Oracle® Fusion Middleware

Identity Management Release Notes

11*g* Release 2 (11.1.2.1)

E39887-18

February 2015

Oracle Fusion Middleware Identity Management Release Notes, 11*g* Release 2 (11.1.2.1)

E39887-18

Contents

3 Upgrade, Migration, and Patching Issues for Oracle Identity and Access Management

4 Oracle Fusion Middleware Administration

5 Oracle Access Management

6 Oracle Entitlements Server

7 Oracle Adaptive Access Manager

8 Oracle Privileged Account Manager

11 Oracle Identity Management Integration

12 Oracle Fusion Middleware on IBM WebSphere

Preface

This preface includes the following sections:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions

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 (11.1.2.1). It includes the following topics:

- Section 1.1, "Latest Release Information,"
- Section 1.2, "Purpose of this Document,"
- Section 1.3, "System Requirements and Specifications,"
- Section 1.4, "Certification Information,"
- Section 1.5, "Downloading and Applying Required Patches,"
- Section 1.6, "Licensing Information,"

1.1 Latest Release Information

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

http://www.oracle.com/technetwork/indexes/documentation/index.html

1.2 Purpose of this Document

This document contains the release information for Oracle Fusion Middleware 11g Release 2 (11.1.2.1). 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:

- Section 1.4.1, "Where to Find Oracle Fusion Middleware Certification Information,"
- Section 1.4.2, "Certification Exceptions,"
- Section 1.4.3, "JMSDELIVERYCOUNT Is Not Set Properly,"
- Section 1.4.4, "Viewer Plugin Required On Safari 4 To View Raw XML Source,"

1.4.1 Where to Find Oracle Fusion Middleware Certification Information

The latest certification information for Oracle Fusion Middleware 11g Release 2 (11.1.2.1) 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 (11.1.2.1) components, see the Release Notes for the specific Oracle Fusion Middleware 11g Release 2 (11.1.2.1) component.

This section contains the following topics:

- Section 1.4.2.1, "Certification Information for Oracle Fusion Middleware 11g R2 with Oracle Database 11.2.0.1,"
- Section 1.4.2.2, "Excel Export Issue on Windows Vista Client,"
- Section 1.4.2.3, "Oracle Forms and Oracle Reports 11g Installer Issues In Windows Vista and Windows XP,"
- Section 1.4.2.4, "Restrictions on Specific Browsers,"

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 (11.1.2.1), 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 SOA Suite - Oracle BPM Worklist application	9901600	Unless you apply this patch, errors appear in the log files when you access the Event Driven page in the Oracle Business Process Management Worklist application.
Oracle XDK for Java	10337609	This patch fixes the following issue. If you use the XSU utility to insert some data into the database, and the database connection had the connection property called `oracle.jdbc.J2EE13Compliant` set to "true", and the target column was some kind of numeric column, then it is possible for the insert to fail with a the following error: `java.lang.NumberFormatException`
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 Access Manager	14101542	This patch corrects an account locking incompatibility with Oracle Identity Manager.
Oracle Enterprise Manager Fusion Middleware Control	17375780	This patch fixes the error: Host and Port is Not Right on OIM Cluster Home Page

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 (11.1.2.1.0). 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"

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.

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.

2.2 Installation Issues and Workarounds

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

- Section 2.2.1, "Error when Installing Oracle Identity Manager Design Console"
- Section 2.2.2, "Mandatory Patches Required for Installing Oracle Identity Manager"
- Section 2.2.3, "JPS Keystore Service Initialization Failure in Join Domain Scenario for Oracle Access Management Domain"

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 late-breaking changes and additional patch requirements, see My Oracle Support document ID 1536894.1.

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.

Table 2–1 Patches Required to Fix Specific Issues with Oracle Identity Manager 11gR2 (11.1.2.1.0)

Oracle Fusion Middleware Product or Component	Patch Number	When to Apply?	Description
Oracle SOA Suite	16702086	After installing Oracle SOA Suite	This is a mandatory Oracle SOA Suite Bundle Patch 11.1.1.6.7 patch. Follow the `README.txt` file for patching instructions.
Oracle SOA Suite	17988119, 18486891, 13973356	After installing Oracle SOA Suite Bundle Patch 11.1.1.6.7	These mandatory Oracle SOA Suite patches need to be applied after Oracle SOA Suite has been upgraded to Bundle Patch 11.1.1.6.7 using patch 16702086. Choose the 11.1.1.6.7 version of these patches, and follow the `README.txt` file for patching instructions.
Oracle User Messaging Service	16366204	After installing Oracle SOA Suite	This is an Oracle User Messaging Service (UMS) patch. Choose the 11.1.1.6.0 version of this patch, and follow the `README.txt` file for patching instructions.
Oracle WebCenter Portal	16472592	After installing Oracle Identity Manager	This is an Oracle WebCenter Portal patch. Follow the `README.txt` file for patching instructions.
Oracle Application Development Framework	19976022	After installing Oracle Identity and Access Management	This is an Oracle Application Development Framework (ADF) patch. Follow the `README.txt` file for patching instructions.
Oracle Platform Security Services	16400771	After installing Oracle Identity Manager	This is an Oracle Platform Security Services (OPSS) patch. Follow the `README.txt` file for patching instructions.
Oracle Virtual Directory - Identity Virtualization Library (libOVD)	18919213	After installing Oracle Identity and Access Management	This is a mandatory patch if you are using Identity Virtualization Library (libOVD). Note that this patch is classified as an Oracle Virtual Directory patch. Download the 11.1.1.6.0 version of this patch, and follow the `README.txt` file for patching instructions.
Oracle Virtual Directory - Oracle Directory Server Enterprise Edition	14016801	After installing Oracle Directory Server Enterprise Edition	This is a mandatory patch if you are using Oracle Directory Server Enterprise Edition. Note that this patch is classified as an Oracle Virtual Directory patch. Download the 11.1.1.6.0 version of this patch, and follow the `README.txt` file for patching instructions.

Table 2–1 (Cont.) Patches Required to Fix Specific Issues with Oracle Identity Manager 11gR2 (11.1.2.1.0)

Oracle Fusion Middleware Product or Component	Patch Number	When to Apply?	Description
Oracle Unified Directory	18489893	After installing Oracle Unified Directory	This is a mandatory patch if you are using Oracle Unified Directory. Download the version of this patch that corresponds with the version of Oracle Unified Directory you installed. Follow the `README.txt` file for patching instructions.
Oracle Access Manager	16513008	After installing Oracle Identity and Access Management	You must apply this patch if you plan to integrate Oracle Identity Manager with Oracle Access Manager. Follow the `README.txt` file for patching instructions.
Oracle Business Intelligence Publisher	14630670	After installing Oracle Identity Manager	This is an Oracle Business Intelligence Publisher patch. Follow the `README.txt` file for patching instructions.
Oracle IDM Tools	17008132	After installing Oracle Identity and Access Management	This is an Oracle IDM Tools patch. Follow the `README.txt` file for patching instructions.
Oracle Business Intelligence Publisher	14088000	After installing Oracle Identity Manager	This is an Oracle Business Intelligence Publisher patch. Follow the `README.txt` file for patching instructions.
Enterprise Manager for Fusion Middleware	17375780	After installing Oracle Identity and Access Management	This is an Enterprise Manager patch. Follow the `README.txt` file for patching instructions.

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.

2.3 Configuration Issues and Workarounds

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

- Section 2.3.6, "Security Store Join Fails on Windows"
- Section 2.3.7, "Weblogic Server Configuration Wizard does not support JDK6 on AIX7"
- Section 2.3.8, "Access Policy Manager Deployments Do Not Target Administration Server in Cluster Scenario"
- Section 2.3.9, "Requests Fail with ClassCastException"
- Section 2.3.10, "Modify PKCS11-Solaris Security Provider Before Running the `configSecurityStore.py` Command When Using Sun JDK 1.7"
- Section 2.3.11, "Server Startup Failure"

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 11g Release 1 (10.3.6) or Oracle WebLogic Server 11g Release 1 (10.3.5)
- Oracle SOA Suite 11.1.1.6.0 (Oracle Identity Manager Users Only)
- Oracle Identity and Access Management 11g Release 2 (11.1.2)

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. Configure domain
2. Configure the `Configsecuritystore`
3. Copy `jps-config.xml` file to `jps-config.xml_old` for recovery and reference
4. 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.

3

Upgrade, Migration, and Patching Issues for Oracle Identity and Access Management

This chapter describes issues associated with the upgrade and migration process of Oracle Identity and Access Management 11g Release 2 (11.1.2.1.0). It includes the following sections:

- Section 3.1, "Upgrade Issues"
- Section 3.2, "Migration Issues"
- Section 3.3, "Patching Issues"

3.1 Upgrade Issues

This section describes issues related to upgrading the following components:

- Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0)
- Oracle Access Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0)
- Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.1.0)
- Oracle Identity Navigator 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Navigator 11*g* Release 2 (11.1.2.1.0)
- Oracle Entitlements Server 11*g* Release 1 (11.1.1.5.0) to Oracle Entitlements Server 11*g* Release 2 (11.1.2.1.0)
- Oracle Identity Manager 9.x to Oracle Identity Manager 11*g* 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 General 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"

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 (11.1.2.1.0). 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.

3.2 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 (11.1.2.1.0)
- Migrating Oracle Adaptive Access Manager 10*g* to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.1.0)
- Migrating Oracle Single Sign-On 10*g* to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0)
- Migrating Sun OpenSSO Enterprise 8.0 to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0)
- Migrating Sun Java System Access Manager 7.1 to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0)
- Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0)
- Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0)
- Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0)

3.2.1 General Issues and Workarounds

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

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

- Section 3.2.1.2, "Server Logs and Assessment Report for Certain Scenarios Show Only English Messages"
- Section 3.2.1.3, "Registering Policy Agent 2.2 Using RREG Fails Due to Unavailability of Agent Template"
- Section 3.2.1.4, "Oracle Access Management 11g Release 2 (11.1.2.0.0) Coexistence, Upgrade, and Migration Supplement"

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 (11.1.2.1.0). 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 (11.1.2.1.0):

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

Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.1.0) discusses how to upgrade or migrate various Single Sign-On and Access Management environments to Oracle Access Management 11g Release 2 (11.1.2.0.0). 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

3.3 Patching Issues

This section describes general issues and workarounds related to applying the Oracle Identity and Access Management 11g Release 2 (11.1.2.1.0) patch to an existing Oracle Identity and Access Management 11g Release 2 (11.1.2.0.0) environment. It includes the following topics:

3.3.1 Updating System Mbean Configuration

In Oracle Access Manager Release 2 (11.1.2.1.0), 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 11.1.2.1.0 patch, you must run the following WLST commands to complete the patching process for OAM:

1. After applying the 11.1.2.1.0 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 11.1.2.1.0 Mbean XML files are copied to the following locations:

   `<DOMAIN_HOME>/config/fmwconfig/mbeans`

   `<DOMAIN_HOME>/config/fmwconfig`

3.3.2 SOA Email Notification Does Not Work

In an Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) deployment that has been upgraded from 11*g* Release 2 (11.1.2.1), SOA email notification does not work.

To workaround this issue:

1. Apply patch 16366204.
2. Start Admin and SOA Server.
3. 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**.

4. Restart the SOA Server.

3.3.3 AD User Management Connector Issues

After you have applied the Oracle Identity and Access Management 11g Release 2 (11.1.2.1.0) 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.

3.3.4 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 11.1.2.1.0 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?.
```

3.3.5 Delete WebLogic Server TMP Directories

After you have applied the Oracle Identity and Access Management 11g Release 2 (11.1.2.1.0) 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:

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

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

3.3.6 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 11.1.2.1.0, 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".

3.3.7 Metadata Services (MDS) Patching Fails if OIM Server is Started Before Middle Tier Upgrade

When you are patching from OIM 11*g* Release 2 (11.1.2.0.0) to OIM 11*g* Release 2 (11.1.2.1.0), Metadata Services (MDS) patching fails if the Oracle Identity Manager Server is started before the Middle Tier upgrade.

The following exception is seen in the MDS report *`ORACLE_HOME`*`/server/logs/`*`MDS_REPORT_DIRECTORY`*`/MDSReport.html`, if you start the OIM Managed Server after the binary upgrade or schema upgrade, and before the middle tier upgrade:

```
java.lang.NullPointerException at
oracle.iam.oimupgrade.mdstransferlisteners.util.CommonUtil.readmetadataMergeCl
assMap(CommonUtil.java:369) at
oracle.iam.oimupgrade.mdstransferlisteners.util.ListenerUtil.postOperation(Lis
tenerUtil.java:148) at
oracle.iam.oimupgrade.mdstransferlisteners.RequestTransferListener.postOperati
on(RequestTransferListener.java:61) at
oracle.mds.internal.transfer.InternalMDSTransfer$1.run(InternalMDSTransfer.jav
a:2183)
```

Workaround:

The workaround for this issue is to apply MDS patching after you complete the Oracle Identity Manager upgrade process. To do this, complete the following steps:

1. Launch the WebLogic Scripting Tool (WLST) by running the following command from the location *`MW_HOME`*`/oracle_common/common/bin`:

   On UNIX: `./wlst.sh`

   On Windows: `wlst.cmd`

2. Connect to the WebLogic Administration Server by running the following command:

```
connect('wls_admin_username','wls_admin_password','t3://hostname:port')
```

In this command,

- *wls_admin_username* is the username of the WebLogic Administration Server.
- *wls_admin_password* is the password of the WebLogic Administration Server.
- *hostname* is the machine where WebLogic Administration Server ia running.
- *port* is the Administration Server port

3. Import the MAR with forced MDS Patching using the following command:

   ```
   importMAR('OIMMetadata','OIM_Managed_Server_Name','true')
   ```

   In this command, *OIM_Managed_Server_Name* is the name of the OIM Managed Server.

   For more information about using importMAR command, see "importMAR" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

3.3.8 Middle Tier Upgrade Fails When Patching OIM 11.1.2.0.0 to 11.1.2.1.0

This issue occurs when you patch Oracle Identity Manager 11*g* Release 2 (11.1.2.0.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0). Middle tier upgrade fails with the following exception when you patch OIM 11.1.2.0.0 to 11.1.2.1.0:

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

The workaround for this issue is as follows:

1. Open the file `OIMUpgrade.sh` from the location *MW_HOME*`/Oracle_IDM1/server/bin` in text editor.
2. In MDSJARS classpath settings, replace the path *$OIM_HOME*`/server/ext/ucp.jar` with *$MW_HOME*`/oracle_common/modules/oracle.ucp_11.1.0.jar`.
3. Save the file `OIMUpgrade.sh`.
4. Run the middle tier upgrade again.

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 in moving from test to production:

- 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`

- For Oracle Identity Manager, Release 11.1.2.1, note the following when you move your environment:

  - If you are using a different database in the target, update the information in the DATASOURCE configGroup, along with any other information that needs to change.
  - In the SERVER_CONFIG configGroup, when you update the Listen Address property, specify the name of the host containing the Oracle SOA Suite server and the Oracle Identity Manager server. Do not specify `All Local Addresses`.
  - When you are using the pasteConfig script with Oracle Identity Manager, you might encounter the following error:

    ```
    SEVERE : [PLUGIN][OIM] ERROR - CLONE-71000 configuration Failed.
     Exiting configuration due to data validation failure.
    SEVERE : [PLUGIN][OIM] CAUSE - CLONE-71000 [VALIDATION]
    [ERROR]:INST-6109: Unable to connect to the Database with the given
     credentials. Invalid service name
    ```

    To correct the problem, take the following steps:

    a. Update the move plan. In the move plan, for Oracle Identity Manager specific data sources, the value of the property Url might have SID pattern rather than service name pattern. Correct the move plan, using the service name pattern in the URL property of the DataSource configGroup instead of the SID.

       Use the following format:

       ```
       <value>jdbc:oracle:thin:@hostname:13477/servicename</value>
       ```

       For example:

       ```
       <value>jdbc:oracle:thin:@example.com:13477/MySID.example.com</value>
       ```

       Do not use the following formats:

       ```
       <value>jdbc:oracle:thin:@hostname:13477:sid</value>
              <value>jdbc:oracle:thin:@hostname:13477:servicename</value>
       ```

    b. Run the pasteConfig script again.
  - If you are using a different database in the target, update the information in the DATASOURCE configGroup, along with any other information that needs to change.
  - In the SERVER_CONFIG configGroup, when you update the Listen Address property, specify the name of the host containing the Oracle SOA Suite server and the Oracle Identity Manager server.

- If you have a source environment that contains Oracle Identity Manager Release 11.1.2.1, and Oracle SOA Suite, Release 11.1.1.*, you must install the following patch before you run the copyConfig script:

  ```
  Patch14501468
  ```

- The movement scripts do not support moving Oracle Identity Manager *Release 11.1.1.** to another environment, either through the movement scripts or manual steps. In addition, if Oracle Identity Manager *Release 11.1.1.** 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
```

- 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 hostname 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.

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*

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

- Section 4.3.1.1, "Combining All Oracle Homes in a Single Inventory File"
- Section 4.3.1.2, "Correction in Moving Oracle Platform Security Services"
- Section 4.3.1.3, "Correction to Link About Supported Databases for MDS"

4.3.1.1 Combining All Oracle Homes in a Single Inventory File

All Oracle homes in the Middleware home on the source environment must be registered in the same Oracle inventory. If you have installed multiple components under the same Middleware home, but used different Oracle inventory locations, the scripts are not able to detect all of the Oracle homes.

To work around this issue, take the following steps:

1. Create a new oraInst.loc pointing to the inventory to which you want to register, using the following commands:

   ```
   cat oraInst.loc
         inventory_loc=new_oraInst_loc_location
         inst_group=g900
   ```

2. Detach the Oracle Home from its current inventory:

   ```
   cd ORACLE_HOME/oui/bin
         ./detachHome.sh -invPtrLoc ORACLE_HOME/oraInst.loc
   ```

3. Attach the Oracle Home to the new inventory by passing new oraInst.loc created in step 1:

   ```
   ./attachHome.sh -invPtrLoc new_oraInst_loc_location
   ```

   Do this for every Oracle home in the Middleware home.

4. Set the necessary dependencies between Oracle homes if required (for example most Oracle homes depend on oracle_common). The dependencies are required when you uninstall. You can check the existing dependencies from the old inventory by checking the file oraInventory/ContentsXML/inventory.xml. The following shows an example of the file:

   ```
   <?xml version="1.0" standalone="yes" ?>
   <!-- Copyright (c) 1999, 2010, Oracle. All rights reserved. -->
   ```

```
<!-- Do not modify the contents of this file by hand. -->
<VERSION_INFO>
   <SAVED_WITH>11.1.0.9.0</SAVED_WITH>
   <MINIMUM_VER>2.1.0.6.0</MINIMUM_VER>
</VERSION_INFO>
<HOME_LIST>
<HOME NAME="OH339778486" LOC="/scratch/oracle/11gMW/oracle_common" TYPE="O"
IDX="1">
   <REFHOMELIST>
      <REFHOME LOC="/scratch/oracle/11gMW/Oracle_WT1"/>
   </REFHOMELIST>
</HOME>
<HOME NAME="OH299443989" LOC="/scratch/oracle/11gMW/Oracle_WT1" TYPE="O"
IDX="2">
   <DEPHOMELIST>
      <DEPHOME LOC="/scratch/oracle/11gMW/oracle_common"/>
   </DEPHOMELIST>
</HOME>
</HOME_LIST>
<COMPOSITEHOME_LIST>
</COMPOSITEHOME_LIST>
</INVENTORY>
```

5. Run the following command to set up dependencies. Note that this is not mandatory for the movement scripts to work, but is needed when you uninstall.

```
./runInstaller -updateHomeDeps
"HOME_DEPENDENCY_LIST={/scratch/oracle/11gMW/Oracle_WT1:/scratch/oracle/11gMW/
oracle_common}" -invPtrLoc ~/oraInst.loc
```

4.3.1.2 Correction in Moving Oracle Platform Security Services

The procedure for moving Oracle Platform Security Services to a new target environment the data is in a database is missing a step. The complete procedure is:

1. Set the environment variables and change to the Oracle home directory:

```
setenv ORACLE_HOME ORACLE_HOME
setenv ORACLE_SID ORACLE_SID
cd $ORACLE_HOME/bin
```

2. Export the data from the source schema:

```
expdp "sys/password@connect_id as sysdba"
           DIRECTORY=DATA_PUMP_DIR SCHEMAS=OPSS_schema_name
           DUMPFILE=export.dmp PARALLEL=2 LOGFILE=export.log
```

3. Create a directory, for example DATA_PUMP_DIR2 and copy the .dmp file to that directory in the target environment.
4. Connect to the database as a user with the sysdba role and execute the following command:

```
CREATE DIRECTORY DATA_PUMP_DIR2 as
'/scratch/oracle/product/11.2.0/dbhome_1/opss_dump';
```

5. Import the data into the target schema:

```
impdp "sys/password@connect_id as sysdba"
          DIRECTORY=DATA_PUMP_DIR2 DUMPFILE=export.dmp
          PARALLEL=2 LOGFILE=import.log
          remap_schema=test_env_schema_name:prod_env_schema_name
          remap_tablespace=test_env_tablespace:prod_env_tablespace
```

```
TABLE_EXISTS_ACTION=REPLACE
```

Note that the import command generates "Job "SYS"."SYS_IMPORT_FULL_01" completed with 6 errors." You can ignore the errors.

4.3.1.3 Correction to Link About Supported Databases for MDS

The section "Databases Supported by MDS" in the *Oracle Fusion Middleware Administrator's Guide* contains an incorrect link to*Oracle Fusion Middleware System Requirements and Specifications*. The correct link is:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-requirements-100147.html

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:

- Section 4.3.2.1, "JRockit SDK Not Certified for IDM"
- Section 4.3.2.2, "oam.conf Lines Formatted Incorrectly"

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`

4.3.2.2 oam.conf Lines Formatted Incorrectly

In section 9.2.3.12.1, "Update Oracle HTTP Server Configuration," lines in the example file do not have the correct formatting; they are split between two lines but should be one line.

To fix this issue, replace:

```
oamhost1.mycompany.com:14100,oamhost2.mycompany.com:14100
WebLogicCluster
```

and

```
WebLogicCluster
oamhost1.mycompany.com:14100,oamhost2.mycompany.com:14100
```

with the following line:

```
WebLogicCluster oamhost1.mycompany.com:14100,oamhost2.mycompany.com:14100
```

5

Oracle Access Management

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

- Section 5.1, "General Issues and Workarounds"
- Section 5.2, "Configuration Issues and Workarounds"
- Section 5.3, "Oracle Access Management Console Issues"
- Section 5.4, "Documentation Errata"

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 around specific services. To streamline your experience, only services with a general issue are included. If you do not find a service-related topic (Security Token Service, for example), there are no general issues at this time.

The following topics are included:

- Section 5.1.1, "General Issues and Workarounds: Access Manager"
- Section 5.1.2, "General Issues and Workarounds: Security Token Service"
- Section 5.1.3, "General Issues and Workarounds: Identity Federation"
- Section 5.1.4, "General Issues and Workarounds: Mobile and Social"

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 5.1.1.1, "LDR_PRELOAD64 Flag Required For WebGate Agent With AIX 6.1 & 7.1."
- Section 5.1.1.2, "ASDK Returns Incorrect Version Details."
- Section 5.1.1.3, "Benign Exceptions Observed."
- Section 5.1.1.4, "Can't Use WLST Commands For Federated SSO Password Policy."
- Section 5.1.1.5, "Exception Logged on Accessing Resource."
- Section 5.1.1.6, "Can't Get Static Method UserSession.getSessionAttributes()."

5.1.1.1 LDR_PRELOAD64 Flag Required For WebGate Agent With AIX 6.1 & 7.1

Support for WebGate agents using the Apache 2.2 server on 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
```

5.1.1.2 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`.

5.1.1.3 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)
```

5.1.1.4 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.

5.1.1.5 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
```

5.1.1.6 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.

5.1.1.7 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.

5.1.1.8 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.

5.1.1.9 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.

5.1.1.10 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.

5.1.1.11 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.

5.1.1.12 Running the Custom RSAPlugin.jar

The RSA plugin has been removed as a system plugin. The functionality can still be accessed by installing and using a custom RSA plugin. These steps should be followed to run a custom RSA plug-in, located in <ORACLE_HOME>/oam/custom_plugins/rsa/RSAPlugin.jar.

1. Download the RSA dependent libraries named `authapi.jar` and `cryptoj.jar`.
2. Add the `authapi.jar` and `cryptoj.jar` libraries to <DOMAIN_HOME>/config/fmwconfig/oam/plugin-lib.
3. Get the custom RSAPlugin.jar file from it's directory and import the plugin to add it to the list of custom plugins.
4. Once successfully imported, distribute and activate the plug-in.

   Activation will fail the first time. When it does, restart the server and activate again. After activation, use the plugin to specify the necessary orchestration steps.

5.1.1.13 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.

5.1.1.14 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 '/'.

5.1.1.15 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.

5.1.1.16 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.

5.1.1.17 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
```

5.1.1.18 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.

5.1.1.19 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: Mobile and Social

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

- Section 5.1.4.1, "Mobile and Social Does not Support the Native Android OS Browser"
- Section 5.1.4.2, "Internet Explorer Users Need to Enable Protected Mode"
- Section 5.1.4.3, "Google Language Menu can Cause the Sign-in Page Flow to Display in Multiple Languages"
- Section 5.1.4.4, "The Mobile and Social Settings Pane can be Dragged out of View"

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 an Internet 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.

5.2 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: 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 System Configuration tab, Security Token Service section, go to Issuance Templates.
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: 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:

- Section 5.2.4.1, "Moving Mobile and Social From a Test to Production Environment on IBM WebSphere"
- Section 5.2.4.2, "Steps Required to Localize the Register Page"
- Section 5.2.4.3, "Mobile Clients do not Translate Error Messages Sent by the Server"
- Section 5.2.4.4, "Yahoo Identity Provider Does not Return First Name and Last Name"
- Section 5.2.4.5, "Once Set, Jail Breaking "Max OS Version" Setting Cannot be Empty"
- Section 5.2.4.6, "Additional Configuration Required After Running Test-to-Production Scripts"

5.2.4.1 Moving Mobile and Social From a Test to Production Environment on IBM WebSphere

The following steps describe how to copy Mobile and Social from a test environment to a production environment.

Important: Complete these steps after you finish moving Access Manager from the test environment to the production environment. For more information, see "Moving Access Manager From a Test to Production Environment on IBM WebSphere" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

---

1. Update `oam-config.xml` in the production environment with the `secretKey` value from the test environment.

   a. In the test environment, use a text editor to open `oam-config.xml` in the `fmwconfig` directory and, for object `accessgate-oic`, copy the value of the `secretKey` attribute.

   For example:

```
<Setting Name="accessgate-oic" Type="htf:map">
  <Setting Name="ConfigurationProfile"
Type="xsd:string">DefaultProfile</Setting>
  <Setting Name="aaaTimeoutThreshold" Type="xsd:string">-1</Setting>
...

  <Setting Name="secretKey"
Type="xsd:string">A686408D1020B93EAA8B411EE0137847FD2968D1285A2A37BB0BE0B00
238F50464E9C01EB3E5319AED6D7CAC81BD9FF7</Setting>
```

   b. In the production environment, use a text editor to open `oam-config.xml` in the `fmwconfig` directory and, for object `accessgate-oic`, replace the value of the attribute `secretKey` with the value from the test host.

2. Copy the `idaas.xml`, `oauth.xml`, and `oic_rp.xml` files from the test environment `fmwconfig` directory to the production environment `fmwconfig` directory.

3. In the production environment, edit the host and port information as appropriate in `oic_rp.xml`.

   Search for the name of the test host and replace it with the name of the production host. Verify that the port number is correct for the host URL.

   For example:

```
<SystemConfiguration>
        <hostURL>https://prod123.example.com:14101</hostURL>
```

4. Stop the node manager.

   Synchronize the node and start the node manager.

5. Restart the oam_server1 and OracleAdminServer applications.

5.2.4.2 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. In the Oracle Access Management console, open the Application Profile under Internet Identity Services, 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.

5.2.4.3 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.

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

The Yahoo Internet 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 Internet Identity Provider configuration page opens.
2. Open the **Application User Attribute Vs Internet Identity Provider User Attributes Mapping** section.
3. In the **Attribute Mapping** section, click **Yahoo** to select it in the **Internet Identity Provider** list.
4. Configure the values as follows:
   - Locate **firstname** in the **Application User Attribute** column and in the corresponding **Internet Identity Provider User Attributes** column, choose **nickname**.
   - Locate **lastname** in the **Application User Attribute** column and in the corresponding **Internet Identity Provider User Attributes** column, choose **fullname**.
5. Save the Application Profile.

5.2.4.5 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.

5.2.4.6 Additional Configuration Required After Running Test-to-Production Scripts

When moving Mobile and Social from a test environment to a production environment, complete the following configuration steps on each production machine after running the Test-to-Production scripts:

1. Launch the Oracle Access Management Console.
2. On the **Policy Configuration** tab, choose **Shared Components** > **Authentication Schemes** > **OIC Scheme** and click Open.

   The Authentication Schemes configuration page opens.

   Update the **Challenge Redirect URL** value to point to the production machine, not the test machine, then click **Apply**.

For example: `https://`*production_machine*`:`*port*`/oic_rp/login.jsp`

3. Update the Mobile and Social credential store framework (CSF) entry to point from the test machine to the production machine. To do this, run the following WLST command:

```
createCred(map="OIC_MAP", key=" https://<production machine host>:<production
machine port>/oam/server/dap/cred_submit ", user="="<description>", password="
DCC5332B4069BAB4E016C390432627ED", desc="<description>");
```

   For `password`, use the value from `oam-config.xml`, which is located in the *domain home*`/config/fmwconfig` directory on the production machine. Use the value from the `RPPartner` entry, `TapCipherKey` attribute.

4. In the Oracle Access Management Console, do the following:

   a. Select the **System Configuration** tab.

   b. Choose **Mobile and Social** > **Internet Identity Services**.

   c. In the **Application Profiles** section, select **OAMApplicaton** and click **Edit**. (If using an application profile name other than OAMApplication, edit that instead.)

   d. Update the **Registration URL** field host name and port to point to the production machine.

   Click **Apply**.

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

5.3.1 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 Element 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"

5.4.1.1 Max Session Time Element Description Update

The description of the Max Session Time element in Chapter 14 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

5.4.2 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, "Tomcat Security Module Fails To Load Custom Attribute Retriever Class"
- Section 6.1.2, "Duplicate Entries of Resource Objects"
- Section 6.1.3, "Finding Default Oracle Entitlements Server Security Module Certificates"
- Section 6.1.4, "Entitlements Server Does Not Recover Connection To Database"
- Section 6.1.5, "Policy Simulator Does Not Open Policies Correctly"
- Section 6.1.6, "Starting Oracle Access Manager When Protected by Entitlements Server Throws Exception"
- Section 6.1.7, "Updating the Opatch Tool"
- Section 6.1.8, "Web Service Fails to Start on WebLogic Server Security Module Managed Server"
- Section 6.1.9, "configureSecurityStore.py Fails if env Command Output Includes Empty Line"
- Section 6.1.10, "Security Module Configuration User Interface Contains Garbled Characters for Asian Locale"
- Section 6.1.11, "Authorization Policy Creation Error Message in Administration Console"

6.1.1 Tomcat Security Module Fails To Load Custom Attribute Retriever Class

The Attribute Retriever Interface resides in the JPS JARs which are loaded by the Tomcat "shared" class loader. Thus, JARs that contain your Custom Attribute Retriever Interface implementations should also be loaded by the "shared" class loader or a class loader that has a "shared" class loader for its ancestor. Be sure to put the Custom Attribute Retriever JARs in the proper place based on this scenario.

6.1.2 Duplicate Entries of Resource Objects

This version of Oracle Entitlements Server allows the creation of duplicate Resource entries in Entitlements and Policies.

6.1.3 Finding Default Oracle Entitlements Server Security Module Certificates

The default Oracle Entitlements Server Security Module (client) certificate is stored in `your_oes_sm_folder/oes_sm_instances/your_oes_sm/security/identity.jks` and the trusted Certificate Authority (CA) certificates are stored in `your_oes_sm_folder/oes_sm_instances/your_oes_sm/security/trust.jks`. Both are JKS certificate stores with the passwords set during the creation of the Security Module instance. The password will be encrypted and stored in standard Oracle Wallet (with autologon). The default Oracle Entitlements Server client keys are generated by itself and signed during the enrollment process.

6.1.4 Entitlements Server Does Not Recover Connection To Database

If the Entitlements Server is started when the database hosting the policy store is down, it will not automatically recover once the database is available. Either of the following will rectify this.

1. Set the database for automatic recovery by defining the following properties:
   - Connection Creation Retry Frequency is needed if the database will be down before the Administration Server starts.
   - Test Connections on Reserve is required if the database goes down after a successful Administration Server start.
2. Restart the Administration Server once the database is live.

6.1.5 Policy Simulator Does Not Open Policies Correctly

If multiple Role Mapping Policies or Authorization Policies are returned as a result of running the Policy Simulator, the correct object reference is not passed and thus, they are not opened correctly. You will see this after clicking Check Access and selecting the Application Roles and Mapping Policies tab. To workaround this issue and open policy details, search for the policies using the Advanced Search screen.

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

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

6.1.7 Updating the Opatch Tool

Oracle recommends that all customers be on the latest version of OPatch. Please review My Oracle Support Note 224346.1 *Opatch - Where Can I Find the Latest Version of Opatch?* and follow the instructions to update to the latest version if necessary. For FMW Opatch usage, please refer to the *Oracle Fusion Middleware Patching Guide*.

6.1.8 Web Service Fails to Start on WebLogic Server Security Module Managed Server

If you follow the steps in sections 9.6.2.7, Configuring Oracle Entitlements Server Web Service Security Module on WebLogic High Availability, or 9.6.2.8, Configuring Oracle Entitlements Server WebLogic Security Module High Availability of the *Oracle Fusion Middleware High Availability Guide*, Web Service fails to start on the WebLogic Server Security Module managed server on the second node. A Java runtime exception error occurs due to a permission issue in the weblogic.policy file.

This error occurs because there is no OES permission in weblogic.policy. To resolve this error, add the following lines on OESHOST2 in `MW_HOME/wlserver_10.3/server/lib/weblogic.policy` file:

```
grant codeBase "file:${oes.client.home}/-" {
        permission java.security.AllPermission;
};
```

6.1.9 configureSecurityStore.py Fails if env Command Output Includes Empty Line

When the `env` command is run against `wlst.sh configureSecurityStore.py` with output containing an empty line, the command will fail. For example:

```
LANG=en_US.utf8
GNOME_KEYRING_PID=16766
<empty line>
PYTHONSTARTUP=/etc/pythonstart
```

An exception message similar to the following may be seen:

```
Welcome to WebLogic Server Administration Scripting Shell
.
Type help() for help on available commands
.
Info: Data source is: opss-DBDS
Info: DB JDBC driver: oracle.jdbc.OracleDriver
Info: DB JDBC URL: jdbc:oracle:thin:@hostname.mycompany.com:1521/db10205
Exception in thread "Main Thread" java.lang.NoClassDefFoundError:
oracle/security/jps/internal/tools/configuration/ldap/LdapServiceEnabler
Caused by: java.lang.ClassNotFoundException:
```

To workaround this issue, remove the empty line and run the command again. For example:

```
% unset GNOME_KEYRING_PID
% set GNOME_KEYRING_PID=16766
```

6.1.10 Security Module Configuration User Interface Contains Garbled Characters for Asian Locale

This issue affects the Microsoft Windows platform only. The Security Module Configuration User Interface (SMConfig UI) may contain garbled characters when set to be Asian Locale. This affects Simplified and Traditional Chinese, Japanese and Korean languages.

To workaround this issue, if using another language is acceptable, you can change the user interface language by setting the locale to the VM parameter in `oessmconfig.bat`. For example, to use English in the US locale:

```
setting -Duser.language=en -Duser.country=US
```

6.1.11 Authorization Policy Creation Error Message in Administration Console

When creating an Authorization Policy in the Administration Console, if invalid condition data for certain data types (like DNS) is built using an equals operator (=) the following system message is displayed:

```
application policy -  expression encoding error
```

This error means that the condition was not built correctly therefore the Authorization Policy could not be created. However, this error is difficult to interpret.

To workaround this issue, re-write the condition using a function instead of the equals operator (=). For example, if the condition was written as:

```
DNS_NAME_ONE_AND_
ONLY(['www.mycompany.com','www.mycompany.com'])='www.anothercompany.com'
```

Re-write the conditions as follows:

```
DNS_NAME_ONE_AND_ONLY(['www.mycompany.com','www.mycompany.com'])=DNS_NAME_FROM_
STRI
NG('www.anothercompany.com')
```

6.2 Configuration Issues and Workarounds

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

- Section 6.2.1, "Config Security Store Fails To Create Policy Store Object"
- Section 6.2.2, "Use Absolute Paths While Running configureSecurityStore.py With -m Join"
- Section 6.2.3, "Wrong Type Defined For PIP Service Provider After Adding PIP Attribute"
- Section 6.2.4, "Starting the OES Domain Gives an Error When Using Derby Database as the Policy Store"

6.2.1 Config Security Store Fails To Create Policy Store Object

Typically, the policy store will recover while its associated database is recovered. If error messages in the WebLogic Server Administration Console document that the data source could not be found in the WebLogic Server, check the data source configuration with WebLogic Developer, retrieve the details of the data source configuration and set the 'Initial Capacity' property to 0; this ensures that the data source will recover while the database starts up.

6.2.2 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`.

6.2.3 Wrong Type Defined For PIP Service Provider After Adding PIP Attribute

The `pip.service.provider` parameter in `jps-config.xml` is required for PIP attributes. When a `jps-config.xml` file without a service provider entry for the `pip.service.provider` parameter is fed to the Administration Console and some PIP attributes are added, a service provider value is automatically added to the `pip.service.provider` with its type defined as AUDIT rather than PIP. In this scenario, after saving `jps-config.xml`, check for the created service provider and manually change the type from AUDIT to PIP.

This step is not required if the service provider is already present before the Administration Console touches the file. Additionally, the Administration Console will not overwrite a service provider entry that is correctly created. This issue only happens when the Administration Console has to add a service provider because of its absence.

6.2.4 Starting the OES Domain Gives an Error When Using Derby Database as the Policy Store

When you start the Oracle Entitlement Server domain after creating a new WebLogic domain for Oracle Entitlement Server using the Oracle Entitlements Server Derby Template, the console displays an error message.

This is because the Oracle Entitlements Server Derby Template does not deploy the IDS task flows, by default.

Workaround:

1. Deploy the $*IDM_HOME*/modules/oracle.idm.ids.config.ui_11.1.2/oracle.idm.ids.config.ui.war as a shared library.
2. Restart the WebLogic Server domain for Oracle Entitlements Server.
3. Log in to the Oracle Entitlements Server Administration Console using the following URL:

   `http://hostname:port/apm/`

6.3 Documentation Errata

This section contains documentation errata for the following document:

- Section 6.3.1, "Oracle Entitlements Server Online Help"

6.3.1 Oracle Entitlements Server Online Help

The online help system contains an older version of *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*. Refer to information in the latest document version available on Oracle Technology Network.

7 Oracle Adaptive Access Manager

This chapter describes issues associated with Oracle Adaptive Access Manager.

It includes the following topics:

- General Issues and Workarounds
- Session Detail Page Issues and Workarounds
- Agent Case-Related Issues and Workarounds
- Multi-Language Support Issues and Limitations
- Documentation Errata

7.1 General Issues and Workarounds

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

- Section 7.1.1, "Many Warnings and One Error During Server Startup in Oracle WebLogic"

7.1.1 Many Warnings and One Error During Server Startup in Oracle WebLogic

There are multiple JMX and DMS related warnings during server startup and one error with following message when accessing oaam_admin for the first time:

```
[2013-02-08T12:07:47.402-08:00] [oaam_admin_server1] [ERROR] [WCS-16178]
[oracle.adfinternal.view.page.editor.utils.ReflectionUtility] [tid:
[ACTIVE].ExecuteThread: '0' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: MATSruleadmin] [ecid:
0000JmvQtubBP9W5Hz5Eif1H5LY800001M,0] [APP: oaam_admin#11.1.2.0.0] Error
instantiating class -
oracle.adfdtinternal.view.faces.portlet.PortletDefinitionDTFactory
```

7.2 Session Detail Page Issues and Workarounds

This section describes Session Details page issues and limitations. It includes the following topic:

- Section 7.2.1, "Session Details Page Has No Scrollbar When Screen Resolution is Low"
- Section 7.2.2, "High and Medium Alert Level Colors Do Not Meet Minimum Color Contrast Ratio"

- Section 7.2.3, "Checkpoint and Transaction Filters Included as Table Column Headers"
- Section 7.2.4, "Checkpoint and Transaction ID Selection Options Do Not Indicate the Data to be Selected"
- Section 7.2.5, "Transaction Data Table Summary Label Does Not Indicate What Data Is Presented"

7.2.1 Session Details Page Has No Scrollbar When Screen Resolution is Low

The Session Details page has no scrollbars which may prevent you from viewing the Alerts summary in the Checkpoint details panel. There is also unused space between the collapsed Session Details and Checkpoints panels.

7.2.2 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.

"High" text contrast is 4.0:1.

"Medium" text contrast is 1.97:1.

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

7.2.3 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 which may cause confusion. This is a known issue, and a workaround is currently not available.

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

In the Session Details Transaction and Checkpoint panels, the selection radio buttons are labeled "Select Row 1" instead of something more meaningful to the user, e.g., "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.

7.2.5 Transaction Data Table Summary Label Does Not Indicate What Data Is Presented

In the Session Details page transactions data table, the transaction data summary tree is labeled "tree table" instead of something more meaningful to the user, e.g., "Transaction Data."

7.3 Agent Case-Related Issues and Workarounds

This section describes issues and limitations related to Agent cases. It includes the following topic:

- Section 7.3.1, "Transaction Cannot Be Null or Empty Error When Replacing an Agent Case with Another Agent Case"
- Section 7.3.2, "Agent Cases Tab is Empty When Signed in as Investigator or Investigation Manager"
- Section 7.3.3, "Refreshing Page in OAAM Admin by User with an Investigator Role Locks the Tabs"

7.3.1 Transaction Cannot Be Null or Empty Error When Replacing an Agent Case with Another Agent Case

When replacing an Agent case with another Agent case, you may see the following pop-up window:

```
Transaction type cannot be null or empty
```

The error message appears when there are no transaction definitions in the system, and you try to replace an Agent case with another Agent case. Currently, you are required to configure at least one transaction definition. The pop-up window does not appear if the system has at least one transaction definition. To work around this issue, configure at least one transaction definition. The problem will be fixed in an upcoming release.

7.3.2 Agent Cases Tab is Empty When Signed in as Investigator or Investigation Manager

In the OAAM Administration Console, the Agent Cases tab is completely blank when signed in as an Investigator or Investigation Manager. The Cases Search page should be displayed along with the search filters and search result table.

As a workaround, perform the following steps:

1. From the Agent Cases tab, click another tab to change the focus. For example, you can click the Sessions or Search Transactions tab.
2. Then, click the **Agent Cases** tab to change the focus back.

Now the Agent Cases tab displays the Agent Cases page and all the functionality work properly.

7.3.3 Refreshing Page in OAAM Admin by User with an Investigator Role Locks the Tabs

When logged in as an Investigator or Investigation Manager (user is a member of the OAAMInvestigatorGroup or the OAAMInvestigationManagerGroup role), after using the browser refresh, some actions in the application do not have effect until a browser refresh is performed again. Each action requires a browser refresh until a new session is started.

7.4 Multi-Language Support Issues and Limitations

This section describes multi-language support issues and limitations. It includes the following topics:

- Section 7.4.1, "Unable to Search KBA Question by Category in Different Locale"
- Section 7.4.2, "Double Apostrophe Displayed in OAAM Administration Console"

7.4.1 Unable to Search KBA Question by Category in Different Locale

Searching for a KBA question using Category with Locale filters does not work. For example:

On 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.

On 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.

7.4.2 Double Apostrophe Displayed in OAAM Administration Console

In some areas of the OAAM Administration Console, the double apostrophe is displayed where a single apostrophe should be when the browser language is set to French. The areas include:

- Tooltips on the Job queue page
- Import operation was successful message
- Tooltip in the Jobs page, such as **Activer l"élément travaux sélectionné**
- Tooltip in **Open Selected** from **Action** menu in all pages
- Policy - Group Linking tab, such as **L"ajout de lien de groupe ne s"applique pas...**
- Policy Set - Action Override tab
- Policy page error messages
- Session page error messages
- User summary - Profile data section, such as **Groupes d"utilisateurs**
- Entities page text, such as **Utilisez l"outil de recherche pour rechercher un...**

7.5 Documentation Errata

This section contains documentation errata for the following document:

- Oracle Fusion Middleware Java API Reference for Oracle Adaptive Access Manager

7.5.1 Oracle Fusion Middleware Java API Reference for Oracle Adaptive Access Manager

Oracle Fusion Middleware Java API Reference for Oracle Adaptive Access Manager does not provide information about the status values for `setUserStatus`. Valid status values are as follows:

```
public static final int STATUS_PENDING_ACTIVATION = 1;
public static final int STATUS_ACTIVE = 2;
public static final int STATUS_DISABLED = 3;
public static final int STATUS_DELETED = 4;
```

STATUS_PENDING_ACTIVATION

The user started registration, but has not completed it. He has entered his username and password and his information has been stored in the database, but he will not be activated until he has completed registration. The user is available in the system, but he is not yet active and cannot perform any operations.

STATUS_ACTIVE

The user is active and available in the system. He has completed registration and can perform all operations.

STATUS_DISABLED

The user is available in the system, but not active. He may be disabled because of fraud or other reasons and cannot perform any operations.

STATUS_DELETED

The user is not available in the system.

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, "Error in OPAM-OIM-WLS-OUD if Account Contains Single Quote"
- Section 8.1.3, "OPAM-OIM:OPAM Catalog Sync Job Fails if Group Name Contains Non-ASCII"
- Section 8.1.4, "idmconfigtool Does Not Create OPAM Admin Roles in Groups Container"

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 Error in OPAM-OIM-WLS-OUD if Account Contains Single Quote

If you are setting up an Oracle Privileged Account Manager-Oracle Identity Manager-Oracle Unified Directory-WebLogic Server integration environment and run an OPAM Catalog Synchronization job using a privileged account name that contains a single quote character (`'`), an exception will occur.

Example trace from `oim_server1-diagnostic.log`:

```
oracle.iam.catalog.exception.CatalogException: Failed to update the Catalog items
with Entity name as 5~cn=testGroup,cn=OPAM,cn=components,cn=IDMRoles,cn=IDMSuite,
dc=example,dc=com at oracle.iam.catalog.repository.DBRepository.updateCatalogItems
(DBRepository.java:651) at oracle.iam.catalog.impl.CatalogServiceImpl.
updateCatalogItems(CatalogServiceImpl.java:84)
```

Or

```
[2013-03-14T19:28:40.270-07:00] [oim_server1] [ERROR] []
[oracle.iam.catalog.repository] [tid: OIMQuartzScheduler_Worker-10]
[userId:oiminternal] [ecid: 0000JpfolZb0vlP5Ifs1yf1HGcF7000003,1:21679]
[APP:oim#11.1.2.0.0] Invalid column index[[java.sql.SQLException: Invalid column
index at oracle.jdbc.driver.OraclePreparedStatement.setTimestampInternal
(OraclePreparedStatement.java:9203)
at oracle.jdbc.driver.OraclePreparedStatement.setTimestamp
  (OraclePreparedStatement.java:9168)
at oracle.jdbc.driver.OraclePreparedStatementWrapper.setTimestamp
  (OraclePreparedStatementWrapper.java:334)
at weblogic.jdbc.wrapper.PreparedStatement.setTimestamp
  (PreparedStatement.java:1038)
at oracle.iam.catalog.repository.DBRepository$1.process(DBRepository.java:614)
at oracle.iam.catalog.repository.DBRepository$1.process(DBRepository.java:554)
at oracle.iam.platform.tx.OIMTransactionCallback.doInTransaction
  (OIMTransactionCallback.java:13)
at oracle.iam.platform.tx.OIMTransactionCallback.doInTransaction
  (OIMTransactionCallback.java:6)
at org.springframework.transaction.support.TransactionTemplate.execute
  (TransactionTemplate.java:128)
at oracle.iam.platform.tx.OIMTransactionManager.execute
  (OIMTransactionManager.java:22)
at oracle.iam.catalog.repository.DBRepository.updateCatalogItems
  (DBRepository.java:554)
at oracle.iam.catalog.impl.CatalogServiceImpl.updateCatalogItems
  (CatalogServiceImpl.java:84)
```

8.1.3 OPAM-OIM:OPAM Catalog Sync Job Fails if Group Name Contains Non-ASCII

If you are setting up an Oracle Privileged Account Manager-Oracle Identity Manager-Oracle Unified Directory-WebLogic integration environment and run an OPAM Catalog Synchronization job using a group name that contains non-ASCII characters, the job will fail with an error.

If you are setting up an Oracle Privileged Account Manager-Oracle Identity Manager-Oracle Unified Directory-IBM WebSphere integration environment and run an OPAM Catalog Synchronization job using a group name that contains a special German Eszett character (**ß**), the job will fail with an error.

8.1.4 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.

8.2 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*

There are no documentation errata items for the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager* 11g Release 2 (11.1.2.1.0), Part Number E27152-03.

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. It includes the following topics:

- Section 9.1, "General Issues and Workarounds"

9.1 General Issues and Workarounds

This topic describes general issues and workarounds for Oracle Identity Navigator. It includes the following topic:

- Section 9.1.1, "Incorrect Release Number for oinav Displays in WebLogic Server Administration Console"

9.1.1 Incorrect Release Number for oinav Displays in WebLogic Server Administration Console

When using the Deployments page in the WebLogic Server administration console, the Oracle Identity Navigator (oinav) release number incorrectly displays as 11.1.1.3.0. This should be 11.1.2.0.0. This does not affect functionality.

10

Oracle Identity Manager

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

- Section 10.1, "Patch Requirements"
- Section 10.2, "General Issues and Workarounds"
- Section 10.3, "Configuration Issues and Workarounds"
- Section 10.4, "Multi-Language Support Issues and Limitations"
- Section 10.5, "Documentation Errata"

10.1 Patch Requirements

This section describes patch requirements for Oracle Identity Manager 11*g* Release 2 (11.1.2). It includes the following sections:

- Obtaining Patches From My Oracle Support (Formerly OracleMetaLink)
- Patch Requirements for Oracle Database 11g (11.1.0.7)
- Patch Requirements for Oracle Database 11g (11.2.0.2.0)
- Patch Requirements for Oracle Database 11g (11.2.0.4.0)
- Patch Requirements for Oracle Database 10g (10.2.0.3 and 10.2.0.4)
- Patch Upgrade Requirement
- Patch Requirement for BI Publisher 11.1.1.6.0

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 FORALL 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
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)

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 11g (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 10–2 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 10–2 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.

10.1.4 Patch Requirements for Oracle Database 11g (11.2.0.4.0)

Table 10–3 lists the patch required for Oracle Identity Manager 11*g* Release 2 (11.1.2) configurations that use Oracle Database 11*g* (11.2.0.4.0).

Table 10–3 Required Patches 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

10.1.5 Patch Requirements for Oracle Database 10*g* (10.2.0.3 and 10.2.0.4)

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 10–4:

Table 10–4 Required Patches for Oracle Database 10g (0.2.0.3 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)

10.1.6 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 10-1 for information about downloading OPatch from My Oracle Support.

10.1.7 Patch Requirement for BI Publisher 11.1.1.6.0

To run the Oracle Identity Manager Reports on BI Publisher 11*g* (11.1.1.6.0), the following patch must be applied on top of BI Publisher 11.1.1.6.0:

p14088000_11g_Generic.zip

10.2 General Issues and Workarounds

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

- Auto-Logged In User is Logged Out After the Cookie Expiry Interval of 120 Seconds
- Localized Display Name Not Reconciled in Oracle Identity Manager Via User/Role Incremental Reconciliation
- Organizations Not Created Because of AD Organization Reconciliation Run
- The SodCheckViolation Field of the Process Form is Not Updated for Request Provisioning
- Blank Page Displayed for Approval Details

10.2.1 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.

10.2.2 Localized Display Name Not Reconciled in Oracle Identity Manager Via User/Role Incremental Reconciliation

When LDAP synchronization is enabled in Oracle Identity Manager with iPlanet via Identity Virtualization Library (libOVD), the localized display names are not populated in mls_usr/mls_ugp for user/role create/update changelog reconciliation. Although the reconciliation event is created, but this is only for the localized display name replacing usr_display_name/ugp_display_name in USR/UGP tables. This is because Oracle Identity Manager is unaware of the backend directory server. It interacts only with OVD/libOVD and uses the data returned in the changelog entries by OVD/libOVD for reconciliation. It does not manipulate the data of the subtypes. iPlanet DS/ODSEE returns only the modified subtype and value to OVD.

To workaround this issue, make changes to all subtypes in the directory server and then try to reconcile into Oracle Identity Manager to ensure that all values exist in the changelog entry result sent by OVD so that Oracle Identity Manager gets the attribute with the values of all subtypes.

For example, if only one subtype, such as lang-ja, for the displayName attribute has to be modified in the LDAP and reconciled into Oracle Identity Manager, and if other subtypes, such as displayName, lang-zh-tw, and lang-fr, already exist in iPlanet/ODSEE, then create a sample ldif file, as shown in Example 10–1, and import it into iPlanet DS/ODSEE with the ldapmodify command. As a result, all the subtypes for the displayName attribute will have separate changelog IDs and will be reconciled into Oracle Identity Manager.

Example 10–1 Sample ldif File

```
dn: cn=AJGroupTEST2,cn=Groups,dc=example,dc=com
changetype: modify
replace: displayName
displayName: All Fusion Roles - All Data RolesTEST2

dn: cn=AJGroupTEST2,cn=Groups,dc=example,dc=com
changetype: modify
replace: displayName;lang-zh-tw
displayName;lang-zh-tw: languser1RolesTEST21-Chinese

dn: cn=AJGroupTEST2,cn=Groups,dc=example,dc=com
```

```
changetype: modify
replace: displayName;lang-fr
displayName;lang-fr: languser1RolesTEST-French

dn: cn=AJGroupTEST2,cn=Groups,dc=example,dc=com
changetype: modify
replace: displayName;lang-ja
displayName;lang-ja: languser1RolesTEST-Japanese1
```

10.2.3 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.

10.2.4 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.

10.2.5 Blank Page Displayed for Approval Details

When you try to open the approval details page in the Pending Approvals section of Oracle Identity Self Service, a blank page is displayed.

To workaround this issue, use Oracle Enterprise Manager to edit the approval task of the required SOA composites to remove the SSL port for Oracle Identity Manager in the Administration tab.

To workaround this issue:

1. Login to Oracle Enterprise Manager by using WebLogic administrator username and password.
2. On the left hand side menu, click **SOA**. Click the **+** sign to expand soa-infra. Click the **+** sign to expand default.
3. Click the required SOA composites under default menu.
4. On the right hand side, click the Approval task under Component Metrics section.
5. Click the **Administration** tab.
6. Set the value of HTTPS port to `0`.

10.2.6 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.

10.2.7 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.

10.2.8 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.

10.2.9 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.

10.2.10 Error Generated if a User is Created When the Corresponding LDAP Container Does Not Exist

When you create a user and the corresponding LDAP container with dynamic rule does not exist, an error is generated. For example, the following containers have been created in the LDAP server:

```
cn=FusionUsers,cn=CAD,dc=us,dc=example,dc=com
cn=FusionUsers,cn=USA,dc=us,dc=example,dc=com
```

If you create a user with country code China where the corresponding container does not exist in LDAP, then the following error is generated:

```
va:1454)
        at weblogic.work.ExecuteThread.execute(ExecuteThread.java:209)
        at weblogic.work.ExecuteThread.run(ExecuteThread.java:178)
Caused By: javax.naming.NameNotFoundException: [LDAP: error code 32 - LDAP
Error 32 : [LDAP: error code 32 - Parent entry not found in the directory.]];
remaining name 'cn=ktestoimuser10
ktestoimuser10,cn=FusionUsers,cn=China,dc=us,dc=example,dc=com'
        at com.sun.jndi.ldap.LdapCtx.mapErrorCode(LdapCtx.java:3066)
        at com.sun.jndi.ldap.LdapCtx.processReturnCode(LdapCtx.java:2987)
        at com.sun.jndi.ldap.LdapCtx.processReturnCode(LdapCtx.java:2794)
        at com.sun.jndi.ldap.LdapCtx.c_createSubcontext(LdapCtx.java:788)
        at com.sun.jndi.toolkit.ctx.ComponentDirContext.p_
createSubcontext(ComponentDirCo
ntext.java:319)
        at
com.sun.jndi.toolkit.ctx.PartialCompositeDirContext.createSubcontext(PartialCo
mpositeDirContext.java:248)
        at
javax.naming.directory.InitialDirContext.createSubcontext(InitialDirContext.ja
va:183)
        at example.iam.platform.entitymgr.provider.ldap.LDAPUtil.createSubcont
```

To workaround this issue, create the missing container in LDAP server that matches the container specified in the LDAPContainerRules.xml file.

10.2.11 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*.

10.2.12 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.

10.2.13 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.

10.2.14 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.

10.2.15 Interrupted Scheduled Job Run Fails on Restarting

When a long running scheduled job is run for a considerable time and the job is interrupted by pressing 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.

10.2.16 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.

10.2.17 Heterogeneous Request for Entitlements Without Primary Account Can Be Submitted

When a heterogeneous request involving entitlements, whose primary accounts are not provisioned, is submitted, no error is generated. This is because the submission of bulk request goes through without any validations, until the request is approved.

This is a known issue, and a workaround is currently not available.

10.2.18 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.

10.2.19 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.

10.2.20 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.

10.2.21 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.

10.2.22 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.

10.2.23 Values in Dependent Combo Box Not Displayed On Selecting Value in Parent Combo Box

When you have a dependent lookup with a combo box and select a value in the parent combo box, the correct values in the dependent combo box are not displayed.

To workaround this issue, add the partialTriggers through WebCenter Composer to refresh the dependent choice. To do so:

1. Find the parent choice list component ID by downloading the JSFF file.

2. In WebCenter Composer, set the partialTriggers property of the dependent list with the parent choice list component id.

10.2.24 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 filtering the records for the requester in the Track Requests page by using Query By Example (QBE) when the user does not have permissions on the requester's organization does not return any result.

This is a known issue, and a workaround is currently not available.

10.2.25 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, drop it on the User Details pages as a check box, and mark the field as read-only.

10.2.26 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 to have the Entitlement=true property being set and the field type to be lookup field:

- **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.

10.2.27 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.

10.2.28 Refresh Button in the Entitlements Tab Does Not Work

In the Entitlements tab of the Application Instances page, the **Refresh** button is not working. Although entitlements are created, but clicking the **Refresh** button does not display the entitlements.

To workaround this issue, click the **Organizations** tab, and then click the **Entitlements** tab again. The entitlements will be displayed in the Entitlements tab.

10.2.29 No Actions for Create To-Do Task and Create Subtask Menu Items

In the Actions menu of the Pending Approvals page, the **Create To-Do Task** and **Create Subtask** menu options are available for approval tasks. These actions are performed by SOA, and therefore, no actions are performed in Oracle Identity Manager for these.

10.2.30 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*.

10.2.31 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
```

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.

10.2.32 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%**).

10.2.33 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.

10.2.34 UDF for Provisioned Users Not Displayed in the UI

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.

To workaround this issue, run the Form Version Control (FVC) utility by specifying the latest version after adding the UDF to the form.

10.2.35 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.

10.2.36 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.

10.2.37 Application Instance Not Activated or Published

If an application instance, which has forms attached to it, is to be used in the request catalog, then either the sandbox must be activated or published.

10.2.38 Benign unknownplatformexception Error

A benign `unknownplatformexception` error is displayed some times when logging in by using any client in Oracle Identity Manager, for example while logging in to the Design Console, although the logging is successful.

This does not result in any loss of functionality.

10.2.39 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.

10.2.40 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.

10.2.41 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.

10.2.42 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.

10.2.43 Initiated Tasks and Administrative Tasks in the Pending Approvals Page Not Used

In the Pending Approvals page of Oracle Identity Self Service, the My Tasks, Initiated Tasks, and Administrative Tasks tabs are displayed. These tabs are generated by SOA. In Oracle Identity Manager, only the My Tasks tab is used.

10.2.44 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.

10.2.45 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.

10.2.46 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.

10.2.47 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 run with a suboptimal plan in few environments, but not in all the 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, the suboptimal SQL can be tuned via locking a better SQL plan in the Oracle Database. This is achieved by using the SQL Profile feature of Oracle Database. 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, SQL Profile can be used to lock a better SQL plan for the SQL in the database environment (by using the SQL Tuning Advisor and subsequent usage of SQL Profiles).

10.2.48 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.

10.2.49 Rule Creation For More Than 10000 Users Fail

Rule creation for group membership does not work if it matches more than 10000 users during the rule creation.

This is a known issue, and a workaround is currently not available.

10.2.50 Some Special Characters Do Not Work Directly in Catalog Search

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 achieve the result set with these special characters, it is recommended to escape these characters with backslash (\). For example, specify **\:\"** or **\(** in the search criteria to escape the **:**, **"**, and **(** special characters.

10.2.51 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.

10.2.52 Error in Adding Data for Process Instance to Child Form

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>

10.2.53 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.

10.2.54 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.

10.2.55 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.

10.2.56 Duplicate Rows in Request Tracking

Request tracking might display duplicate rows for the same request when searching by beneficiary. Ignore the duplicate rows.

10.2.57 Help Desk and Beneficiaries Cannot View Approval Status

Only the requestor and approver of a request and the System Administrator are allowed to track the approval status. Help Desk user and beneficiaries of the request cannot view the approval status.

This is a known issue, and a workaround is currently not available.

10.2.58 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.

10.2.59 Use Request Details to Approve Requests That Do Not 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.

10.2.60 Justification Not Persisted

Oracle Identity manager does not persist the Justification entered during a request process, and therefore, this data will not be available for reporting.

10.2.61 The Refresh Button in Some Pages Do Not Work Properly

Due to ADF caching, some of the pages do not refresh properly on clicking the **Refresh** button.

To workaround this, close the tab and re-open it.

10.2.62 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.

10.2.63 Accessibility Compliance

Currently, the system is not compliant completely with Accessibility guidelines and the Accessibility link provided does not function.

10.2.64 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.

10.2.65 Request Summary Report Does Not Work

The existing Request Summary Report does not work in Oracle Identity Manager 11*g* Release 2 (11.1.2) because of request model changes.

This is a known issue, and a workaround in currently not available.

10.2.66 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.

10.2.67 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.

10.2.68 Application Instance Administrator Cannot Create Forms

Only System Administrators or System Configurators can create forms and attach it to application instances.

10.2.69 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.

10.2.70 Unpublished Entitlements Provisioned Via Access Policy

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.

10.2.71 Organization UDF Not Supported

Oracle Identity Manager does not support user defined fields (UDFs) in this release.

10.2.72 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.

10.2.73 Apply and Revert Buttons Remain Disabled After Changing UDF value

After you change the value of a user defined field (UDF) and move out of the field, the **Apply** and **Revert** buttons remain disabled. Note that if you change the value of a predefined field, then these buttons are enabled as expected.

To workaround this issue:

1. Create a sandbox and activate it. Open the page that contains the UDF, and click **Customize**.
2. Select **View**, **Source**.
3. Note the value of the valueChangeListener property of a predefined field. To do so:
    a. Click the predefined field, and then click **Edit** to open the Component Properties dialog box.
    b. Copy the value of the valueChangeListener property.
4. Export the sandbox as a ZIP file.
5. Extract the ZIP file and edit the jsff.xml file for the specific screen.
6. Add the following attributes to the ADF tag, for example af:inputText, for the UDF:
    - valueChangeListener=*VALUE_COPIED_IN_STEP3*
    - autoSubmit="true"
7. Create the ZIP file for the sandbox.
8. Import the sandbox.
9. Publish the sandbox.

10.2.74 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.

10.2.75 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.

10.2.76 Approval Page Customization Not Supported

Approval page customization is not supported in this release. Therefore, functionalities, such as requester-only and approver-only, cannot be achieved.

10.2.77 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.

10.2.78 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.

10.2.79 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.

10.2.80 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.

10.2.81 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.

10.2.82 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.

10.2.83 Number Type Lookup Code Not Supported

Oracle Identity Manager does not support number type lookup code in this release.

10.2.84 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.

10.2.85 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.

10.2.86 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.

10.2.87 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*.

10.2.88 Entitlements Provisioned to Users Not Displayed After Upgrade

In an upgraded deployment of Oracle Identity Manager 11*g* Release 2 (11.1.2), 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.

10.2.89 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.

10.2.90 UMS Fails to Send Notification While Provisioning Account

If a notification template has been attached to a corresponding provisioning task, then while provisioning an account for OIM user, a notification message is not sent and a NullPointerException error message is logged if only UMS notification provider is configured. Notification templates are not supported in Oracle Identity Manager 11*g* Release 2 (11.1.2).

10.2.91 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.

10.2.92 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.

10.2.93 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.

10.2.94 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.

10.2.95 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.
```

10.2.96 Worklist Views Do Not Work After Applying Patch 16385074

After applying patch 16385074 for SOA 11.1.1.6.0, clicking the worklist views in the Inbox do not refresh the results in the view tables. This is because the application cache contains the old copy of the JSP files changed in the patch.

Therefore, to workaround this issue, clear the contents of the following directory:

OIM_DOMAIN_HOME/servers/*OIM_SERVER*/tmp/_WL_user/

10.2.97 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.

10.2.98 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.

10.2.99 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.

10.2.100 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.

10.2.101 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.

10.2.102 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

10.2.103 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

10.2.104 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.

10.2.105 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.

10.2.106 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.
```

10.2.107 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 attribte 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

10.2.108 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 Configuration Issues and Workarounds

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

10.3.1 Deep Linking of Identity URL in SOA Email Notification Does Not Work

When you embed an identity URL in SOA email notification, it does not work. To avoid this issue, apply the following SOA patch after installing SOA:

#15211191 - EMAIL NOTIFICATION DOESN'T EMBED URL PROPERLY IF IT CONTAINS /IDENTITY

10.3.2 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.

10.3.3 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.

10.3.4 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.

10.3.5 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.

10.3.6 Email Not Readable When Oracle Identity Manager Configured in SSL Mode

When Oracle Identity Manager is configured in SSL mode, the body of the email sent for approval task assignment from SOA is not readable. The following is displayed in the email body content:

```
Error 500--Internal Server Error
From RFC 2068 Hypertext Transfer Protocol -- HTTP/1.1:
10.5.1 500 Internal Server Error

The server encountered an unexpected condition which prevented it from fulfilling
the request.
```

10.3.7 Request Might Fail if SOA Server is Enabled to SSL Mode

If SOA, Oracle Identity Manager, and WebLogic Servers are enabled to listen on SSL port, then requests might fail.

To workaround this issue, enable both the SSL and non-SSL listen ports for SOA, Oracle Identity Manager, and WebLogic Servers by using the WebLogic Administrative Console.

10.3.8 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 Multi-Language Support Issues and Limitations

This section describes multi-language issues and limitations. It includes the following topics:

- UI Components are Displayed in English on non-English Web Browsers
- Date Format in Search Criteria Displayed in MM/dd/yyyy hh:mm:ss Format on non-English Locale
- BI Publisher 11g Reports Displayed in English Although Translation Files Are Available
- Date Format in BI Publisher Report Not Displayed Per Report Locale Setting
- Translated Values Not Displayed for User Type and Locale
- Catalog Search With Special Non-ASCII Characters Do Not Work Correctly
- Polish Translation of BI Publisher Files Do Not Work
- Localized String for Cart is Truncated in the Catalog Search Results Page
- Request Type and Status Search Options Displayed in Server Locale
- Values Not Displayed Per Browser Language Setting
- Challenge Questions and Password Policy Messages Displayed in Server Locale
- Values for Organization Type and Status Displayed in English
- MLS and MR Support Not Available
- Request Status and Request Type Displayed in English
- Error Displayed If User Login Contains Special Character
- Task Stage Name and Task Assignee Label Displayed in English
- Escalating Request Displayed Warning in Server Locale
- Some Predefined View Names Cannot Be Translated
- Request Task Details Displayed in Server Locale

10.4.1 UI Components are Displayed in English on non-English Web Browsers

On the Lookups or Form Details pages in Oracle Identity System Administration, most UI components are displayed in English on non-English web browsers.

This is known issue, and a workaround is currently not available.

10.4.2 Date Format in Search Criteria Displayed in MM/dd/yyyy hh:mm:ss Format on non-English Locale

On Oracle BI Publisher Enterprise, while running Oracle Identity Manager 11*g* Release 2 (11.1.2) reports, the date fields on the search criteria panel are always displayed in the MM/dd/yyyy hh:mm:ss format on non-English locale. This is irrespective of the report locale or UI language selected for the current logged-in BI Publisher user. This is because the date format cannot be globalized because it is designed in the report data model and uses Java-provided date format pattern letters.

10.4.3 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.

10.4.4 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.

10.4.5 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.

10.4.6 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.

10.4.7 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.

10.4.8 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.

10.4.9 Request Type and Status Search Options Displayed in Server Locale

The values in the Request Type and Status lists in the search panel of the Track Requests tab are intermittently displayed in server locale instead of browser locale when Oracle Identity Manager is started or restarted.

To workaround this issue, close the Track Requests tab and reopen it.

10.4.10 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.

10.4.11 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.

10.4.12 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.

10.4.13 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.

10.4.14 Request Status and Request Type Displayed in English

The values of the Request Status and Request Type fields are displayed in English instead of browser language in the Request Details page and the Pending Request portlet of the Home page.

This is a known issue, and a workaround is not available.

10.4.15 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
```

10.4.16 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.

10.4.17 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.

10.4.18 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

10.4.19 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.

To workaround this issue:

1. Navigate to the Inbox in Oracle Identity Self Service.
2. Click the Edit User Preferences icon on the Worklist Views section toolbar. The Edit User Preferences dialog box is displayed.
3. For Use language settings of, select the **Browser** option.
4. Click **OK**.

10.5 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:

- Section 11.1, "Integrating Access Manager and Oracle Adaptive Access Manager"
- Section 11.2, "Documentation Errata"

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 topic:

- Section 11.1.1, "File Not Found Exception Displayed for Entering Incorrect AdminServer User Name and Password"

11.1.1 File Not Found Exception Displayed for Entering Incorrect AdminServer User Name and Password

When integrating Access Manager and Oracle Adaptive Access Manager, if an administrator runs the `setupOAMTAPIntegration` script and enters the wrong OAAM AdminServer user name and OAAM AdminServer password, the following incorrect error message is displayed:

```
java.io.FileNotFoundException: .\config\jps-config.xml
```

An error message should be displayed to inform the administrator that he had entered the incorrect user name and password.

11.2 Documentation Errata

This section 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*.

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:

- Section 12.1, "General Issues and Workarounds"
- Section 12.2, "Configuration Issues and Workarounds"
- Section 12.3, "Documentation Errata"

12.1 General Issues and Workarounds

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

- Section 12.1.1, "Additional Debug/TRACE Details in Exception Message"
- Section 12.1.2, "Cell Creation Fails When Multiple Templates are Selected With Oracle Identity Manager in the Same Session"
- Section 12.1.3, "Opening Identity Directory Service Profile Displays Warning Popup in Oracle Entitlements Server"
- Section 12.1.4, "Cannot Create CSF Mapping in IBM WebSphere with Target Domain in WebLogic Server"
- Section 12.1.5, "OIMAdmin Keys Credential Might Be Lost"
- Section 12.1.6, "Warnings, Errors and Stack Traces Appear in oaam_admin Log File of OAAM Configured on IBM WebSphere"
- Section 12.1.7, "Task Details Page Might Throw ADFC-12000 Errors"
- Section 12.1.8, "Some Approval Policies Not Deleted After Upgrade"
- Section 12.1.9, "Oracle Identity Federation Audit Records Not Moved to Database"
- Section 12.1.10, "All Channels Cannot be SSL Enabled between OIM and Database Server on Websphere"

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 the issue:

1. 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`.
2. Set the `com.ibm.CORBA.ShortExceptionDetails` system property to `true` 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 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;
 /
```

12.1.9 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.

12.1.10 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.

Workaround:

OIM application has three different channels to the database:

- Data Sources
- Direct DB for DDL operations
- Custom registry

Workaround:

To enable only one SSL, on each data source add the following custom property:

```
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.

12.2 Configuration Issues and Workarounds

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

- Section 12.2.1, "SSLHandshakeException Error for Google and Yahoo IdP Partners"
- Section 12.2.2, "Controlled-Push Policy Distribution Fails on Oracle Entitlements Server Administration Server"
- Section 12.2.3, "Shell Syntax Error Seen When Configuring Fusion Middleware Products on IBM Websphere Application Server on Solaris SPARC64 5.10 Machines"
- Section 12.2.4, "Error Displayed When Accessing DMS Spy for Oracle Access Manager on IBM Websphere"
- Section 12.2.5, "oaam_offline_was.ear File Missing antlr-2.7.6.jar File in IBM WebSphere Environment"
- Section 12.2.6, "Use Custom Certificate to Configure SSL for Oracle Entitlements Administration on IBM Websphere"

- Section 12.2.7, "Oracle Identity Manager Server Configuration on IBM WebSphere Fails If Sun JDK is Used During Installation"
- Section 12.2.8, "Error Generated When Extending an OAAM WebSphere Cell to Include OIM Template"

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 oaam_offline_was.ear File Missing antlr-2.7.6.jar File in IBM WebSphere Environment

OAAM Offline is not loading the correct number of records and rules are not being processed. The offline logs show the following error:

```
java.lang.NoClassDefFoundError: antlr.TokenStream
```

The offline environment cannot process rules because the `antlr-2.7.6.jar` file is missing from the `oaam_offline_was.ear` file.

As a workaround, perform the following steps on the command line from the `IDM_ORACLE_HOME` directory before running `was_config.sh`.

```
cd IDM_ORACLE_HOME/oaam/oaam_offline/ear
mv oaam_offline_was.ear oaam_offline_was.ear.bak
mkdir temp
cd temp
jar xf ../oaam_offline_was.ear
mkdir war_tmp
cd war_tmp
jar xf ../oaam_offline.war
cp IDM_ORACLE_HOME/oaam/oaam_libs/was_native_jar/antlr-2.7.6.jar ./WEB-INF/lib
```

```
jar -cfm ../oaam_offline.war META-INF/MANIFEST.MF  *
cd ..
rm -rf war_tmp
jar -cfm ../oaam_offline_was.ear META-INF/MANIFEST.MF *
cd ..
rm -rf temp
```

12.2.6 Use Custom Certificate to Configure SSL for Oracle Entitlements Administration on IBM Websphere

When an Oracle Entitlements Server domain on IBM Websphere is created (by applying OES WAS template), by default SSL is configured using the demoTrust and keystore certificates signed by the demo certificate (CerGenCA). In a production environment, Oracle recommends you change the default setting and use a custom trust and identity key store.

12.2.7 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.

12.2.8 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.

12.3 Documentation Errata

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

- Adding Targets to Oracle Privileged Account Manager

- Differences When Integrating Oracle Privileged Account Manager with Oracle Identity Manager
- Online Help for IBM WebSphere Options in the Oracle Identity Manager Configuration Assistant

12.3.1 Adding Targets to Oracle Privileged Account Manager

The following section should be added to the "Managing Oracle Privileged Account Manager on IBM WebSphere" chapter in the *Oracle Fusion Middleware Third-Party Application Server Guide for Oracle Identity and Access Management*.

12.3.1.1 Differences When Adding Targets to Oracle Privileged Account Manager on IBM WebSphere

The procedure for adding targets to Oracle Privileged Account Manager is described in "Adding Targets to Oracle Privileged Account Manager" of the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*. However, the process for configuring an Oracle database target is slightly different if you are using Oracle Privileged Account Manager on IBM WebSphere:

If you select an Oracle database target, then no driver jar is required. For other target systems, you must include one of the following third-party jars:

- **For MSSQL**: Copy the `sqljdbc4.jar`.
- **For MySQL**: Copy the `mysql-connector-java-5.1.20-bin.jar`.
- **For Sybase**: Copy the `jconn4.jar`.

You can modify the connector jars to include these third-party jars as follows:

1. Make a back-up copy of the DBUM connector bundle, which is available in

   ```
   ORACLE_HOME/connectors/dbum/bundle/org.identityconnectors.dbum-1.0.1116.jar
   ```

2. Create a `temporary/lib` folder and put the third-party jars in that folder.
3. Update the bundle with the third-party jar:

   ```
   jar -uvf org.identityconnectors.dbum-1.0.1116.jar lib/JAR_NAME
   ```

4. Remove the `temporary/lib` folder.
5. Restart all Oracle Privileged Account Manager processes for the change to take effect.

For more information, refer to "Installing the Connector on the Connector Server" in the *Oracle Identity Manager Connector Guide for Database User Management*.

12.3.2 Differences When Integrating Oracle Privileged Account Manager with Oracle Identity Manager

The following information should be added to the "Managing Oracle Privileged Account Manager on IBM WebSphere" chapter of the *Oracle Fusion Middleware Third-Party Application Server Guide for Oracle Identity and Access Management*.

12.3.2.1 Differences When Running the `opamSetup` Script

The basic procedure for running the Oracle Privileged Account Manager-Oracle Identity Manager integration setup script (`opamSetup`) is described in "Running the `opamSetup` Script" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.

However, if you are running this script on an IBM WebSphere server, there is a minor difference in the description of the `ctxFactory` option. The usual context factory name (noted parenthetically in the table) is different for IBM WebSphere as shown here:

Option	Description
-ctxFactory <*Initial context factory*>	Provide the name of the context factory (usually com.ibm.websphere.naming.WsnInitialContextFactory).

12.3.3 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*.