Oracle® Fusion Middleware

Identity Management Release Notes

11*g* Release 2 (11.1.2)

E35820-09

February 2015

ORACLE®

Oracle Fusion Middleware Identity Management Release Notes, 11*g* Release 2 (11.1.2)

E35820-09

Contents

5 Oracle Access Management

9 Oracle Privileged Account Manager

10 Oracle Identity Navigator

11 Oracle Identity Governance Framework

12 Oracle Identity Manager

13 IdM Integration

Preface

This preface includes the following sections:

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see these Oracle resources:

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

Conventions

The following text conventions are used in this document:

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

1 Introduction

This chapter introduces Oracle Fusion Middleware Identity Management Release Notes, 11g Release 2 (11.1.2). It includes the following topics:

1.1 Latest Release Information

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

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

1.2 Purpose of this Document

This document contains the release information for Oracle Fusion Middleware 11g Release 2 (11.1.2). It describes differences between Oracle Fusion Middleware and its documented functionality.

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

1.3 System Requirements and Specifications

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

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

1.4 Certification Information

This section contains the following:

1.4.1 Where to Find Oracle Fusion Middleware Certification Information

The latest certification information for Oracle Fusion Middleware 11g Release 1 (11.1.1) 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 1 (11.1.1) components, see the Release Notes for the specific Oracle Fusion Middleware 11g Release 1 (11.1.1) component.

This section contains the following topics:

1.4.2.1 Certification Information for Oracle Fusion Middleware 11g R1 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 => 'ODS'
      ,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

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 Upgrading Sun JDK From 1.6.0_07 to 1.6.0_11

For information, see {{{Author needs to replace cross reference.}}}

1.4.4 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.

1.4.5 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 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.

For additional patching information, see {{{Author needs to find and replace cross reference.}}}.

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 Identity Manager	16390983	This patch is critical if you are using Oracle Unified Directory in active-active mode as shown in the topology diagrams 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. See Section 2.2.1, "Apply Patches and Manually Copy OIM Adapter Template."
Oracle Platform Security Services	15894053	Required with Patch 16390983.

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

This chapter describes issues associated with the installation and configuration process of Oracle Identity and Access Management 11*g* Release 2 (11.1.2). It includes the following sections:

- Section 2.1, "General Issues and Workarounds"
- Section 2.2, "Configuration Issues and Workarounds"
- Section 2.3, "Mandatory Patches for Installing Oracle Identity Manager"

2.1 General Issues and Workarounds

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

- Section 2.1.1, "Error when Installing OIM Design Console"
- Section 2.1.2, "Launching Oracle Identity Manager Configuration Wizard on AIX with JDK7"
- Section 2.1.3, "Simple Security Mode Does Not Work on AIX"
- Section 2.1.4, "Unable to Add Weblogic Password in the Fusion Middleware Configuration Wizard"
- Section 2.1.5, "JPS Keystore Service Initialization Failure in Join Domain Scenario for Oracle Access Management Domain"

2.1.1 Error when Installing OIM Design Console

When you are trying to install Oracle Identity Manager (OIM) Design Console on a Windows machine that has firewall between the machine and the OIM 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 OIM Design Console, you must open port 7 in the firewall.

2.1.2 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>`

2.1.3 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.

2.1.4 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)

2.1.5 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 (OPSS) configuration does not exist but passwords are already available from OIM installation in the Credential Store Framework (CSF) 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 OPSS (`jps-config.xml`) configuration.

2.2 Configuration Issues and Workarounds

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

2.2.1 Apply Patches and Manually Copy OIM Adapter Template

The patches and workaround described in this note are required only if you are integrating Oracle Access Manager or Oracle Identity Manager with Oracle Unified Directory, and Oracle Unified Directory is configured for High Availability in active-active mode.

After performing a fresh installation of Oracle Identity and Access Management, apply the patch for Oracle Identity Manager Bug 16390983 and also Patch 15894053.

Then manually copy the file `adapter_template_oim.xml` from *`ORACLE_COMMON_HOME`*`/modules/oracle.ovd_11.1.1/templates/` to: *`IAM_ORACLE_HOME`*`/libovd/`. For example:

```
cp ORACLE_COMMON_HOME/modules/oracle.ovd_11.1.1/templates/adapter_template_oim.xml
IAM_ORACLE_HOME/libovd/
```

2.2.2 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.

2.2.3 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 (OAM) 11*g* Release 2 (11.1.2) or Oracle Identity Manager (OIM) 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>
```

2.2.4 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.

2.2.5 Warning Messages from idmConfigTool -upgradeLDAPUsersForSSO are Safe to Ignore

If you upgrade existing LDAP users using a command such as:

```
idmConfigTool.bat -upgradeLDAPUsersForSSO input_file=filename
```

you might see warning messages similar to these:

```
WARNING: Expiry date not present in cn=oamadmin,cn=Users,
dc=us,dc=oracle,dc=com
WARNING: Expiry date not present in cn=weblogic_idm,cn=Users,
dc=us,dc=oracle,dc=com
WARNING: Expiry date not present in cn=orcladmin, cn=Users,
dc=us,dc=oracle,dc=com
```

These messages do not impact function and can be safely ignored.

2.3 Mandatory Patches for Installing Oracle Identity Manager

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

> **Note:** This section provides the mandatory patches that were available at the time of publishing the release notes. For additional changes and revised patch requirements, see My Oracle Support document ID 1908280.1.

The patches must be downloaded only after you have installed Oracle Identity Manager using the Oracle Identity and Access Management 11*g* Release 2 (11.1.2) Installer and before starting the Oracle Identity Manager configuration.

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 11g Release 2 (11.1.2)

Oracle Fusion Middleware Product or Component	Patch Number/Name	When to Apply?	Description
Oracle Application Access Controls Governor	13931550	After installing Oracle Identity and Access Management	This is a mandatory Oracle Application Access Controls Governor patch. Follow the `README.txt` file for patching instructions.
Oracle Containers for J2EE	14049150	After installing Oracle Identity and Access Management	This is a mandatory Oracle Containers for J2EE patch. Follow the `README.txt` file for patching instructions.
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. This patch will overwrite any previously applied SOA patch.
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. Select patch version 11.1.1.6.7, download the 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. Select patch version 11.1.1.6.0, download the patch, and follow the `README.txt` file for patching instructions.
Oracle Application Development Framework	19597633	After installing Oracle Identity and Access Management	This is an Oracle Application Development Framework (ADF) patch. Follow the `README.txt` file for patching instructions.

Table 2–1 (Cont.) Patches Required to Fix Specific Issues with Oracle Identity Manager 11g Release 2 (11.1.2)

Oracle Fusion Middleware Product or Component	Patch Number/Name	When to Apply?	Description
Oracle Virtual Directory	14016801	After installing Oracle Identity and Access Management	This is a mandatory Oracle Virtual Directory 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. Select patch version 11.1.1.6.0, download the patch, and follow the `README.txt` file for patching instructions.
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.

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.

3

Upgrade and Migration Issues for Oracle Identity and Access Management

This chapter describes issues associated with the upgrade and migration process of Oracle Identity and Access Management 11*g* Release 2 (11.1.2). It includes the following sections:

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

3.1 Upgrade Issues

This section describes issues related to upgrading the following components:

- Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2)
- 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)
- 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)
- Oracle Identity Navigator 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Navigator 11*g* Release 2 (11.1.2)
- Oracle Entitlements Server 11*g* Release 1 (11.1.1.5.0) to Oracle Entitlements Server 11*g* Release 2 (11.1.2)
- Oracle Identity and Access Management 11*g* Release 1 (11.1.1.3.0) to Oracle Identity and Access Management 11*g* Release 2 (11.1.2)
- Oracle Identity Manager 9.x to Oracle Identity Manager 11*g* Release 2 (11.1.2)

3.1.1 General Issues and Workarounds

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

- Section 3.1.1.1, "OIM-OAM-OAAM: 11.1.1.5.0 to 11.1.2: Error Reset Password in First Login"
- Section 3.1.1.2, "Save Column with Multiple/Null Values to be Manually Updated for LookupByQuery"
- Section 3.1.1.3, "Entitlements Assigned in OIM 11.1.1.5.0 Are Not Shown in the Entitlement Tab After Upgrade"

3.1.1.1 OIM-OAM-OAAM: 11.1.1.5.0 to 11.1.2: Error Reset Password in First Login

While upgrading an OAM-OIM-OAAM integrated11*g* R1 (11.1.1.5.0) environment to 11*g* R2 (11.1.2), when the user tries to login into `http://bej301133.cn.oracle.com:7777/identity` for the first time, the user is redirected to the password management page. However, when the user clicks **Submit** after editing the user profile, an error message pops up.

The workaround is as follows:

On UNIX:

1. Go to the following location:

   ```
   IAM_ORACLE_HOME/server/apps
   ```

2. In this location, create a directory by using the following command:

   ```
   mkdir temp
   ```

3. Copy the `oracle.iam.console.identity.self-service.ear` file to the `temp` folder that you created in step 2, by running the following command:

   ```
   cp oracle.iam.console.identity.self-service.ear temp
   ```

4. Go to the `temp` folder that you created :

   ```
   cd temp
   ```

5. Extract the contents of the `oracle.iam.console.identity.self-service.ear` file by running the following command:

   ```
   jar -xvf oracle.iam.console.identity.self-service.ear
   ```

   The folder `META-INF/` is automatically created in the location.

6. Locate the `weblogic-application.xml` file in the folder `META-INF`, and edit the contents of the file by adding the following packages before the parameter `</weblogic-application>`:

```
<prefer-application-packages>
<package-name>oracle.iam.*</package-name>
<package-name>oracle.security.am.common.nap.*</package-name>
<package-name>oracle.security.am.common.aaaclient.*</package-name>
<package-name>oracle.security.am.common.*</package-name>
</prefer-application-packages>
```

7. Save the changes made in the `weblogic-application.xml` file and exit.
8. Package the extracted contents back into the `oracle.iam.console.identity.self-service.ear` file by running the following command:

```
jar -cvf oracle.iam.console.identity.self-service.ear
```

9. Copy the contents of the `temp` folder to the original location `IAM_ORACLE_HOME/server/apps`.

   Ensure that you take a backup of the files of the existing location, before you replace the content.

3.1.1.2 Save Column with Multiple/Null Values to be Manually Updated for LookupByQuery

This bug is related to manual updations that a customer would need to perform as a post-upgrade step. This happens when there are multiple values specified for the **Column Names** attribute while defining `lookupby` in a 9.x environment.

If the OIM 9.x Role or User data model contains UDFs of type `Lookup Query`, then after upgrading, do the following:

For Role:

1. Start the Design Console.
2. Select **Administration**.
3. Select **User Defined** field and select **Roles**.
4. Ensure that the property for **Column Names** and **Lookup Column Name** is set to the desired column name for the **Role Lookup Query UDF**. If the value is not present, provide an appropriate value, and click **Save**.

This updates the MDS definitions. These fields are visible in the OIM 11.1.2 Administrator user interface.

For Users:

1. Start the Configuration Service user interface.
2. Select **Administration**.
3. Select **User Defined** field.
4. Open the **User** configuration service, open the UDFs which are of type `Lookup By Query`. Specify the required value in **Column to Display** and **Column to save** fields.
5. Click **Save**.

This will update the MDS definitions for the User Lookup Query UDFs. These fields are visible in the OIM 11.1.2 Administrator user interface.

3.1.1.3 Entitlements Assigned in OIM 11.1.1.5.0 Are Not Shown in the Entitlement Tab After Upgrade

Entitlements assigned to OIM 11*g* Release 1 (11.1.1.5.0) users are not shown in the **Entitlement** tab after upgrading to OIM 11*g* Release 2 (11.1.2).

Entitlement or child forms provisioned to OIM 11*g* Release 1 (11.1.1.5.0) users, according to access policy, is removed from OIM 11*g* Release 1 (11.1.1.5.0) users after upgrading to OIM 11*g* Release 2 (11.1.2).The resource is shown in **Accounts** in the provisioned state.

3.1.1.4 OIM-OAM: Upgrade to OAM 11.1.1.5.2 or Later Mandatory Before Upgrade to OIM 11.1.2

If you wish to integrate OIM 11*g* Release 2 (11.1.2) with OAM for single sign-on, then you must upgrade OAM 11*g* Release 1 (11.1.1.5.0) to OAM 11*g* Release 1 (11.1.1.5.2) or later. If do not upgrade OAM 11*g* Release 1 (11.1.1.5.0) to OAM 11*g* Release 1 (11.1.1.5.2) or later, the auto-login functionality will not work.

The workaround for this issue is as follows:

For the auto-login functionality to work, upgrade OAM 11*g* Release 1 (11.1.1.5.0) to OAM 11*g* Release 1 (11.1.1.5.2) or later.

3.1.1.5 Lookup Values Do Not Get Saved in the My Information Page

The **Look Up** values selected do not get saved in the **My Information** page. An error, like the following, is displayed:

```
JBO-27010: Attribute set with value Senior Member Technical Staff for L1__c
@ in UserEO has invalid precision/scale
```

The workaround for this issue is as follows:

Create UDF as **Drop Down** rather then as **Look Up**.

In step 5, ensure that **Searchable in Picklist** is not selected. Save the form.

In step 12, add UDF on **My Information Page** as **ADF Select One Choice**.

3.1.1.6 Bulk User Modify Does Not Work After Upgrade

Bulk User modify functionality does not work after upgrade.

The workaround for this issue is as follows:

1. Export the following artifact from MDS:

   `/metadata/iam-features-requestactions/model-data/ModifyUserDataset.xml`

2. Change the flag `available-in-bulk="true"` for the following attributes:
   - `User Type`
   - `Role`
   - `User Manager`
   - `Start Date`
   - `End Date`

- usr_timezone
- FA Language

3. Change the length for attribute fax to 4000.
4. Import the `ModifyUserDataset.xml` into MDS.

3.1.1.7 Upgrading Oracle Access Manager 11*g* R1 (11.1.1.5.0) to Oracle Access Management Access Manager 11*g* R2 (11.1.2) on AIX Platform Fails

Upgrading OAM 11.1.1.5.0 to Access Manager 11.1.2 on AIX platform fails. The upgrade appears complete and the first Access Manager Server starts up without any problem. However, subsequent servers fails to start up and shows the following message:

```
<Warning> <Coherence> <BEA-000000> <Oracle Coherence GE 3.7.1.1 <Warning>
(thread=Cluster, member=n/a): This Member(Id=0, Address=XX.XX.XX.XX:9097,
MachineId=6803, Location=site:,machine:XXXXXX,process:3080574,
Role=WeblogicServer) has been attempting to join the cluster using WKA list
[XXXXXX/XX.XX.XX.XX:9095] for 30 seconds without success; this could indicate a
mis-configured WKA, or it may simply be the result of a busy cluster or active
failover.>
<Warning> <Coherence> <BEA-000000> <Oracle Coherence GE 3.7.1.1 <Warning>
thread=Cluster, member=n/a): Delaying formation of a new cluster; waiting for
well-known nodes to respond>
```

Oracle Access Management Access Manager upgrade fails for Java version with the following artifacts:

```
java version "1.6.0"
Java(TM) SE Runtime Environment (build pap6460sr10-20111208_01(SR10))
IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 AIX ppc64-64
jvmap6460sr10-20111207_96808 (JIT enabled, AOT enabled)
J9VM - 20111207_096808
JIT  - r9_20111107_21307ifx1
GC   - 20110519_AA)
JCL  - 20111104_02
```

Oracle Access Management Access Manager requires IBM java version with the following artifacts, as a prerequisite:

```
java version "1.6.0"
Java(TM) SE Runtime Environment (build pap6460sr9fp2-20110627_03(SR9 FP2))
IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 AIX ppc64-64
jvmap6460sr9-20110624_85526 (JIT enabled, AOT enabled)
J9VM - 20110624_085526
JIT  - r9_20101028_17488ifx17
GC   - 20101027_AA)
JCL  - 20110530_01
```

3.1.1.8 Update setdomainenv Before Starting the Oracle Access Management Access Manager Servers

In addition to the steps provided in "Upgrading Oracle Access Manager 11g Release 1 (11.1.1.5.0) Environments" in the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management*, complete the following task before starting the Access Manager domain after upgrading:

1. Go to the following directory:

   On UNIX:

```
cd <OAM_DOMAIN_HOME>/bin
```

On Windows:

```
cd <OAM_DOMAIN_HOME>\bin
```

where

<OAM_DOMAIN_HOME> is the complete path to the Access Manager domain home. The following example shows the complete path:

On UNIX, it is located in the <MW_HOME/user_projects/domains/<oam_domain> directory.

On Windows, it is located in the <MW_HOME\user_projects\domains\<oam__domain> directory.

2. Edit the setDomainEnv file by running the following command:

   On UNIX:

   ```
   vi setDomainEnv.sh
   ```

   On Windows:

   ```
   vi setDomainEnv.cmd
   ```

3. Search for EXTRA_JAVA_PROPERTIES and select the property that looks like the following:

   ```
   EXTRA_JAVA_PROPERTIES="-DOAM_POLICY_FILE=${DOMAIN_
   HOME}/config/fmwconfig/oam-policy.xml -DOAM_CONFIG_FILE=${DOMAIN_
   HOME}/config/fmwconfig/oam-config.xml -DOAM_ORACLE_HOME=${OAM_ORACLE_
   HOME} -Doracle.security.am.SERVER_INSTNCE_NAME=${SERVER_NAME}
   -Does.jars.home=${OAM_ORACLE_HOME}/server/lib/oes-d8
   -Does.integration.path=${OAM_ORACLE_
   HOME}/server/lib/oeslib/oes-integration.jar -Does.enabled=true
   -Djavax.xml.soap.SOAPConnectionFactory=weblogic.wsee.saaj.SOAPConnectio
   nFactoryImpl
   -Djavax.xml.soap.MessageFactory=oracle.j2ee.ws.saaj.soap.MessageFactory
   Impl
   -Djavax.xml.soap.SOAPFactory=oracle.j2ee.ws.saaj.soap.SOAPFactoryImpl
   ${EXTRA_JAVA_PROPERTIES}"

   export EXTRA_JAVA_PROPERTIES
   ```

4. Add -Doam.oes.new=true property before -DOAM_POLICY_FILE. The file looks like the following after making the changes:

   ```
   EXTRA_JAVA_PROPERTIES="-Doam.oes.new=true -DOAM_POLICY_FILE=${DOMAIN_
   HOME}/config/fmwconfig/oam-policy.xml -DOAM_CONFIG_FILE=${DOMAIN_
   HOME}/config/fmwconfig/oam-config.xml -DOAM_ORACLE_HOME=${OAM_ORACLE_
   HOME} -Doracle.security.am.SERVER_INSTNCE_NAME=${SERVER_NAME}
   -Does.jars.home=${OAM_ORACLE_HOME}/server/lib/oes-d8
   -Does.integration.path=${OAM_ORACLE_
   HOME}/server/lib/oeslib/oes-integration.jar -Does.enabled=true
   -Djavax.xml.soap.SOAPConnectionFactory=weblogic.wsee.saaj.SOAPConnectio
   nFactoryImpl
   -Djavax.xml.soap.MessageFactory=oracle.j2ee.ws.saaj.soap.MessageFactory
   Impl
   -Djavax.xml.soap.SOAPFactory=oracle.j2ee.ws.saaj.soap.SOAPFactoryImpl
   ${EXTRA_JAVA_PROPERTIES}"

   export EXTRA_JAVA_PROPERTIES
   ```

3.1.1.9 Authorization Policies Containing No Resources Are Not Extracted

This issue typically affects rolling upgrade customers, upgrading from OAM 11.1.1.3.0 to Oracle Access Management Access Management 11.1.2. Application domains which have authorization policies that contains no resources are not extracted by the `exportAccessData` command during upgrade. This does not impact other application domain extraction. The following error message is shown:

```
SEVERE: Resource :  not found
```

The workaround for this issue is to either remove all authorization policies that contain no resources before upgrading or manually configure them.

3.1.1.10 T2P Failure in an Upgraded Environment

Known issue.

Test to Production (T2P) fails in an environment with OAM, OAAM, or OIN that is upgraded from 11.1.1.5.0 to 11.1.2.0.0.

3.1.1.11 OIM Upgrade: Access Policy Based Provisioning of EBS Resource Does Not Work

Access based provisioning does not work for most of the resource objects created through connector import.

The workaround for this issue is as follows:

Before upgrading OIM schemas, do the following:

1. Log in to the OIM database schema.
2. Run the following SQL scripts:

```
BEGIN
execute immediate 'ALTER table OBJ MODIFY OBJ_ALLOWALL default ''1''';
execute immediate 'ALTER table OBJ MODIFY OBJ_ALLOW_MULTIPLE default
''1''';
execute immediate 'ALTER table OBJ MODIFY OBJ_SELF_REQUEST_ALLOWED
default ''1''';
execute immediate 'ALTER table OBJ MODIFY OBJ_OBJADMINONLY default
''0''';
END;
```

3.1.1.12 TCORGANIZATIONNOTFOUNDEXCEPTION Error While Creating New Organizations

In some specific environment, after upgrading OIM 11.1.1.5.0 to OIM 11.1.2, when you click on the **Create Organization** tab from the Identity Console, you may see this error:

```
TCORGANIZATIONNOTFOUNDEXCEPTION
```

To workaround, close the exception and create a new organization.

3.1.1.13 Forgot User Login Flow Shows System Error

Forgot User Login feature does not work after upgrading to OIM 11.1.2.

The workaround for this issue is as follows:

Create a notification template manually with the following credentials:

1. Log in to the System Administration Console.
2. Select **Notification**.

3. In the search box, search for **ForgottenUsernameNotification**, **PasswordExpiredNotification**, and **PasswordWarningNotification**.
4. Do the following if you do not see any of them listed in the search results:

   ForgottenUsernameNotification:

   a. Select the Create Notification Template. It is located above the search results with a plus icon, next to the pencil icon. The Create Notification Template screen appears.

   b. Enter the following details:

      – **Template Name:** ForgottenUsernameNotification

      – **Available Event:** ForgottenUsername

      – **Encoding:** UTF-8

      – **Message Subject:** Your User Login

      – **Type:** HTML

      – **Short Message:** User Login

      – **Long Message:**

```
<html><head></head>
<body>
<p>
  Your $tenantName user login - $userLoginId
</p>
</body>
</html>
```

   c. Click **Save**.

   PasswordExpiredNotification:

   a. Select the Create Notification Template. It is located above the search results with a plus icon, next to the pencil icon. The Create Notification Template screen appears.

   b. Enter the following details:

      – **Template Name:** PasswordWarningNotification

      – **Available Event:** PasswordWarning

      – **Encoding:** UTF-8

      – **Message Subject:** Password Expiry Warning

      – **Type:** HTML

      – **Short Message:** Password Expiry

      – **Long Message:**

```
<html><head></head>
<body>
<![CDATA[ <p>
Your Password is about to be Expired. Please reset your Password.
        </p><p>
    UserID: %1<br>
    </p><p>
          For any issues, please contact [admin email or phone]
    </p>]]>
```

```
</body>
</html>
```

c. Click **Save**.

PasswordExpiration:

a. Select the Create Notification Template. It is located above the search results with a plus icon, next to the pencil icon. The Create Notification Template screen appears.

b. Enter the following details:

- **Template Name:** PasswordExpiredNotification
- **Available Event:** PasswordExpiration
- **Encoding:** UTF-8
- **Message Subject:** Password Expired
- **Type:** HTML
- **Short Message:** Password Expired
- **Long Message:**

```
<html><head></head>
<body>
<![CDATA[ <p>
Your Password has Expired. Please reset your Password.
         </p><p>
     UserID: %1<br>
     </p><p>
           For any issues, please contact [admin email or phone]
     </p>]]>
</body>
</html>
```

c. Click **Save**.

3.1.1.14 OIM Middle Tier Upgrade Patch Domain Report Shows Error for Foreign JNDI Provide Creation

This issue occurs if you upgrade the middle tier twice, during the OIM 11.1.1.5.0 to 11.1.2 upgrade process. The middle tier upgrade patch domain report shows error for **Foreign JNDI Provide Creation**, eventhough the parameter `oim.domainextension.jndiprovider.patch` is set to `false` in the `oimupgrade.properties` file.

The following is a sample patch domain report displayed when you perform the middle tier upgrade twice:

```
Domain Component                    Status
Foreign JNDI Provider Creation      Error
```

Ignore this error report for **Foreign JNDI Provider Creation**.

3.1.1.15 Matching Rule is Lost During the OIM 11.1.1.5.0 Upgrade

When you upgrade OIM 11.1.1.5.0 to 11.1.2, the customization made for the matching rule is lost.

The workaround for this issue is to redo the customization for the matching rule in OIM 11.1.2.

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)
- Migrating Oracle Adaptive Access Manager 10*g* to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2)
- Migrating Oracle Single Sign-On 10*g* to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2)
- Migrating Sun OpenSSO Enterprise 8.0 to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2)
- Migrating Sun Java System Access Manager 7.1 to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2)
- Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2)
- Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2)
- Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2)

3.2.1 General Issues and Workarounds

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

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

This issue occurs when you upgrade Oracle Single Sign-On 10*g* to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2). 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):

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

3.2.1.3 Migration of J2EE Agent 2.2 is not Supported

Known issue.

Migration of the profile of J2EE Agent 2.2 from Sun Java System Access Manager 7.1 to Oracle Access Management Access Manager 11g release 2 (11.1.2) is not supported, and therefore, the run-time verification support for the same is not available.

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) 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

4

Oracle Identity Management Administration

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

4.1 General Issues and Workarounds

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

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
  ```

- 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
  ```

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 documentation errata and updates for the *Oracle Fusion Middleware Administrator's Guide*:

- In the procedure for moving Oracle Privileged Account Manager to a target environment, the following step is not required:

  If the *ORACLE_HOME* path is different in the source and the target environments, then you must manually update some references in DOMAIN_HOME/config/fmwconfig/opam/-config.xml. These references include lines with bundleJar locations that point to jar files in ORACLE_HOME.

  For example, in a default set-up, the lines with bundleJar references include:

```
<connector bundleJar="ORACLE_HOME/connectors/ldap/bundle/
org.identityconnectors.ldap-1.0.6380.jar" targetType="ldap">
<connector bundleJar="ORACLE_
HOME/connectors/genericunix/bundle/org.identityconnectors.genericunix-1.0.0.jar
"targetType="unix">
<connector bundleJar="ORACLE_HOME/connectors/dbum/bundle/
org.identityconnectors.dbum-1.0.1116.jar" targetType="database">
```

  Ensure that *ORACLE_HOME* is the correct path for the target environment, because the value from a source environment would have been migrated.

  See "Move Oracle Privileged Account Manager to a New Target Environment" in the *Oracle Fusion Middleware Administrator's Guide*.

- In the task "Move Access Manager 11g to a New Target Environment" in the section "Moving Identity Management to a New Target Environment", you need to manually copy the obAccessclient.xml file *only* if you are not also moving WebGate.

- In the task "Move Oracle Identity Manager to a New Target Environment" in the section "Moving Identity Management to a New Target Environment", note the

following and perform edit, if necessary, after you copy exported custom reconciliation profiles to the target system:

If a reconciliation profile is imported in any MDS environment with the attribute configure="true," it automatically generates all the required configuration for that environment and updates this property to false. In this case, after you export this profile from source environment, edit the file and add the configure='true' property before importing to the target environment.

5 Oracle Access Management

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

5.1 General Issues and Workarounds

This section describes general issue and workarounds organized around specific services. To streamline your experience, only services with a 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:

5.1.1 General Issues and Workarounds: Access Manager

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

5.1.1.1 Exception Regarding WebGate Profiles Is Expected

When validating a WebGate 11g profile using the OAM Test Tool, an exception may be displayed on the invoking screen when the test tool connects to the OAM server - even though the screen shows a successful connection. This is expected and can be ignored.

5.1.1.2 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 '/'.

5.1.1.3 Access Manager Server Start Causes Exception Error

When the Access Manger Server is started, an ArmeRUNTIME exception error is thrown.

The exception error does not cause any loss of functionality.

5.1.1.4 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.

5.1.1.5 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.

5.1.1.6 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
```

5.1.1.7 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.

5.1.1.8 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:

- Issues with Searches and Non-English Browser Settings

5.1.2.1 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:

- Requesters, Relying Parties and Issuing Authorities **`Partner Type`** field to **`Requester`**, **`Relying Party`** or **`Issuing Authority`** when the Oracle Access Management Console browser setting is non-English.
- Token Issuance Templates **`Token Type`** to **`Username`** when the Oracle Directory Services Manager browser setting is non-English
- Token Validation Templates **`Token Type`** to **`Username`** when the Oracle Directory Services Manager 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 issue and workarounds for Oracle Access Management Identity Federation (Identity Federation). It includes the following topic:

- Section 5.1.3.1, "Federation Metadata is not Accessible after Upgrade"
- Section 5.1.3.2, "Federation Redirect URLs May be Overwritten in Concurrency Mode"
- Section 5.1.3.3, "Errors when Webgate has Credential Collector Option Enabled"

5.1.3.1 Federation Metadata is not Accessible after Upgrade

After upgrade from PS1 to R2 the new environment also contains identity federation. If you enable identity federation and try to access the federation metadata there is an error.

To work around this problem, issue the following WLST commands:

```
connect('<username>', '<password>', 't3://<host>:port')

domainRuntime()

putStringProperty('/stsglobal/jaxbcontextpath','oracle.security.fed.xml.soap.v
11:oracle.security.fed.xml.soap.v12:oracle.security.fed.xml.security.dsig:orac
le.security.fed.xml.security.enc:oracle.security.fed.xml.security.trust.v12:or
acle.security.fed.xml.security.trust.v13:oracle.security.fed.xml.security.trus
t.v14:oracle.security.fed.xml.ws.addressing.v09:oracle.security.fed.xml.ws.add
ressing.v10:oracle.security.fed.xml.ws.policy.v12:oracle.security.fed.xml.secu
rity.wss.ext.v10:oracle.security.fed.xml.security.wss.ext.v11:oracle.security.
fed.xml.security.wss.policy.v11:oracle.security.fed.xml.security.wss.policy.v1
2:oracle.security.fed.xml.security.wss.utility.v10:oracle.security.fed.xml.sec
urity.saml.v11.assertion:oracle.security.fed.xml.security.saml.v11.protocol:or
acle.security.fed.xml.security.saml.v1x.assertion:oracle.security.fed.xml.secu
rity.saml.v1x.protocol:oracle.security.fed.xml.security.saml.v1x.metadata:orac
le.security.fed.xml.security.saml.v20.assertion:oracle.security.fed.xml.securi
ty.saml.v20.protocol:oracle.security.fed.xml.security.saml.v20.metadata:oracle
.security.fed.xml.security.identity.v10:oracle.security.fed.xml.security.openi
d.v20:oracle.security.fed.xml.security.openid.v20.xrd')
```

5.1.3.2 Federation Redirect URLs May be Overwritten in Concurrency Mode

In concurrency mode where several clients use the Access Manager server for Federation at the same time, the redirect URLs created by Access Manager and the Federation Plugin for a client may be overwritten with the redirect URL created for another client.

5.1.3.3 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.

5.2 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 orkarounds for Oracle Access Management Access Manager (Access Manager). It includes the following topics:

- Section 5.2.1.1, "Enabling OpenSSO Agent Configuration Hotswap"

5.2.1.1 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, "Incorrect Value in the Kerberos Validation Template"
- Section 5.2.2.3, "No Console Support Removing Partner Encryption or Signing Certificates"
- Section 5.2.2.4, "Resource URLs Removed During Create Like (Duplicate) Operation"
- Section 5.2.2.5, "Error Sending USERNAME TOKEN with NONCE"

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 Incorrect Value in the Kerberos Validation Template

In the Security Token Service Kerberos Validation template, the Kerberos Principal No Domain value in the drop down list sets an incorrect value:

Incorrect Value: STS_KERBEROS_NODOMAIN

Correct Value: STS_KERBEROS_PRINCIPAL_NODOMAIN

To use the Kerberos Principal No Domain option the Administrator must select a blank field in drop down list and manually set STS_KERBEROS_PRINCIPAL_ NODOMAIN in the field near the list.

1. From the Oracle Access Management Console System Configuration tab, Security Token Service section, go to Token Validation Template:
2. Click the Add button.
3. Provide a name, select token type as Kerberos and enter other details.
4. In the Token Mapping tab, select Map Token to User from the down list and then enable Enable Simple User Mapping.
5. From User Token Attribute drop down, select Kerberos Principal No Domain: select a blank field in drop down list and manually set STS_KERBEROS_ PRINCIPAL_NODOMAIN in the field near the list.
6. Give a value for the Datastore Attribute and Save.

In oam-config.xml, the User Token Attribute should set STS_KERBEROS_PRINCIPAL_ NODOMAIN as the value.

5.2.2.3 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
```

5.2.2.4 Resource URLs Removed During Create Like (Duplicate) Operation

When using the Security Token Service Create Like (duplicate) button with existing Relying Parties, the URLs listed in the Resource URLs section of the original relying party are removed (but should not be modified).

The Administrator must manually re-enter the necessary URLs, or not use the Create Like button when creating Relying Parties.

5.2.2.5 Error Sending USERNAME TOKEN with NONCE

The following error can be seen in Security Token Service logs when sending USERNAME TOKEN with NONCE:

```
<oracle.security.fed.model.util.rdbms.RDBMSBatchExecutor> <FEDSTS-11013> <SQL
```

Error seen while interacting with the database:

```
java.sql.BatchUpdateException: ORA-12899: value too large for column
"DEV_OAM"."ORAFEDBLOBSTORE"."BLOBID"
```

Have the client send a smaller nonce.

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:

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.

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.

5.2.3.3 Data is Cached in the Keystore Templates Table upon Validation Error

When data entered in the keystore templates table in the Oracle Access Management Console is rejected due to a validation error, the error is shown and the invalid row of the table is not saved.

However, this invalid row is cached in the user interface and closing and reopening the Federation Setting tab does not refresh the data. You must log in again to refresh the data.

5.2.3.4 Cannot Specify Multiple Non-Proxy Hosts for Identity Federation

In the Federation Settings page of the Oracle Access Management Console, the non-proxy hosts field is meant to take a delimited list of non-proxy hosts using a semi-colon (;) separator.

However this field currently does not allow semi-colons (;) in the input characters.

If you need to specify more than one non-proxy host (for example host1 and host2), the workaround is to use WLST as follows:

```
connect(<adminuser>,<adminpassword>,'t3://<HOST_NAME>:<WLS_ADMIN_PORT>')

domainRuntime()

putStringProperty("/fedserverconfig/nonproxyhosts", "host1;host2")
```

5.2.3.5 Invalid IdP is Created if Incorrect Metadata Imported

When creating an IdP with the Oracle Access Management Console, if you choose an invalid Metadata XML file (such as an SP metadata file), you get an error message indicating that the metadata is invalid. The message is as follows:

```
ADFC-10001: cannot instantiate class
'oracle.security.am.fed.oif.managedbeans.idp.EditIDProviderMB'
```

However if you still continue with the task and click **Save**, the IdP is created with the incorrect metadata file and there is an exception in the console, which makes the console unusable until you re-login.

5.2.3.6 WLST Commands for OpenID IdP Partner

The Federation WLST commands to add an OpenID IdP partner are not listed in the WLST Federation help.

The supported commands are:

- `addOpenID20IdPFederationPartner`: Creates an OpenID 2.0 IdP Federation partner
- `addOpenID20GoogleIdPFederationPartner`: Adds Google as an OpenID 2.0 IdP Partner
- `addOpenID20YahooIdPFederationPartner`: Adds Yahoo as an OpenID 2.0 IdP Partner

addOpenID20IdPFederationPartner

The syntax is as follows:

```
addOpenID20IdPFederationPartner(partnerName, ssoURL, discoveryURL,
description)
```

The parameters are as follows:

- `partnerName`=The name of the partner to be created.
- `ssoURL`=The endpoint URL of the IdP (OP).
- `discoveryURL`=The discovery URL of the IdP (OP).
- `description`=Description of the partner. This is optional.

addOpenID20GoogleIdPFederationPartner

The syntax is as follows:

```
addOpenID20GoogleIdPFederationPartner()
```

This command does not take any parameters.

addOpenID20YahooIdPFederationPartner

The syntax is as follows:

```
addOpenID20YahooIdPFederationPartner()
```

This command does not take any parameters.

5.2.3.7 No Console Support for Federation OpenID IdP Partner

The federation IdP partner page, accessed in the Oracle Access Management Console from the System Configuration tab, Identity Federation, Identity Providers, does not provide support for OpenID IdP/OP partners.

As a workaround, you can use the Federation OpenID WLST commands to add an OpenID IdP/OP partner. For details, see Section 5.2.3.6.

5.2.3.8 SSO Error when federationscheme for a Partner Protects a Resource

This issue is seen in the following scenario:

- A Federation IdP partner has been added.
- An Authentication Scheme and Module were created using the Oracle Access Management Console or WLST commands for that IdP partner.
- An authentication policy is created using the newly created Authentication Scheme for that partner.
- A resource is protected with this policy.

Due an incorrect configuration in the newly created Authentication Module for that partner, an error will be seen in the browser and logs.

The workaround is as follows:

1. Log in to the Oracle Access Management Console.
2. Click the **System Configuration** Tab.
3. On left hand side, click **Access Manager**.
4. Expand **Authentication Modules**.
5. Expand **Custom Authentication Module**.
6. Double-click on the new Federation authentication module (*IdPName*FederationPlugin).
7. Go to the **Steps Orchestration** tab in the right hand side.
8. For the drop-down called `Initial Step`, change that to `FedAuthnRequestPlugin`.

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, "Once Set, Jail Breaking "Max OS Version" Setting Cannot be Empty"
- Section 5.2.4.2, "Additional Configuration Required After Running Test-to-Production Scripts"

5.2.4.1 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.

5.2.4.2 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

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

- Oracle Fusion Middleware Administrator's Guide for Oracle Access Management
- Oracle Fusion Middleware Developer's Guide for Oracle Access Management

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

The description of the Max Session Time element in Chapter 13, Registering and Managing OAM 11g Agents has been updated.

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

There are no documentation issues in the Oracle Fusion Middleware Developer's Guide for Oracle Access Management.

6

Oracle Adaptive Access Manager

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

6.1 General Issues and Workarounds

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

6.1.1 "Last Used On" Column Does Not Sort in Fingerprint Details Page

Due to a bug, you cannot sort on the "Last Used On" column for the tabs in the Fingerprint Detail.

6.1.2 ADF Exceptions When Incorrect Password Entered for OAAM Admin

When a user tries to log in to the OAAM Admin Console with incorrect passwords, ADF exceptions appear in the log. They do not impact the functionality.

6.1.3 Session Alert Message is Hard-Coded and Not Translated

The alert messages in the standard policies packaged with Oracle Adaptive Access Manager support a number of languages. However, the alert messages are not globalized.

The Oracle BI Publisher report **RecentLogins** is impacted by this issue. The alert messages from the out-of-the-box policies that appear in the **RecentLogins** report will not follow the report's locale settings.

6.2 Scheduler Issues and Workarounds

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

6.2.1 Altering the Schedule Parameters Does Not Affect Next Recurrence

Altering the schedule parameters of a Scheduled Task does not have any effect for the next recurrence if the start date/time is not changed.

6.2.2 Pause and Cancel Job Status Does Not Appear in Job Instance Tab

The Pause and Cancel Job statuses are not shown in the Job Instance tab when a job is canceled or paused.

6.3 Audit and Reporting Issues and Workarounds

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

6.3.1 Commit Snapshot Diff Event Detail Truncated

The Commit Snapshot Diff event detail does not fit entirely into the data field because event logs are part of the audit information. Since snapshot data can be large, it is not practical to log all data to the audit log. Hence for audit purpose, data that is larger than the available audit event data space may appear truncated in the audit event.

6.3.2 BI Publish 11*g* Search Transaction Report Issues

The following are issues in the BI Publisher Search Transactions Report:

- When all transaction types are selected, the common Transaction and Entity fields should be available in the drop down lists. In BI Publisher, the drop down lists are empty when a specific transaction type is not selected.
- The Transaction field, Transaction Value field, Entity field, and Entity Value field may not be intuitive to the user. For example, when the user selects an attribute from the Transaction field, he must enter the value in the Transaction Value field when there is another Transaction Value 2 field. Incorrect results are displayed if the values are interchanged.
- Transaction 2 field does not have a drop down lists. The user is unable to manually enter the attribute if he wants to search by the second Transaction field.
- The results page does not display the searched attributes. For example, the user searches by Entity Field: Creditcard Number with Value:1111. The credit card information is not available in the results page. The Session ID and Transaction ID are shown as hyperlinks and when clicked, the user is redirected to an error page.

6.4 Configuration Issues and Workarounds

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

6.4.1 Linked Entities and the Order of Configuration

The transaction definition is not updated when linking an entity to one that has been added to a transaction. The workaround is to configure the transaction definition in this order:

1. Configure entities.
2. Link entities.
3. Add entity instances to transactions.

6.4.2 SP2-0606 Error Generated for Loading OAAM Partition Schemas

While loading the OAAM partition RCU schemas, the following error messages are generated in the `oaam_partn.log` :

```
SP2-0606: Cannot create SPOOL file "db_setup.lis"
SP2-0606: Cannot create SPOOL file "cr_vcrypt_obj.lis"
SP2-0606: Cannot create SPOOL file "vr_policy_init.lis"
SP2-0606: Cannot create SPOOL file "v_user_init.lis"
SP2-0606: Cannot create SPOOL file "v_scorepolicy.lis"
SP2-0606: Cannot create SPOOL file "cr_v_Q_global.lis"
SP2-0606: Cannot create SPOOL file "cr_vcrypt_config.lis"
SP2-0606: Cannot create SPOOL file "cr_v_ans_hint.lis"
SP2-0606: Cannot create SPOOL file "cr_v_b_locale.lis"
SP2-0606: Cannot create SPOOL file "oaam_db_patch_oracle_10_1_4_5_01.log"
SP2-0606: Cannot create SPOOL file "oaam_db_patch_oracle_10_1_4_5_02.log"
SP2-0606: Cannot create SPOOL file "create_monitor_rollup.lst"
SP2-0606: Cannot create SPOOL file "oaam_db_patch_oracle_10_1_4_5_07.log"
```

The error message occurs because the spooling of the OAAM partition to the file does not occur. Functionality is not impacted and the message can be safely ignored.

6.4.3 Input for Create_Purge_Proc.SQL

When running the `create_purge_proc.sql` script, you will be asked to:

```
Enter value for oaam_data_tbs
Enter value for oaam_indx_tbs
```

The two values to enter are as follows:

```
Enter value for oaam_data_tbs: <SchemaPrefix>_BRSADATA
```

```
Enter value for oaam_indx_tbs: <SchemaPrefix>_BRSAINDX
```

You can find these values by executing the following query as an OAAM schema user:

```
select tablespace_name from user_tablespaces;
```

6.4.4 OAAM Command Line Scripts May Fail

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

Due to a bug, under certain circumstances, the OAAM command line scripts may fail.

If the OAAM command line script fails to launch, execute the script as follows:

bash *script_name*

6.4.5 Setting Up the CLI Environment

Due to a bug, as part of setting up the CLI environment, users must execute the following command on the command line from the CLI working directory:

```
chmod 750 findjar.sh
```

6.4.6 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`.

7

Oracle Entitlements Server

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

- General Issues and Workarounds
- Configuration Issues and Workarounds
- Documentation Errata

7.1 General Issues and Workarounds

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

- Tomcat Security Module Fails To Load Custom Attribute Retriever Class
- Duplicate Entries of Resource Objects
- Finding Default Oracle Entitlements Server Security Module Certificates
- Entitlements Server Does Not Recover Connection To Database
- Policy Simulator Does Not Open Policies Correctly
- Starting Oracle Access Manager When Protected by Entitlements Server Throws Exception
- Updating the Opatch Tool

7.1.1 Tomcat Security Module Fails To Load Custom Attribute Retriever Class

The Attribute Retriver Interface resides in the JPS JARs which are loaded by the Tomcat "shared" class loader. Thus, JARs that contain your Custom Attribute Restriver 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.

7.1.2 Duplicate Entries of Resource Objects

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

7.1.3 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.

7.1.4 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.

7.1.5 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.

7.1.6 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.

7.1.7 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*.

7.2 Configuration Issues and Workarounds

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

7.2.1 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.

7.2.2 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`.

7.2.3 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.

7.3 Documentation Errata

There are no documentation errata for this release.

8

Oracle Fusion Middleware High Availability and Enterprise Deployment

This chapter describes issues associated with High Availability and Enterprise Deployments.

It includes the following topics:

- Section 8.1, "General Issues and Workarounds"

8.1 General Issues and Workarounds

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

- Section 8.1.1, "Exception When Running LDAPConfigPostSetup.sh"
- Section 8.1.2, "JRockit Install Fails on Some Linux Versions"

8.1.1 Exception When Running LDAPConfigPostSetup.sh

When you run the script `LDAPConfigPostSetup.sh` to configure Oracle Identity Manager, as described in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*, Section 12.15, "Configuring Oracle Identity Manager to Work with the Oracle Web Tier," you might see the following exception in the log file:

```
java.lang.ClassNotFoundException:
oracle.as.jmx.framework.standardmbeans.spi.JMXFrameworkProviderImpl
```

This exception is harmless and can safely be ignored.

8.1.2 JRockit Install Fails on Some Linux Versions

When you attempt to install JRockit, as described in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*, Section 8.2.1.1, "Installing JRockit," the installation might fail due to a JVM crash. This has been observed with Linux 6u2, specifically:

Linux slc04ugo 2.6.39-100.5.1.el6uek.x86_64 #1 SMP Tue Mar 6 20:26:00 EST 2012 x86_64 x86_64 x86_64 GNU/Linux

To resolve this issue, update to Oracle Linux 6.3.

9

Oracle Privileged Account Manager

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

9.1 General Issues and Workarounds

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

9.1.1 Some of the Target Page Strings Will Not be Translated

Some strings on the Targets page in the Administrator user interface will not be translated because those strings are not externalized on the Oracle Privileged Account Manager server side.

9.1.2 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.

9.1.3 Create Target in OPAM Does Not Work When Browser Locale=German

If you select the German locale when creating a new target on any browser, the `Connection to OPAM server could not be established:` error message will display. This issue does not occur with any other locales.

To workaround this issue, select English as the preferred language.
For example, using Firefox, the steps are as follows:

1. Open the Firefox browser window and select **Tools** > **Options**.

2. When the Options dialog displays, select the **Content** icon.
3. On the Content page, locate the Languages section and click **Choose**.
4. When the Languages dialog displays, select **English** and then click **Move Up** until English is at the top of the language list.

   Note: If English is not visible in the Languages list, click the **Select a language to add** button. Locate and select **English**, then click the **Add** button.

5. Click **OK** to close the dialog boxes.

9.1.4 OPAM Console Cannot Find Users from Identity Store Configured in WebLogic

In the Oracle Privileged Account Manager Console, accounts can be granted to users from the WebLogic Identity Store. The Oracle Privileged Account Manager Console provides a user interface to look up users from the primary Identity Store (first on the list of Providers in the WebLogic Security Realm configuration).

Oracle Privileged Account Manager Console user look-ups can fail for the following reasons:

- The user may not be part of the first Identity Store Provider in WebLogic Security Realm.
- Service-Oriented Architectures (SOA) (Oracle Identity Manager with SOA) and Oracle Privileged Account Manager have been configured in the same WebLogic domain.

  Installing SOA alters the Identity Store configuration in the JPS default context, which causes user look-up failures in other components such as Oracle Privileged Account Manager.

Solution:

- Check that the list of Providers is ordered correctly in the WebLogic Security Realm configuration, and verify that the user is part of the first Provider listed. If not, then re-order the Provider list appropriately.
- Check whether SOA and Oracle Privileged Account Manager are configured on same WebLogic domain. If so, the workaround is to configure SOA and Oracle Privileged Account Manager in separate domains.

9.2 Configuration Issues and Workarounds

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

- Section 9.2.1, "Use Absolute Paths While Running configureSecurityStore.py With -m Join"

9.2.1 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.

9.3 Documentation Errata

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

- Section 9.3.1, "Clarify Locating the Oracle Privileged Account Manager Connector Bundles"
- Section 9.3.2, "Update to opam-config.xml File Location"
- Section 9.3.3, "Update to opam-config.xsd Information"
- Section 9.3.4, "Unsupported Database Target Types Noted in Oracle Privileged Account Manager Admin Guide"

9.3.1 Clarify Locating the Oracle Privileged Account Manager Connector Bundles

The following sentence in section 3.2.2, "Locating the Oracle Privileged Account Manager Connector Bundles," in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*,

"The connector bundles shipped with Oracle Privileged Account Manager include:"

should be revised to read as follows:

"The connectors that are pushed into ORACLE_HOME/connectors are actually shipped with Oracle Identity Manager. Of all the connectors in this directory, only the following three connectors are certified with Oracle Privileged Account Manager for this release:"

9.3.2 Update to opam-config.xml File Location

The following sentence in section 3.2.3, "Consuming ICF Connectors," in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*

"During domain creation, the opam-config.xml file is copied to the DOMAIN_HOME/config/fmwconfig directory, and this file is applicable for that domain."

should be revised to read as follows:

"During domain creation, the opam-config.xml file is copied to the DOMAIN_HOME/config/fmwconfig/opam directory, and this file is applicable for that domain."

9.3.3 Update to opam-config.xsd Information

The following paragraph in section 3.2.3, "Consuming ICF Connectors," in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*,

"The opam-config.xsd file (also located in the ORACLE_HOME/opam/config directory) describes the schema for opam-config.xml. If any changes are made to DOMAIN_HOME/config/fmwconfig/opam-config.xml, it should verified with the opam-config.xsd file."

should be revised to read as follows:

"The opam-config.xsd file (also located in the ORACLE_HOME/opam/config directory) describes the schema for opam-config.xml. If any changes are made to DOMAIN_

`HOME/config/fmwconfig/opam/opam-config.xml`, it should verified with the `opam-config.xsd` file."

9.3.4 Unsupported Database Target Types Noted in Oracle Privileged Account Manager Admin Guide

Information provided for the **Database Connection URL** parameter in Table 5-2, "Basic Configuration Parameters for Targets" in section 5.1.2.2 of the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager* is incorrect.

Oracle Privileged Account Manager only supports Oracle target systems for the 11.1.2.0.0 release. The entry should not include the MSSQL, MySQL, DB2, or Sybase examples.

10 Oracle Identity Navigator

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

- General Issues and Workarounds

10.1 General Issues and Workarounds

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

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

10.1.1 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.

11

Oracle Identity Governance Framework

This chapter describes issues associated with Oracle Identity Governance Framework. There are no known issues at this time.

12

Oracle Identity Manager

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

12.1 Patch Requirements

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

12.1.1 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/`

12.1.2 Patch Requirements for Oracle Database 11g (11.1.0.7)

Table 12–1 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 12–1 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 12–1 are also available by the same names for Solaris SPARC 64 bit.

12.1.3 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 12–2 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 12–2 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.

12.1.4 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 12–3:

Table 12–3 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)

12.1.5 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 12-1 for information about downloading OPatch from My Oracle Support.

12.1.6 Patch Requirement for SOA Email Notification

The following patch resolves the known issue with SOA email notification:

Patch number 15211191 on My Oracle Support - Apply this patch on the SOA server to resolve the known issue described in "Deep Linking of Identity URL in SOA Email Notification Does Not Work".

The description of this patch on My Oracle Support is "EMAIL NOTIFICATION DOESN'T EMBED URL PROPERLY IF IT CONTAINS /IDENTITY".

12.1.7 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

12.2 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
- Modification of Disabled Account and Requesting Entitlement for the Account is Allowed

12.2.1 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.

12.2.2 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 12–1, 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 12–1 Sample ldif File

```
dn: cn=AJGroupSUJA2,cn=Groups,dc=oracle,dc=com
changetype: modify
replace: displayName
displayName: All Fusion Roles - All Data RolesSUJA2

dn: cn=AJGroupSUJA2,cn=Groups,dc=oracle,dc=com
changetype: modify
replace: displayName;lang-zh-tw
displayName;lang-zh-tw: languser1RolesSUJA21-Chinese

dn: cn=AJGroupSUJA2,cn=Groups,dc=oracle,dc=com
changetype: modify
replace: displayName;lang-fr
displayName;lang-fr: languser1RolesSUJA-French

dn: cn=AJGroupSUJA2,cn=Groups,dc=oracle,dc=com
changetype: modify
replace: displayName;lang-ja
displayName;lang-ja: languser1RolesSUJA-Japanese1
```

12.2.3 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.

12.2.4 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.

12.2.5 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. Remove the HTTPS port.

Note: HTTPS port and hostname can be configured directly in the SOA composite, and the configuration should follow the installation topology.

12.2.6 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.

12.2.7 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.

12.2.8 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.

12.2.9 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.

12.2.10 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=oracle,dc=com
cn=FusionUsers,cn=USA,dc=us,dc=oracle,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=oracle,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 oracle.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.

12.2.11 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*.

12.2.12 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.

12.2.13 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.

12.2.14 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.

12.2.15 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.

12.2.16 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.

12.2.17 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.

12.2.18 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.

12.2.19 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=oracle,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=oracle,dc=com'.
  5. Click **Save/Apply**.
  6. Retry the role grant.

12.2.20 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.

12.2.21 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.

12.2.22 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.

12.2.23 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.

12.2.24 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.

12.2.25 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.

12.2.26 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.

12.2.27 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.

12.2.28 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.

12.2.29 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.

12.2.30 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*.

12.2.31 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.

12.2.32 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%**).

12.2.33 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.

12.2.34 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.

12.2.35 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.

12.2.36 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.

12.2.37 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.

12.2.38 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.

12.2.39 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.

12.2.40 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.

12.2.41 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.

12.2.42 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.

12.2.43 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.

12.2.44 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.

12.2.45 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.

12.2.46 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.

12.2.47 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).

12.2.48 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.

12.2.49 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.

12.2.50 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.

12.2.51 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.

12.2.52 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>

12.2.53 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.

12.2.54 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.

12.2.55 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.

12.2.56 Duplicate Rows in Request Tracking

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

12.2.57 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.

12.2.58 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.

12.2.59 Approver Cannot Approve Request From Request Details Page

When a request is created for enable user, disable user, delete user, and so on, which does not have a cart item or form associated to it, the approver will not be able to take action on the request from the Request Details page.

To workaround this issue, verify the request information using the request details page, but perform the necessary approval action directly from the Pending task list.

12.2.60 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.

12.2.61 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.

12.2.62 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.

12.2.63 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.

12.2.64 Accessibility Compliance

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

12.2.65 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.

12.2.66 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.

12.2.67 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.

12.2.68 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.

12.2.69 Application Instance Administrator Cannot Create Forms

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

12.2.70 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.

12.2.71 AD Groups Associated to the Account Not Reconciled

When Active Directory reconciliation is run, the AD groups that are associated to the account are not reconciled to the AD child table.

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

12.2.72 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.

12.2.73 Organization UDF Not Supported

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

12.2.74 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.

12.2.75 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.

12.2.76 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.

12.2.77 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.

12.2.78 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.

12.2.79 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.

12.2.80 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.

12.2.81 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.

12.2.82 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.

12.2.83 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.

12.2.84 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 componets.
3. Setup the partial rendering of the component.

12.2.85 Number Type Lookup Code Not Supported

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

12.2.86 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.

12.2.87 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.

12.2.88 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.

12.2.89 Pending Approvals Page Customization Causes Browser to Hang

In the Pending Approvals page, when you click Customize and select the Source that you want to hide from the My Task tab, the Web browser stops responding.

12.3 Configuration Issues and Workarounds

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

12.3.1 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

12.3.2 Benign Connection Error From OIA For SoD Chek

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.

12.3.3 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.

12.3.4 Oracle Identity Manager Fails to Find orclPwdExpirationDate

When Oracle Identity Manager is configured with libOVD/OID and OAM integration is enabled, 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.

12.4 Multi-Language Support Issues and Limitations

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

12.4.1 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.

12.4.2 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.

12.4.3 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.

12.4.4 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.

12.4.5 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.

12.4.6 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.

12.4.7 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.

12.4.8 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.

12.4.9 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.

12.4.10 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.

12.4.11 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.

12.4.12 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.

12.4.13 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.

12.4.14 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.

12.5 Documentation Errata

Currently, there are no documentation issues to note.

13

IdM Integration

This chapter contains release note items for Oracle Identity Management component integrations.

Topics include:

- Section 13.1, "Configuration and Integration Issues and Workarounds"
- Section 13.2, "Documentation Errata"

13.1 Configuration and Integration Issues and Workarounds

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

- setupOAMTapIntegration.sh Fails to Run on OEL6
- Authentication Results in Two User Sessions
- Setting Up the CLI Environment in Access Manager-OAAM and Access Manager-OAAM-OIM Integrations
- generateOTP() API Has Been Deprecated

13.1.1 setupOAMTapIntegration.sh Fails to Run on OEL6

When the setup script setupOAMTapIntegration.sh is launched on the OEL 6 platform, it fails with following error:

```
setupOAMTapIntegration.sh: line 13: source: setCliEnv.sh: file not found
-Djava.security.policy=conf/jmx.policy -classpath
oracle.oaam.integration.asa.IntegrationUtil setupOAMTapIntegration
readFromFile=conf/bharosa_properties/oaam_cli.properties
setupOAMTapIntegration.sh: line 21: -Djava.security.policy=conf/jmx.policy:
No such file or directory
```

To resolve this problem, launch the script as follows:

```
bash script_filename
```

13.1.2 Authentication Results in Two User Sessions

In an Access Manager-OAAM-OIM integrated environment, any authentication results in two user sessions being created in Oracle Access Management Access Manager (visible in Oracle Access Management Console under Session Management, and in the `OAM_SESSIONS` table in MDS).

One session is created by the IAMSuiteAgent (which is configured in OAAM as the Java agent as part of the OAAM-Access Manager configuration); and the other session is created by the actual WebGate within the Oracle HTTP Server (OHS) web tier.

13.1.3 Setting Up the CLI Environment in Access Manager-OAAM and Access Manager-OAAM-OIM Integrations

During the set up of Access Manager and Oracle Adaptive Access Manager, the `setupOAMTapIntegration` script fails with a `NoClassDefFoundError` error. To work around this issue, when setting up the CLI environment in the Access Manager and OAAM and Access Manager-OAAM-OIM integrations, execute the following command on the command line from the CLI working directory:

```
chmod 750 findjar.sh
```

13.1.4 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*.

13.2 Documentation Errata

This section contains documentation errata and updates for the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*, Part Number E27123-01. Topics include:

- Additional Properties for preConfigIDStore and prepareIDStore
- Login through /oaam_server No Longer Works After OAAM and Access Manager TAPScheme Integration
- Incorrect Setting for bharosa.uio.proxy.mode.flag Causes OAAM and Access Manager 11g Integration to Fail
- IDContext Claims in the Access Manager-OAAM TAP Integration
- OAAM Password Length Limited to 25 Characters

13.2.1 Additional Properties for preConfigIDStore and prepareIDStore

This update applies to sections 2.4.1 preConfigIDStore Command and 2.4.2 prepareIDStore Command.

An additional property, IDSTORE_ADMIN_PORT, must be specified when using the preConfigIDStore command or the prepareIDStore command and the targeted identity store is an instance of Oracle Unified Directory (OUD). This property is required to connect to and configure the OUD identity store.

For example, you would set this property as follows in the properties file:

```
IDSTORE_ADMIN_PORT: 4444
```

Additionally, the properties IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the SSL connection to the OUD identity store.

13.2.2 Login through /oaam_server No Longer Works After OAAM and Access Manager TAPScheme Integration

This update applies to section 8.7 Troubleshooting Common Problems.

After a standard installation of both OAAM and Access Manager and then performing the OAAM and Access Manager TAPScheme integration steps, the URL `/oaam_server` is no longer able to authenticate any users.

When the user navigates to the URL and enters his username, he is directed to the page where he enters his password. After submitting the password, the login fails and the following error is displayed:

```
Error Sorry, the identification you entered was not recognized. Please try again
```

There is no workaround. The URL `/oaam_server` is not intended for use with OAAM and Access Manager integration using the TAP scheme. The URL is used for testing the OAAM configuration before proceeding with the integration steps. After integration, the user should not have direct access to the OAAM Server.

13.2.3 Incorrect Setting for bharosa.uio.proxy.mode.flag Causes OAAM and Access Manager 11g Integration to Fail

This update applies to section 8.7 Troubleshooting Common Problems.

OAAM and Access Manager integration using TAP fails with the following message:

```
Sorry, the identification you entered was not recognized.
```

Access Manager and OAAM integration using TAP fails when you integrate Access Manager using TAP and also customize OAAM using the OAAM extensions shared library and you set the property `bharosa.uio.proxy.mode.flag` to `true`. If you integrate and customize using the shared library, you must set the property to `false`.

13.2.4 IDContext Claims in the Access Manager-OAAM TAP Integration

To use IDContext claims in the Access Manager and OAAM TAP integration, follow the below steps:

1. In `<Domain-home>/config/fmw-config/oam-config.xml`, search for the setting with the `TAP partner name`. You would have specified the `TAP Partner name` while registering the TAP partner for Access Manager. For example, `OAAMPartner`. Change the OAAM partner's TapTokenVersion from `v2.0` to `v2.1`.
2. Change the version setting on the OAAM side from `v2.0` to `v2.1` by adding/editing a property through the OAAM Admin Console. To do this, proceed as follows:
   a. Log in to the OAAM Admin Console.
   b. In the navigation tree, click **Environment** and double-click **Properties**. The Properties search page is displayed.
   c. Search for property with name `oaam.uio.oam.dap_token.version` and set its value to `v2.1`.
   d. In case the property does not exist, add a new property with the name `oaam.uio.oam.dap_token.version` and the value as `v2.1`.
3. In the TAP Scheme of the Access Management policy, add the following challenge parameter:

TAPOverrideResource=http://IAMSuiteAgent:80/oamTAPAuthenticate. To do that, proceed as follows:

a. Log in to the Oracle Access Management Console.

b. Click the **Policy Configuration** tab to the left of the screen.

c. In the navigator tree, expand the **Authentication Schemes** node.

d. Double-click **TAPScheme** authentication scheme.

e. To add another parameter to an existing parameter, position your cursor in the **Challenge Parameter** field and press **Enter** using your keyboard.

f. In the new line, add TAPOverrideResource=http://IAMSuiteAgent:80/oamTAPAuthenticate for a challenge parameter of TAPScheme.

13.2.5 OAAM Password Length Limited to 25 Characters

When users logs in to OAAM server for the first time, and they enter a password more than 25 bytes, they are returned to the page for the user name with an error that their password was invalid.

OAAM accepts a limit of 25 characters for passwords.

To work around this issue, update the character limit specified by the following property in the oaam_cli.properties file:

```
bharosa.authentipad.textpad.datafield.maxLength
```

For existing deployments, you can update this property value using the OAAM Administration Console or shared library.