *`Oracle_Home`*`/oui` directory.
2. Search for `JRE_LOCATION`.
3. Change the value of the `JRE_LOCATION` to point to an IBM JDK.
4. Save the `orapram.ini` file.
5. Start the Oracle Universal Installer Configuration Assistant by running the `config.sh` file (on UNIX) or `config.bat` file (on Windows), located in the *`OIM_HOME`*`/bin` directory.

12.2.6 Error Generated When Extending an OAAM WebSphere Cell to Include OIM Template

When you run the `was_config` command to extend an Oracle Adaptive Access Manager cell to include the Oracle Identity Manager template, you may see the following warning:

```
Conflict detected
CFGFWK -42001: The following duplicate elements exists in a configuration,
discarding new elements from a incomming template
```

You can safely ignore this error message.

12.2.7 Configuration Fails When Performing Silent Installation of Identity and Access Management Components on Solaris Sparc64 with WebSphere

If you are performing a silent installation of Identity and Access Management components on Solaris Sparc64 with WebSphere, then the configuration fails with the following error:

```
Java HotSpot(TM) 64-Bit Server VM warning: Exception java.lang.OutOfMemoryError
occurred dispatching signal SIGTERM to handler-the VM may need to be forcibly
terminated
```

Workaround:

To avoid this issue, add `-javaoption "-XX:MaxPermSize=512m"` in the `wsadmin.sh` command, as shown below:

```
IDM_HOME/common/bin/wsadmin.sh -f config_soa.py -profileName Dmgr01 -javaoption
"-Doracle.cie.log=PATH/cielogs/config_soa_cie_debug.log
-Doracle.cie.log.priority=debug" -javaoption "-XX:MaxPermSize=512m"
```

12.2.8 Configuring Database Security Store Fails When the -D Path Contains "\r"

When you configure the Database Security Store using the `configureSecurityStoreWas.py` script on Windows operating systems, the configuration fails if the path specified with the `-d` parameter contains `\r`.

12.2.9 New IDS Profile Requires OES Server Restart

After adding an IDS profile and binding an application to the profile, you must restart the OES server for the new profile to function properly; otherwise, when you perform user/group searches on the bound application in APM, an error occurs and no search results are returned. The workaround is only required on IBM Websphere.

12.2.10 Oracle Identity Manager Silent Installation Fails Without the -force Option

On a bare OS machine that does not have the libXext.so files, if you run the `runInstaller` command by setting the DISPLAY variable and do not use the `-force` option with the command, then the command fails with an error. To avoid this issue, perform any one of the following:

- Do not set the DISPLAY variable, or remove the DISPLAY variable setting, as shown:

  ```
  unsetenv DISPLAY
  ```

- Run the `runInstaller` command with the `headless` option set to `true`, as follows:

  ```
  ./runIsntaller -J-Djava.awt.headless=true OTHER_ARGUMENTS
  ```

12.2.11 Prerequisite Check Fails in Oracle Identity Manager Silent Installation

While silently installing Oracle Identity Manager on a bare OS machine without the X libraries, the installation completes successfully, bug the prerequisite check fails with the following error message:

```
Expected result: One of
oracle-6,oracle-5.6,enterprise-5.4,enterprise-4,enterprise-5,redhat-6.1,redhat
-6,redhat-5.4,redhat-4,redhat-5,SuSE-10,SuSE-11
Actual Result: oracle-Oracle
```

```
Check complete. The overall result of this check is: Failed
```

To workaround this issue, install lsb_release rpm or pass the `-ignoreSysPrereqs` parameter with the `runInstaller` command.

12.2.12 The wsadmin Script Throws MissingResourceException

While running the wsadmin scripts for silent configuration for cell, the following exception is logged:

```
java.util.MissingResourceException: Can't find resource for bundle
java.util.PropertyResourceBundle, key _shortDescription
        at java.util.ResourceBundle.getObject(ResourceBundle.java:421)
        at java.util.ResourceBundle.getString(ResourceBundle.java:435)
        at com.oracle.cie.domain.script.help.Help.getHelpTopic(Help.java:561)
```

This is benign exception and can be ignored.

12.3 Upgrade Issues and Workarounds

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

- Section 12.3.1, "Errors Displayed When Running Patch Set Assistant on Solaris 10"
- Section 12.3.2, "Some Approval Policies Not Deleted After Upgrade"
- Section 12.3.3, "Exception When Upgrading Oracle Identity Manager Middle Tier"

12.3.1 Errors Displayed When Running Patch Set Assistant on Solaris 10

On Solaris 10 machines, when you run the Patch Set Assistant for patching Oracle Identity and Access Management on WebSphere application server, the following error is displayed:

```
WAS_HOME=<PATH to WAS_HOME>: is not an identifier
```

Workaround:

Before running the Patch Set Assistant on Solaris 10 machines, you must download and apply the patch number 16270302 to the *IAM_ORACLE_HOME* directory.

To download the patch, do the following:

1. Log in to My Oracle Support.
2. Click **Patches & Updates**.
3. Select **Patch name or Number**.
4. Enter the patch number.
5. Click **Search**.
6. Download and install the patch.

The patching instructions are provided in the `README.txt` file that is provided with the patch.

12.3.2 Some Approval Policies Not Deleted After Upgrade

In an Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) deployment on IBM WebSphere Application Server that has been upgraded from Release 9.x, some approval policies are not deleted.

To delete the policies, manually run the following SQL script:

```
DECLARE

 BEGIN

 DELETE FROM REQUEST_APPROVAL_POLICIES
 WHERE
 RAP_POLICY_NAME in (
 'AssignRolesWithCallbackRL',
 'AssignRolesWithCallbackOL',
 'CreateRoleWithCallbackRL',
 'CreateUserWithCallbackRL',
 'CreateUserWithCallbackOL',
 'DeleteRoleWithCallbackRL',
 'DeleteUserWithCallbackRL',
 'DeleteUserWithCallbackOL',
 'DisableUserWithCallbackOL',
 'DisableUserWithCallbackRL',
 'EnableUserWithCallbackRL',
 'EnableUserWithCallbackOL',
 'ModifyRoleWithCallbackRL',
 'ModifyUserWithCallbackRL',
 'ModifyUserWithCallbackOL',
 'RemovefromRolesWithCallbackRL',
 'RemovefromRolesWithCallbackOL');

 COMMIT;
 END;
 /
```

12.3.3 Exception When Upgrading Oracle Identity Manager Middle Tier

This issue occurs when you upgrade Oracle Identity Manager 9.1.x.x to 11.1.2.2.0. The following exception is displayed when you upgrade Oracle Identity Manager middle tier:

```
Error Code: 900
Call: EXECUTE PROCEDURE OIM_RECOMPILE_DB_OBJECTS()
Query: DataModifyQuery()
Dec 16, 2013 10:15:39 PM com.thortech.util.logging.Logger info
INFO: Result Size = 1 PACKAGE STATUS = VALID
Dec 16, 2013 10:15:39 PM com.thortech.util.logging.Logger info
INFO: Recompiling packages - RDBMS
[EL Warning]: 2013-12-16 22:15:39.957--ClientSession(476657190)--Exception
[EclipseLink-4002] (Eclipse Persistence Services - 2.3.1.v20111018-r10243):
org.eclipse.persistence.exceptions.DatabaseException
Internal Exception: java.sql.SQLSyntaxErrorException: ORA-00900: invalid SQL
statement
```

This is a benign exception and can be ignored.

12.4 Documentation Errata

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

12.4.1 Online Help for IBM WebSphere Options in the Oracle Identity Manager Configuration Assistant

When using the Oracle Identity Manager Configuration Assistant, the online help for the configuration screens does not describe the IBM WebSphere-specific options. For more information about the IBM WebSphere options, see "Configuring Oracle Identity Manager for Single-Node Setup" in the chapter, "Managing Oracle Identity Manager on IBM WebSphere" in the *Oracle Fusion Middleware Third-Party Application Server Guide for Oracle Identity and Access Management*.

13

High Availability and Enterprise Deployment

This chapter describes issues associated with Oracle Fusion Middleware high availability and enterprise deployment. It includes the following topics:

- "Configuration Issues and Workarounds"
- "New Topic for Configuring High Availability for Identity and Access Management Components Chapter"

13.1 Configuration Issues and Workarounds

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

- "Log in to Authorization Policy Manager Fails"
- "NullPointerException Occurs and Policy Does Not Save When OAAM Server Fails Over"
- "NullPointerException Occurs and Transaction Does Not Save When OAAM Server Fails Over"

13.1.1 Log in to Authorization Policy Manager Fails

If you have upgraded the Oracle Entitlements Server (OES) Administration Server from version 11g R2 PS1 to 11g R2 PS2 in a high availability cluster environment and you are in the process of configuring high availability, you cannot log into Authorization Policy Manager (APM). When you start the APM Administration Server and managed servers then try to log into the APM console, the system returns the following exception:

```
javax.el.PropertyNotFoundException The class
'oracle.security.apm.ui.bean.ApmMainManagedBean' does not have the property
'roleTemplateEnabled'
```

To log into APM, you must manually redeploy APM in the Administration Console from IDM_HOME.

13.1.2 NullPointerException Occurs and Policy Does Not Save When OAAM Server Fails Over

If you are creating a policy in the Administration Console and one OAAM Server is down and failover occurs, a NullPointerException opens when you click **Apply**. The policy does not save successfully.

To resolve this issue, open the Create Policy page, enter the settings you had entered previously, and click **Apply**.

13.1.3 NullPointerException Occurs and Transaction Does Not Save When OAAM Server Fails Over

If you are creating a transaction in the Administration Console and the OAAM Server is down and failover occurs, a NullPointerException opens when you click **Apply**. The transaction does not save successfully.

To resolve this issue, open the Create Transaction page, enter the settings you had entered previously, and click **Apply**.

13.2 Documentation Errata

This section contains Documentation Errata for the Oracle Fusion Middleware High Availability Guide.

13.2.1 New Topic for Configuring High Availability for Identity and Access Management Components Chapter

The following topic should be section 9.1.3.16 in the "Configuring High Availability for Identity and Access Management Components" chapter of the *Oracle Fusion Middleware High Availability Guide*. This topic does not replace the existing section 9.1.3.1.6, but precedes it.

Updating the SOA Config RMI URL for Identity Manager

To update the SOA Config RMI URL for Identity Manager:

1. Log in to Enterprise Manager.
2. Select **Farm_IDMDomain –> Identity and Access –> OIM –> oim(11.1.1.2.0)**
3. Select **System MBean Browser** from the menu or right click to select it.
4. Select **Application defined Mbeans –> oracle.iam –> Server: wls_oim1 –> Application: oim –> XML Config –> Config —> XMLConfig.SOAConfig –> SOAConfig**
5. Change **SOA Config RMI URL** to: `cluster:t3://soa_cluster`
6. Click **Apply**.

14

Platform-Specific Issues and Workarounds

This chapter describes issues associated with the installation, configuration, deployment, and patching process of Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) on porting platforms. It includes the following sections:

- Section 14.1, "Installation Issues and Workarounds"
- Section 14.2, "Configuration Issues and Workarounds"
- Section 14.3, "Deployment Issues and Workarounds"

14.1 Installation Issues and Workarounds

At this point, there are no installation issues reported on porting platforms.

14.2 Configuration Issues and Workarounds

At this point, there are no configuration issues reported on porting platforms.

14.3 Deployment Issues and Workarounds

This section describes deployment issues and their workarounds on porting platforms. It includes the following topics:

- Section 14.3.1, "Errors Displayed When Deploying Oracle Identity and Access Management on HP Itanium64"
- Section 14.3.2, "Identity and Access Management Deployment Fails During Configuration Phase with Out of Memory Error on IBM AIX"
- Section 14.3.3, "Identity and Access Management Deployment Fails During Preconfigure Phase on IBM AIX"

14.3.1 Errors Displayed When Deploying Oracle Identity and Access Management on HP Itanium64

When you try to deploy Oracle Identity and Access Management on HP Itanium 64-bit platform, using the `iamDeploymentWizard.sh` script, the following errors are displayed:

```
uname: illegal option -- p
usage: uname [-amnrsvil] [-S nodename]
./iamDeploymentWizard.sh[353]: test: Specify a parameter with this command.
./iamDeploymentWizard.sh[353]: test: Specify a parameter with this command.
```

The above errors are also displayed when you run the `runIAMDeployment.sh` script.

Workaround:

These errors are harmless and can be safely ignored.

14.3.2 Identity and Access Management Deployment Fails During Configuration Phase with Out of Memory Error on IBM AIX

When you deploy Identity and Access Management on AIX, the Administration Server log throws out of memory errors, and the deployment fails in the configure phase for IAMAccessDomain. The following errors are displayed:

```
[AdminServer] [ERROR] [] [Coherence] [tid: Logger@9264948 3.7.1.1] [userId:
<anonymous>] [ecid: 0000K8m1Gl_CKuP5IfDCif1IUqMD000003,1:23800] [APP:
oam_admin#11.1.2.0.0]
Oracle Coherence GE 3.7.1.1
<Error>(thread=DistributedCache:DistributionCache, member=1): [[
java.lang.OutOfMemoryError: Java heap space
```

Workaround:

Set the environment variable `USER_MEM_ARGS` as shown below, and restart the Identity and Access Management Deployment.

```
export USER_MEM_ARGS="-Xms256m -Xmx1536m"
```

14.3.3 Identity and Access Management Deployment Fails During Preconfigure Phase on IBM AIX

During Identity and Access Management Deployment on IBM AIX on POWER Systems (64-bit), the preconfigure phase fails.

The `runIAMDeployment-preconfigure.log` file contains the following error:

```
Error executing /bin/sh /bin/ps guwww | grep NodeManager:
Exit Code = 1!DETAIL=Error executing /bin/sh /bin/ps guwww | grep
NodeManager:
.
Exit Code = 1
```

Workaround:

Before you start Identity and Access Management Deployment, complete the following tasks:

1. Open the command-line interface.
2. Run the following command:

   ```
   * sh -c 'echo NodeManager >/dev/null; for x in 1..5; do sleep 86400; done' &
   ```

3. When the deployment is complete, stop the command.

15

Deployment Issues and Workarounds

This chapter describes issues associated with Oracle Identity and Access Management Deployment. It includes the following topics:

15.1 Fields Not Defaulted To Blank On Unchecking Configure Virtual Hosts Option

When creating a deployment response file, if you select the **Configure Virtual Hosts** option on the Configure Virtual Hosts screen, enter values for the Virtual Host Name fields, and then uncheck the **Configure Virtual Hosts** option, the following behavior is noticed:

In an idle situation, when you uncheck the **Configure Virtual Hosts** option, then the values that you had entered for the Virtual Host Names should be removed from the screen, and these values should not get captured in the deployment response file. But this does not happen. The fields are not emptied when the Configure Virtual Hosts option is unchecked, and the values get captured in the deployment response file. This may result in the deployment failure.

Workaround:

You must manually delete the values that you had entered for the Virtual Host Name fields if you uncheck the **Configure Virtual Hosts** option.

15.2 Oracle Identity and Access Management Deployment Fails During Preconfiguration Phase on HPIA64

When you try to perform Deployment on a HPIA64 platform using the Oracle Identity and Access Management 11g Release 2 (11.1.2.2) Repository, it fails with an error during the preconfiguration phase. You might see the following error in the log:

```
WLSTException: Could not connect to nodemanager
```

To resolve the issue, proceed as follows:

1. Download Patch 18549017.
2. Set the `OPATCH_JRE_MEMORY_OPTIONS` environment variable as follows:

```
setenv OPATCH_JRE_MEMORY_OPTIONS "-d64 -mx512m -XX:MaxPermSize=256m"
```

3. Apply the patch by following the instructions in the patch `README.txt`.
4. Download the latest 11.1.2.2.0 WebGate installer from the download site listed in the Oracle Identity and Access Management Download, Installation, and Configuration ReadMe 11g Release 2 (11.1.2.2), at: http://docs.oracle.com/cd/E23104_01/download_readme.htm/download_readme_idmr2.htm
5. Extract the contents of the downloaded zip file and use them to replace the existing WebGate installer, at `installers/webgate` within the Repository.
6. Begin the Deployment process again.

15.3 Additional Documentation

For up-to-date information related to the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*, see Note: 1662923.1: Updates for Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0). This document is available on My Oracle Support at https://support.oracle.com.