Oracle® Fusion Middleware

Release Notes for Identity Management

11*g* Release 2 (11.1.2.3)

E54495-10

July 2018

Contains information on installing, upgrading, configuring, and administering Oracle Identity Management products. Also includes information about known software issues and their workarounds for this release.

Oracle Fusion Middleware Release Notes for Identity Management, 11*g* Release 2 (11.1.2.3)

E54495-10

Copyright © 2001, 2018, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1 Introduction

2 Installation and Configuration Issues for Oracle Identity and Access Management

3 Upgrade and Migration Issues for Oracle Identity and Access Management

4 Oracle Fusion Middleware Administration

5 Oracle Access Management

6 Oracle Entitlements Server

7 Oracle Adaptive Access Manager

8 Oracle Mobile Security Suite

9 Oracle Privileged Account Manager

10 Oracle Identity Manager

11 Oracle Identity Management Integration

12 High Availability and Enterprise Deployment

Preface

This preface includes the following sections:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions

Audience

This document is intended for users of Oracle Fusion Middleware 11*g* Release 2 Patch Set 3 (11.1.2.3).

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 2 Patch Set 3 (11.1.2.3)*
- 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 Release Notes for Identity Management, 11*g* Release 2 (11.1.2.3).

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 Help Center.

`http://docs.oracle.com/en/`

1.2 Purpose of this Document

This document contains the release information for Oracle Fusion Middleware 11*g* Release 2 (11.1.2.3). 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 information.

1.4.1 Where to Find Oracle Fusion Middleware Certification Information

The latest certification information for Oracle Fusion Middleware 11*g* Release 2 (11.1.2.3) 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 Regarding Websphere Application Server Support

Oracle Identity Management no longer supports servers running on Websphere Application Server. See the Oracle Fusion Middleware support matrix for the most current supported system configurations. A direct link to the support matrix is in Section 1.4.1, "Where to Find Oracle Fusion Middleware Certification Information."

1.4.3 Certification Exceptions

This section describes known issues (exceptions) and workarounds associated with Oracle Fusion Middleware 11g certifications. For a list of known issues associated with specific Oracle Fusion Middleware 11*g* Release 2 (11.1.2.3) components, see the Release Notes chapter for that component. This section contains the following topics:

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

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

1. Apply patch 8897382 to fix bug 8897382.

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

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

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

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

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

1.4.3.2 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.

1.4.3.3 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.

1.4.3.4 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.

1.4.3.5 OIM Installation on Oracle Database 12c with Non-CDB Requires Execution of xaview.sql Script

To create the Oracle Identity Manager (OIM) schema on Oracle Database 12*c* with non-container database (non-CDB), you must execute the database's `xaview.sql` script to create `XAVIEW` objects on the database prior to running RCU. These objects are required to create the Oracle Identity Manager schema.

For Oracle Database 10*g* and 11*g* databases, these objects are automatically created by RCU if they are not already in place. Oracle Database 12*c* databases have a new `XAVIEW` structure that requires the explicit creation of these objects.

To create these objects on Oracle Database 12*c*, perform the following steps before running RCU to create the OIM schema:

1. Log on to sqlplus as the `SYS` database user.
2. Execute the following command:

   ```
   @xaview.sql
   ```
   The `xaview.sql` script resides in the *`ORACLE_HOME`*`/rdbms/admin` directory. *`ORACLE_HOME`* is the Oracle home directory on the database host where the database is installed.

1.4.3.6 Oracle Database 12c (12.1.0.x) with PDB is not Supported in 11g Release 2 (11.1.2.3)

Oracle Database 12*c* (12.1.0.x) database with PDB (pluggable database) is not supported in Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3). Non-container database (Non-CDB) is the only supported database type for this release.

1.5 Restrictions on Specific Browsers

The following browser issues have been observed.

- Internet Explorer Browser Goes Blank When Adding Portlets in Oracle Webcenter
- Unable to View the Output of a JSPX Page in Internet Explorer 7
- Unable to View the Output of SVG files in Internet Explorer 7
- Java Plugin for Discoverer Plus Not Downloaded Automatically on Firefox
- Viewer Plugin Required On Safari 4 To View Raw XML Source

1.5.1 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 until 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.

1.5.2 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.

1.5.3 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/`.

1.5.4 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.

1.5.5 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.

1.6 Downloading and Applying Required Patches

After you install and configure Oracle Fusion Middleware 11*g* Release 2 (11.1.2.3), 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 available at the time these Release Notes were published.

> **Note:** There are some mandatory patches that must be applied for installing and configuring Oracle Identity Manager. For information about these patches, see Section 1.6.1, "Mandatory Patches Required for Installing Oracle Identity Manager."
>
> Along with the Oracle Identity Manager patches, some of the Oracle Database versions require patches. To identify the patches required for Oracle Identity Manager 11*g* Release 2 (11.1.2.3) configurations that use Oracle Databases, see Section 10.1, "Patch Requirements."

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

Oracle Fusion Middleware Product or Component	Bug/Patch Number	Description
Oracle Virtual Directory	16943171	This patch is critical if you are using Oracle Unified Directory in active-active mode, as shown in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*. Failure to apply this patch might result in data inconsistency in the event of a failover.
Oracle IDM Tools	17008132	This patch corrects ACI issues affecting Oracle Unified Directory.
Oracle WebLogic Server	14182177	Fixes the error: `StuckThreads in AdminServer`.
Oracle Unified Directory	18461856	Fixes "Run LDAP User Create and Update Reconciliation job" failure.
Oracle Identity Manager	23172221	Fixes the error: `When user tries to login for the the first time, after setting up challenge questions and password, the user is asked to login again.`

1.6.1 Mandatory Patches Required for Installing Oracle Identity Manager

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

> **Note:** This section provides the mandatory patches that were available at the time of publishing the release notes. For additional changes and revised patch requirements, see My Oracle Support Document ID 1966494.1.

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

For information about any additional patches that you might have to apply, see Section 1.6, "Downloading and Applying Required Patches."

Table 1–2 Patches Required to Fix Specific Issues with Oracle Identity Manager 11g Release 2 (11.1.2.3.0)

Oracle Fusion Middleware Product or Component	Patch Number/Name	When to Apply?	Description
Oracle WebLogic Server	18398295	After installing Oracle Identity and Access Management	This Oracle WebLogic Server patch is required only if you are using Multi Byte Character Set. Follow the `README.txt` file for patching instructions.
Oracle WebLogic Server	14404715	After installing Oracle Identity and Access Management	This is a mandatory Oracle WebLogic Server patch. Follow the `README.txt` file for patching instructions.
Oracle WebLogic Server	16844206	After installing Oracle Identity and Access Management	This is a mandatory Oracle WebLogic Server patch. Follow the `README.txt` file for patching instructions.
Oracle WebLogic Server	13964737	After installing Oracle Identity and Access Management	This is a mandatory Oracle WebLogic Server patch when running WebLogic Server with Oracle JDK 7 Update 40 or later. Follow the `README.txt` file for patching and post-patching instructions. After you apply this patch, you must start the Node Manager with Java Secure Socket Extension (JSSE) enabled. To start the Node Manager with JSSE enabled, see "Set the Node Manager Environment Variables" in *Node Manager Administrator's Guide for Oracle WebLogic Server*. After starting Node Manager with JSSE enabled, you must start the WebLogic Administration Server and Managed Servers with JSSE enabled. For more information, see "Using the JSSE-Enabled SSL Implementation" in *Securing Oracle WebLogic Server*.
Oracle WebLogic Server	20780171	After installing Oracle Identity and Access Management	This is a mandatory Oracle WebLogic Server patch when running WebLogic Server with Oracle JDK 7. Follow the `README.txt` file for patching instructions.
Oracle WebLogic Server	13351178	After installing Oracle Identity and Access Management	This is a mandatory Oracle WebLogic Server patch. Follow the `README.txt` file for patching instructions.
Oracle Identity and Access Management Life Cycle Management (LCM) Tools	22083030	After installing Oracle Identity and Access Management LCM Tools	This Oracle Identity and Access Management LCM Bundle Patch 11.1.2.3.160419 patch is required if you are using the LCM Tools. Follow the `README.txt` file for patching instructions.

Table 1–2 (Cont.) Patches Required to Fix Specific Issues with Oracle Identity Manager 11g Release 2 (11.1.2.3.0)

Oracle Fusion Middleware Product or Component	Patch Number/Name	When to Apply?	Description
Oracle Identity and Access Management	22675286	After installing Oracle Identity and Access Management	This is a mandatory Oracle Identity Management Suite Bundle Patch 11.1.2.3.160419 patch. Follow the `README.txt` file for patching instructions.
Oracle Identity Manager	23172221	After installing Oracle Identity and Access Management	This is a mandatory Oracle Identity Manager patch. Follow the `README.txt` file for patching instructions.

To download the patches, do the following:

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

Patching Instructions

The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

1.7 Licensing Information

Licensing information for Oracle Fusion Middleware is available at:

`http://oraclestore.oracle.com`

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

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

2

Installation and Configuration Issues for Oracle Identity and Access Management

This chapter describes issues associated with the installation and configuration process of Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3). It includes the following sections:

- Installation Issues and Workarounds
- Configuration Issues and Workarounds

2.1 Installation Issues and Workarounds

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

- While preparing the hosts for IDM deployment using IDMLCM tool, you must install the Linux *lsb_release* packages. In the absence of the *lsb* Linux packages, pre-verify if the respective host fails and the failure can be confirmed from the log file *IDMLCM_HOME/provisioning/logs/<machine-name>/healthcheck-error/logs/healthchecker/IDM_<machine-name>-PreInstallChecks_mandatory_<timestamp>.log*

  The log file has an error similar to:

  ```
  java.util.concurrent.ExecutionException: java.io.IOException: Cannot
  run program "lsb_release": error=2, No such file or directory
  
  at java.util.concurrent.FutureTask.report(FutureTask.java:122)
  ```

- If IDMLCM is used for deployment and if a user prepares and configures the directory manually (not using the option Prepare Directory using IDMLCM), it is recommended to configure the system users and groups with the same names that is shipped in the sample input file for preparing directories.

  This file is available at *idmlcm_home/existing_directory/idmtools/input_parameters.properties*.

  If non-compliant with the suggested user and group names you might encounter an error or failure during the deployment.

  > **Note:** It is recommended that you use the same usernames and Groupnames as per the file and it is not required that the domain be the same.For example, cn=oamLDAP,dc=oracle,dc=com instead of cn=oamLDAP,dc=example,dc=com.

Apart from the above Known Issues, this section also describes the following topics:

- Section 2.1.1, "Prerequisite Check Fails When Installing SOA and Oracle Identity and Access Management on SUSE Linux Enterprise Server 10 SP 3+"
- Section 2.1.2, "Opatch Errors When Applying One-off Patches During Oracle Identity and Access Management Installation,"
- Section 2.1.3, "Health Check Fails on Solaris 11 while Installing OIM,"

> **Note:** The *prov_run* command performs the entire deployment automatically. This is only supported if you are using the *prov_run* command to perform the deployment. If you are running the deployment manually using the *runIAMDeployment* commands then IDMLCM directory preparation is not supported.

2.1.1 Prerequisite Check Fails When Installing SOA and Oracle Identity and Access Management on SUSE Linux Enterprise Server 10 SP 3+

When you try to install Oracle SOA Suite and Oracle Identity and Access Management on SUSE Linux Enterprise Server 10 Service Pack (SP) 3+, the system prerequisite check for the `compat-libstdc++-5.0.7` package fails because this package is missing on your system.

After the other system requirements have been met, you can safely ignore this system prerequisite check for the `compat-libstdc++-5.0.7` package by specifying `-ignoreSysPrereqs` when you start the installer.

```
./runInstaller -ignoreSysPrereqs
```

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

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

Error-1

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

Description and Workaround:

These are warning messages which can be ignored.

Error-2

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

```
can be reused on different platforms and in multiple OPatch silent installs.

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

2.1.3 Health Check Fails on Solaris 11 while Installing OIM

When you run the healthcheck on Solaris 11 during installation, it fails to detect any missing packages. Solaris 11 doesn't have `usrucbps` pre-installed by default. As a result, it uses the `/usr/ucb/ps -auxwww` command to check whether the Node Manager has started properly or not, and fails at this stage.

To resolve this issue, run the following command before you install OIM:

```
pkg install compatibility/ucb
```

2.2 Configuration Issues and Workarounds

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

- Section 2.2.1, "Problem with OIM User Roles in an Integrated OIM, OAM, OMSS, and Active Directory Environment"
- Section 2.2.2, "WebLogic Administration Server Fails to Start on Windows with SQLIntegrityConstraintViolationException Error"
- Section 2.2.3, "Password for OAM Schema on Oracle Database 11g Expires Every 180 Days"
- Section 2.2.4, "bip_datasource Exceptions Appear in AdminServer.log During Identity and Access Management Deployment"
- Section 2.2.5, "Coherence Request Timeout Exception during Service Start"

Note: In certain scenarios, the IDM R2PS3 deployment using IDMLCM tool, the Oracle Unified Directory ACIs may not be updated in all OUD instances. After the deployment, check the *OUD_ORACLE_INSTANCE/OUD/config/config.ldif* file on all OUD instances for the presence of ACIs mentioned in section Update Oracle Unified Directory ACIs for LDAP Synchronization of the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management* document.

When you enable the Identity auditor feature in OIM, perform the following configuration changes for the OIM-BI Publisher integration to work fine.

1. Login to *IAM*GovernanceDomain Enterprise management console.
2. Open the system MBean browser and update the MBean:

   ```
   oracle.iam:Location=wlsoim1,name=Discovery,type=XMLConfig.DiscoveryConfig,XMLCo
   nfig=Config,Application=oim,ApplicationVersion=11.1.2.0.0
   ```
   with value as http://igdadmin.example.com/, where igdadmin.example.com is the Governance Domain admin Load balancer URL.

2.2.1 Problem with OIM User Roles in an Integrated OIM, OAM, OMSS, and Active Directory Environment

If you have configured Microsoft Active Directory as the LDAP directory in an integrated, Oracle Identity Manager (OIM), Oracle Access Manager (OAM), and Oracle Mobile Security Suite (OMSS) environment, then any user roles created in OIM will not be recognized by OAM or OMSS.

For example, if you log in to the OIM Console and create a new role called, "omssrole," and then you log into the OAM Console and search for that role, the role will not be found.

The workaround to this problem is to configure OIM so that it sets the `sAMAccountName` attribute to the same value as the `CN` attribute for each of the groups that it creates in the Active Directory instance. This workaround must be applied before creating any new roles in OIM.

1. Open a new terminal window on the host where OIM is installed.
2. Connect to OIM Governence domain Administration Server.

   For example:

   ```
   WL_HOME/server/bin/setWLSEnv.sh
   WL_HOME/common/bin/wlst.sh
   wls:/offline> connect ("weblogic", "admin_password",
                               "t3://OIMHOST.example.com:7001")
   ```
3. Enter the following WLST command to add the `sAMAccountName` attribute to all groups in the directory:

   ```
   wls:/IAMGovernanceDomain/serverConfig>
   addPluginParam(adapterName='dir1',pluginName='UserManagement',
                           paramKeys='addAttribute',paramValues='group,
                           samaccountname=%cn%',contextName='oim')
   ```
4. Exit from WLST and locate the following file in the Domain home directory:

   ```
   DOMAIN_HOME/config/fmwconfig/ovd/oim/adapters.os_xml
   ```
5. Verify that the following entry has been added to the adapters.os_xml file:

   ```
   <ns2:param name="addAttribute" value="group,samaccountname=%cn%"/>
   ```
6. Restart the OIM Managed Server (for example, wls_oim1).

2.2.2 WebLogic Administration Server Fails to Start on Windows with SQLIntegrityConstraintViolationException Error

When you attempt to start the WebLogic Administration Server on Windows after installing and configuring Oracle Identity and Access Management, the Administration Server might fail to start with a `java.sql.SQLIntegrityConstraintViolationException` error.

As a workaround, open the *`DOMAIN_HOME`*`\bin\setDomainEnv.cmd` file, and set `-DDISABLE_CONFIG_ENTITY` to `true`.

For example:

```
-DDISABLE_CONFIG_ENTITY=true
```

Then, restart the Administration Server.

2.2.3 Password for OAM Schema on Oracle Database 11*g* Expires Every 180 Days

The default password lifetime used for a user created on a newly installed Oracle Database 11*g* database is 180 days. After 180 days, the password automatically expires.

When the Oracle Access Manager (OAM) schema password expires, the OAM environment will become inoperable.

To avoid this problem, you can do one of the following:

Solution 1: Change the default password policy for the database by configuring the password settings in the `DEFAULT` database profile (or in another relevant profile assigned to the OAM schema) so that the current OAM schema password will never expire.

To do this, you can use the `ALTER PROFILE` statement to set the `PASSWORD_LIFE_TIME` and `PASSWORD_GRACE_TIME` parameters to `UNLIMITED` in the OAM schema user's profile.

For more information about the password-related settings in the default profile and how to configure them, see "Configuring Password Settings in the Default Profile" in the *Oracle Database Security Guide*.

See *Oracle Database SQL Language Reference* for more information about using `ALTER PROFILE` to modify the default password settings.

or

Solution 2: Reset the password before it expires.

To reset the OAM schema password on an Oracle Database 11*g* database, you must first update the password for both the OPSS schema and OAM schema in the WebLogic Server Administration Console and then update the passwords in the database.

> **Note:** For more information, refer to My Oracle Support Document ID 1545889.1.

1. Update the password for OPSS in the WebLogic Server Administration Console:
    1. From the **Domain Structure** menu, expand **Services** and click **Data Sources**.
    2. Select the **opss-DBDS** data source in the Data Sources table.
    3. Select the **Configuration > Connection Pool** sub tab.
    4. Click **Lock & Edit** in the Change Center.
    5. Enter a new password for the OPSS schema in the **Password** and **Confirm Password** fields.
    6. Click **Save** to save the new password.
2. Update the password for OAM in the WebLogic Server Administration Console:
    1. From the **Domain Structure** menu, expand **Services** and click **Data Sources**.
    2. Select the **oamDS** data source in the Data Sources table.
    3. Select the **Configuration > Connection Pool** sub tab.
    4. Enter a new password for the OAM schema in the **Password** and **Confirm Password** fields.
    5. Click **Save** to save the new password, and then click **Activate Changes** in the Change Center.
3. Stop the servers (Administration Server and Managed Servers) in your environment.

4. Log on to sqlplus as the SYS database user, and update the schema passwords in the database:

   ```
   SQL> ALTER USER OAM_SCHEMA_USER IDENTIFIED BY NEW_PASSWORD;
   SQL> ALTER USER OPSS_SCHEMA_USER IDENTIFIED BY NEW_PASSWORD;
   ```

   For example:

   ```
   SQL> ALTER USER DEV_OAM IDENTIFIED BY password;
   SQL> ALTER USER DEV_OPSS IDENTIFIED BY password;
   ```

5. Start WLST from the *MW_HOME*/oracle_common/common/bin directory. For example:

   ```
   cd MW_HOME/oracle_common/common/bin
   ./wlst.sh
   ```

6. Run the WLST modifyBootStrapCredential command as follows:

   ```
   modifyBootStrapCredential(jpsConfigFile='DOMAIN_HOME/config/fmwconfig/jps-confi
   g.xml', username='prefix_OPSS', password='new_password')
   ```

7. Exit WLST:

   ```
   exit()
   ```

8. Start the servers in your environment.

2.2.4 bip_datasource Exceptions Appear in AdminServer.log During Identity and Access Management Deployment

If you are using the Life Cycle Management (LCM) Tools to perform an Identity and Access Management deployment, you might encounter the following exception for the bip_datasource connection pool in the AdminServer.log file during the preconfigure phase:

```
java.net.UnknownHostException: dbhost.example.com: Name or service not known
```

This exception related to the use of dbhost.example.com by the bip_datasource connection pool is harmless and can be safely ignored.

2.2.5 Coherence Request Timeout Exception during Service Start

In certain scenarios, when you are using the LCM tools to automatically deploy Oracle Identity and Access Management, a *RequestTimeoutException* may be generated and seen in the IAM Access domain server logs:

```
com.tangosol.net.RequestTimeoutException: Timeout during service start
```

If you encounter this error, perform the following workaround:

1. Shut down the Access Domain servers, including admin server and the managed servers.

   Refer to Starting and Stopping IAMAccessDomain Services in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management* for instructions on stopping the servers in the correct order.

2. Locate the startup.properties file used by nodemanager to start the Access domain Admin server:

   ```
    IAD_ASERVER_HOME/servers/AdminServer/data/nodemanager/startup.properties
   ```

3. Edit the startup.properties file, locate the property, *Arguments* in the file and append to it:

   -Djava.net.preferIPv4Stack=true

4. Restart the Access domain servers, including the admin server and the managed servers.

Refer to Starting and Stopping IAMAccessDomain Services in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management* for instructions on starting the servers in the correct order.

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 11g Release 2 (11.1.2.3.0). It includes the following sections:

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

3.1 Manual Upgrade Issues

This section describes issues related to upgrading the following:

- Upgrading Oracle Identity and Access Management components from 11g Release 2 (11.1.2.1.0) to 11g Release 2 (11.1.2.3.0)
- Upgrading Oracle Identity and Access Management components from 11g Release 2 (11.1.2) to 11g Release 2 (11.1.2.3.0)
- Upgrading Oracle Identity and Access Management components from 11g Release 1 (11.1.1.7.0) to 11g Release 2 (11.1.2.3.0)
- Upgrading Oracle Identity and Access Management components from 11g Release 1 (11.1.1.5.0) to 11g Release 2 (11.1.2.3.0)
- Upgrading Oracle Identity and Access Management components from 9.1.x.x to 11g Release 2 (11.1.2.3.0)

For the list of upgrade, migration, and patching issues reported in 11g Release 2 (11.1.2.2.0), see "Upgrade, Migration, and Patching Issues for Oracle Identity and Access Management" in the *Oracle Fusion Middleware Release Notes* for 11g Release 2 (11.1.2.2.0).

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

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

3.1.1 Manual Upgrade Issues and Workaround

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

- Null Pointer Exception While Creating IDS or ESSO Profile After Upgrading Oracle Access Manager
- Error When Accessing My Entitlements Page After Upgrading Oracle Identity Manager to 11.1.2.3.0
- Exception When you Click on 'Edit' link After Creating Application Instance
- 'Generate Entitlement Forms' Option not Available on Clicking 'Regenerate View' After Upgrading Oracle identity Manager
- Error While Upgrading Oracle Identity Manager Binaries Due to Wrong OPatch version
- Pre-Upgrade Report for OIM Detects Your Existing OIM version as 11.1.2.0.0 Though the Actual Version is 11.1.2.1.0
- Exception When Opening a User After Upgrading Oracle Identity Manager
- Exception When Upgrading Oracle Access Manager System Configurations Using upgradeConfig() Command
- Global Common ID Attribute Value Missing During IDS Profile Creation After Upgrading Oracle Entitlements Server
- Error When Restarting Oracle Adaptive Access Manager Managed Server After Redeploying Oracle Adaptive Access Manager Applications
- Warning While Upgrading Oracle Entitlements Server 11.1.1.5.0 Binaries to 11.1.2.3.0
- Double Authentication Required for OAAM Admin User After Upgrading OAM-OAAM Integrated 11.1.1.7.0 Environment
- OIM Middle Tier Online Upgrade Fails When Upgrading 11.1.1.7.0 OIM-OAM-OAAM Integrated Environment
- Registration and Track Registration Links Not Working After Upgrading OIM-OAM-OAAM Integrated 11.1.1.7.0 Environment
- Human Workflow Error While Moving From Test to Production After Upgrading Oracle Identity Management 11g Release 1 Environments

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

This issue occurs when you upgrade Oracle Identity Manager 9.x or Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.3.0). The LOV fields for User, Role, and Organization Forms on User Interface are not upgraded correctly.

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

The workaround is as follows:

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

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

2. Create and activate a sandbox.
3. Click **Form Designer**.
4. Search for **User form**, and open it.

5. For each LOV UDF, create the UDF with the name same as the UDF name in the `User.xml` file. Make sure you select both **Searchable** and **Searchable Picklist**.
6. Repeat for all the searchable LOV fields of Role and Organization forms.
7. Publish the sandbox.

3.1.1.2 Updating System Mbean Configuration

In Oracle Access Manager Release 2 (11.1.2.3.0), the System Mbean Configuration files have been modified to remove the dependency on domain home. The `copyMbeanXmlFiles` command moves the domain Mbean jars out of the domain home to eliminate any future upgrade or patching issues.

After you have applied the 11.1.2.3.0 patch, you must run the following WLST commands to complete the patching process for OAM:

1. After applying the 11.1.2.3.0 patch set, use the Patch Set Assistant to update the Oracle Access Manager Components as described in "Updating Your Schemas with Patch Set Assistant".

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

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

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

   On Unix operating systems:

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

   On Windows operating systems:

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

3. After a successful run of the above command, verify that the 11.1.2.3.0 Mbean XML files are copied to the following locations:

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

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

3.1.1.3 SOA Email Notification Does Not Work

In an Oracle Identity Manager 11*g* Release 2 (11.1.2.3.0) deployment that has been upgraded from 11g Release 2 (11.1.2.1.0) or 11*g* Release 2 (11.1.2), SOA email notification may not work in some cases. To ensure that the workaround described in this section is applicable, do the following:

1. Ensure that the WebLogic Administration Server and SOA Managed Server(s) are running.
2. Log in to the Oracle Enterprise Manager.
3. Expand **Weblogic Domain** in the left pane.

4. Right-click on the ***`WLS_DOMAIN`***, and select **System MBeans Browser**.
5. Go to **Application Defined MBeans**, and click the following in the order specified:
   a. oracle.as.soainfra.config
   b. WorkflowIdentityConfig
   c. human-workflow
   d. WorkflowIdentityConfig.ConfigurationType
   e. jazn.com
   f. WorkflowIdentityConfig.ConfigurationType.ProviderType
   g. JpsProvider
   h. WorkflowIdentityConfig.ConfigurationType.ProviderType.PropertyType
   i. jpsContextName
6. Check the **Value** attribute. If value is `default`, the workaround described in this section is not applicable, and you should check email driver configuration in Enterprise Manager.

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

To workaround this issue, complete the following steps:

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

3.1.1.4 AD User Management Connector Issues

After you have applied the Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) patch, the AD User Management 11.1.1.5.0 reconciliation profile used for Oracle Identity Manager may be overwritten.

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

3.1.1.5 Harmless Error After Applying Interim Patch 14481477

If Interim Patch 14481477 was applied to the existing Oracle Identity and Access Management 11g Release 2 (11.1.2.0.0) environment before applying the 11.1.2.3.0 patch, you may see the following warning. You can safely ignore this error message.

Error Message:

```
OUI-10221:The install touches a component that is patched by interim
patches'Interim Patch# 14481477'. The interim patches affect other components not
included in the install.
You may rollback the interim patches 'Interim Patch# 14481477'using OPatch for
consistency before performing the upgrade. You may also choose to ignore this
```

```
warning and continue with the upgrade. If you choose to continue, the conflicting
patches will be removed from the inventory. However, some files that are not
updated during the upgrade may be left behind. Contact Support to check
applicability and availability of interim patches 'Interim Patch# 14481477' for
this install.
Do you want to ignore the patch conflicts and continue with the upgrade?.
```

3.1.1.6 Delete WebLogic Server TMP Directories

After you have applied the Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) patch, some of the transaction screens may not open properly. To correct this issue, delete the server-level temporary directories as described below.

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

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

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

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

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

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

3.1.1.7 Classpath Issue While Patching Oracle Identity Manager Middle Tier

If you receive the following error message while updating your Oracle Identity Manager (OIM) Middle Tier from 11.1.2.0.0 to 11.1.2.3.0, you must update the `ucp.jar` classpath in the `OIMUpgrade.sh` script.

Error Message:

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

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

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

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

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

3.1.1.8 OAuth Service Policy is Missing After Upgrade

This issue occurs if you upgrade an Oracle Access Management 11.1.2.0.0 environment to version 11.1.2.3.0. The `ms_oauth/oauth2/**` policy that is required for OAuth Services is missing. To correct this issue, complete the following steps.

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

      The Launch Pad opens.

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

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

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

      The OAMAuthentication "Service Provider Configuration" page opens.

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

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

      The OAuth Identity Domains page opens.

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

      The Identity Domain Configuration page opens.

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

      The Service Provider configuration page opens.

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

   i. Click **Save**.

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

This issue occurs when you upgrade Oracle Access Management Access Manager 11*g* Release 2 (11.1.2) to 11.1.2.3.0. The upgrade logs have the messages **"the Prerequisite check "CheckApplicable" failed"** and **"Required component(s) missing"**. You can ignore these messages.

3.1.1.10 Errors While Starting OIM Server After Successful Upgrade

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

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

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

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

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

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

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

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

3.1.1.11 obLockedOn Attribute Missing From Oracle Internet Directory After Upgrading Access Manager to 11.1.2.3.0

This issue occurs when you upgrade Oracle Access Management Access Manager 11*g* Release 2 (11.1.2) to 11.1.2.3.0. After upgrading Access Manager 11.1.2 to 11.1.2.3.0, the `obLockedOn` attribute will be missing from the Oracle Internet Directory (OID). You must add this attribute back to the Oracle Internet Directory.

The workaround for this issue is as follows:

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

3.1.1.12 Exception When Upgrading Oracle Identity Manager Middle Tier

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 1 (11.1.1.7.0), or 11*g* release 1 (11.1.1.5.0), or 9.1.x.x to 11.1.2.3.0. The following exception is displayed when you upgrade Oracle Identity Manager middle tier:

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

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

3.1.1.13 Active Directory User Management 11.1.1.5.0 Connector May Not Work After Upgrading Oracle Identity Manager to 11.1.2.3.0

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 2 (11.1.2) with Active Directory 11.1.1.5.0 connector to Oracle Identity Manager 11*g* Release 2 (11.1.2.3.0). After you upgrade Oracle Identity Manager 11.1.2 to 11.1.2.3.0, Active Directory user management 11.1.1.5.0 reconciliation profile gets corrupted.

The workaround for this issue is as follows:

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

1. Log in to the Oracle Identity Manager 11.1.2.3.0 Design Console by running the following command from the location `*ORACLE_HOME*/designconsole/`:

   On UNIX: `./xlclient.sh`

   On Windows: `xlclient.cmd`

2. Expand **Resource Management**.
3. Click **Resource Objects**.
4. Search for the name **Xellerate Organization**.
5. In the Resource Object details page, go to the **Object Reconciliation** tab.
6. Click **Create Reconciliation Profile**. A message will pop up when the profile is created successfully.

3.1.1.14 Error While Starting OIM Server After Upgrading OIM 9.1.x.x to 11.1.2.3.0

This issue occurs when you upgrade Oracle Identity Manager 9.1.x.x to 11.1.2.3.0. After upgrading to 11.1.2.3.0, when you start the OIM Server, the following error is displayed:

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

This error message can be ignored.

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

This issue occurs when you upgrade Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.1.0) to 11*g* Release 2 (11.1.2.3.0). After upgrading to 11.1.2.3.0, when you log in to the OAAM Admin Server or OAAM Offline Server for the first time, the following warning message is displayed:

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

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

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

This issue occurs when you upgrade Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2) to 11*g* Release 2 (11.1.2.3.0). After you upgrade OAAM Admin Server and OAAM Offline Server to 11.1.2.3.0, the following error is seen in the upgrade log file:

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

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

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

This issue occurs when you upgrade Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2.3.0). After the upgrade process, when you start the OAAM admin and managed servers, the following exception is displayed as a notification:

```
[2013-10-24T13:20:01.698-07:00] [oaam_admin_server1] [NOTIFICATION] []
[oracle.adfdt.model.mds.MDSApplicationService] [tid: [ACTIVE].ExecuteThread:
'3' for queue: 'weblogic.kernel.Default (self-tuning)'] [userId: <anonymous>]
[ecid: d19903e12f34a6b2:-55051c63:141ebc57e5a:-8000-000000000000019f,0] [APP:
oaam_admin#11.1.2.0.0] [[
oracle.mds.exception.NoTipCustomizationLayerException: MDS-00091: Unable to
customize /oracle/oaam/view/DataBindings.cpx, empty or null value for tip
customization layer user
at oracle.mds.core.MDSSession.getMutableMO(MDSSession.java:4150)
at oracle.mds.core.MDSSession.getMutableMO(MDSSession.java:2110)
at oracle.mds.core.MDSSession.getMutableMO(MDSSession.java:1985)
at
oracle.adfdt.model.mds.MDSApplicationService.findApplication(MDSApplicationSer
vice.java:58)
at
oracle.adfdt.model.mds.MDSModelDesignTimeContext.initServices(MDSModelDesignTi
meContext.java:232)
at
oracle.adfdt.model.mds.MDSModelDesignTimeContext.<init>(MDSModelDesignTimeCont
ext.java:82)
at
oracle.adfdt.mds.MDSDesignTimeContext.<init>(MDSDesignTimeContext.java:81)
at
oracle.adfdt.mds.MDSDesignTimeContext.<init>(MDSDesignTimeContext.java:69)
at
oracle.adfinternal.view.page.editor.Page.getDesignTimeBindingContainer(Page.ja
va:618)
at
```

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

3.1.1.18 Some Apps are in Prepared State After Upgrade

After you upgrade Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2.3.0), the following Apps are in 'Prepared' state:

- oaam_admin
- oaam_offline
- oaam_server

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

3.1.1.19 Error When Accessing OAAM

After you upgrade Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.7.0) to 11*g* Release 2 (11.1.2.3.0), when you login to EM, and click **Identity & Access** and then click **OAAM**, the following error message is displayed:

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

To resolve this issue, perform the following steps:

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

3.1.1.20 Grant/Revoke Requests Cannot be Viewed After OIM Upgrade

This issue occurs after you upgrade Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2.3.0). Grant/revoke requests raised for roles with OIM Roles role category cannot be viewed after upgrade. After upgrade, when you create a request in 11.1.1.5.0, the following error message is displayed in the UI:

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

These requests are not valid in 11*g* Release 2 (11.1.2.3.0), as these roles are not to be added to the Catalog.

3.1.1.21 Error During REQUEST_TYPE Upgrade

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2.3.0). Following error is displayed in the middle tier upgrade logs during REQUEST_TYPE upgrade:

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

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

To resolve this issue, perform the following steps:

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

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

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

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

3.1.1.22 Exception in Log File After OAAM Upgrade

This issue occurs after you upgrade Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2.3.0). After the upgrade process, when you start the OAAM admin and managed servers, the following exception is displayed as a warning in the `AdminServer-Diagnostic.log` file:

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

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

3.1.1.23 OAAM Administration Server Shows Version 11.1.2.1.0 After Upgrade

This issue occurs when you upgrade Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.1.0) Bundle Patch 01 (BP01) to 11.1.2.3.0, and if you had not applied Bundle Patch 01 correctly. If you had not applied BP01 correctly when you upgraded OAAM 11.1.2.1.0 to 11.1.2.1.0 BP01, and if you still upgrade to 11.1.2.3.0, you will continue to see the product version as 11.1.2.1.0 on the OAAM Administration Server.

The workaround for this issue is as follows:

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

3.1.1.24 OAAM Admin Redeploy Does Not Work When Upgrading OAAM to 11.1.2.3.0

This issue occurs when you upgrade Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.1.0) Bundle Patch 01 (BP01) to 11.1.2.3.0. When upgrading OAAM to 11.1.2.3.0, OAAM_Admin redeploy does not work.

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

3.1.1.25 Identifying and Recompiling INVALID Schema Objects After Upgrading Oracle Identity Manager to 11.1.2.3.0

After you upgrade Oracle Identity Manager to 11.1.2.3.0, few OIM Database objects may temporarily be in `INVALID` state due to alterations in underlying dependencies. Such objects get auto compiled on first time invocation in Oracle Database. However, you can optionally recompile the `INVALID` objects. To identify and recompile the `INVALID` schema objects, do the following:

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

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

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

   ```
   BEGIN

   UTL_RECOMP.recomp_serial('<Schema_Name>');

   END;
   ```

3.1.1.26 Error While Executing ConfigureSecurityStore.py

During the Oracle Entitlements Server 11.1.2.3.0 upgrade process, `Opatch (17403853)` does not get applied, and when you execute `configureSecurityStore.py`, the following error message is displayed:

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

```
Txn(JpsDBDataManager.java:1492)
```

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

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

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

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) high availability environments to Oracle Identity Manager 11*g* Release 2 (11.1.2.3.0).

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

```
<AuthPolicyMergeListener : loadPolicies() : Problem in seeding authorization
policies. Please verify if you have run Middle Tier Upgrade before starting
OIM Server. Please restart the application after running Middle Tier Upgrade.
If the problem still occurs, refer to the documentation to manually update
the authorization policies access denied
(oracle.security.jps.service.policystore.PolicyStoreAccessPermission
Context:APPLICATION Context Name:OracleIdentityManager Admin
Resource:APPLICATION_POLICY Actions:manage)>
java.security.AccessControlException: access denied
(oracle.security.jps.service.policystore.PolicyStoreAccessPermission
Context:APPLICATION Context Name:OracleIdentityManager Admin
Resource:APPLICATION_POLICY Actions:manage)
```

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

3.1.1.28 LabelExistsException While Starting Oracle Identity Manager Server After Upgrade

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) high availability environments to Oracle Identity Manager 11*g* Release 2 (11.1.2.3.0).

When you start the Oracle Identity Manager Server after upgrading Oracle Identity Manager 11.1.2.1.0 high availability environments to 11.1.2.3.0, the following exception is thrown:

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

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

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

This issue occurs when you create IDS or ESSO profile after upgrading Oracle Access Manager 11g Release 1 (11.1.1.5.0) to Access Manager 11g Release 2 (11.1.2.3.0).

The workaround for this issue is as follows:

1. Create the directory *`$DOMAIN_HOME`*`/config/fmwconfig/ovd/ids`.

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

3.1.1.30 Error When Accessing My Entitlements Page After Upgrading Oracle Identity Manager to 11.1.2.3.0

This issue occurs when you upgrade Oracle Identity Manager 11g Release 2 (11.1.2) to 11g Release 2 (11.1.2.3.0). After upgrading Oracle Identity Manager 11.1.2 to 11.1.2.3.0, when you access My Entitlements page, the following error is displayed:

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

The workaround for this issue is as follows:

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

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

This issue occurs when you upgrade Oracle Identity Manager 11g Release 2 (11.1.2.1.0) high availability environments to 11.1.2.3.0. After you create an application instance, when you click on the `Edit` link, the following exception is thrown:

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

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

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

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

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

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

This issue occurs after you upgrade Oracle Identity Manager 11g Release 2 (11.1.2) or 11g Release 2 (11.1.2.1.0) to 11.1.2.3.0.

After you upgrade Oracle Identity Manager to 11.1.2.3.0, when you click Regenerate View for the existing forms that contain entitlement attributes, the Generate Entitlement Forms option is not displayed. Use one of the following workarounds when this issue occurs:

- Create new form for the affected application instance. The new form should work as expected, that is Generate Entitlement Forms option will be available for new forms.
- Manually fix the existing form. The procedure for fixing the application instances whose entitlement attributes use Lookup code in the process form is different from the procedure for fixing the application instance whose entitlement attributes use Lookup Query in the process form. The entitlement attributes which use Lookup Code in the process form are represented as Lookup fields in the Form Designer. The entitlement attributes which use Lookup Query in the process form are represented as Text fields in the Form Designer. Depending upon what the entitlement attributes are using, complete one of the following procedures to manually fix the forms:

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

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

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

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

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

Repeat this step to fix all the child form EO xmls that have entitlement attributes.

- Recreate the zip file and import it back using Enterprise Manager. For more information about importing metadata files, see "Importing Metadata Files from MDS" Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.

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

This issue occurs when you upgrade Oracle Identity Manager binaries to 11*g* Release 2 (11.1.2.3.0). The supported OPatch version for Oracle Identity Manager upgrade is 11.1.0.9.9. Different OPatch version might cause patch application failure. The following error will be displayed in the install logs if incorrect OPatch version is used:

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

The workaround for this issue is to ensure that the OPatch version in `*OIM_HOME*` and `*MW_HOME*/oracle_common` is 11.1.0.9.9, before you upgrade Oracle Identity Manager binaries to 11.1.2.3.0.

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

- On UNIX: `*ORACLE_INVENTORY_LOCATION*/logs`

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

- On Windows: `*ORACLE_INVENTORY_LOCATION*\logs`

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

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

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

If any OPatch fails, apply the failed patches manually.

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

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) environments which was upgraded from Oracle Identity Manager 11*g* Release 2 (11.1.2.0.0), to 11.1.2.3.0. When you generate the pre-upgrade report, it detects your existing OIM version as 11.1.2.0.0 instead of 11.1.2.1.0. If you check the schema version using the query `select * from schema_version_registry`, it shows 11.1.2.1.0. This occurs if XSD table values are not updated after schema upgrade.

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

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

3.1.1.35 Exception When Opening a User After Upgrading Oracle Identity Manager

This issue occurs when you upgrade Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) to 11*g* Release 2 (11.1.2.3.0).

After you upgrade Oracle Identity Manager to 11.1.2.3.0, when you open a user, the following exception is displayed:

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

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

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

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

   For information about exporting metadata files to MDS, see "Exporting Metadata Files to MDS" in the *Developing and Customizing Applications for Oracle Identity Manager*.

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

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

This issue occurs if you are upgrading Oracle Access Manager 11*g* Release 2 (11.1.2.0.0) environments which was previously upgraded from 11*g* Release 1 (11.1.1.5.0), to Oracle Access Manager 11*g* Release 2 (11.1.2.3.0).

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

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

The workaround for this issue is as follows:

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

3.1.1.37 Global Common ID Attribute Value Missing During IDS Profile Creation After Upgrading Oracle Entitlements Server

After you upgrade Oracle Entitlements Server 11*g* Release 2 (11.1.2.1.0) to Oracle Entitlements Server 11*g* Release 2 (11.1.2.3.0), when you create Identity Store Profile using APM, the default value of the Global Common ID Attribute will be missing.

The workaround for this issue is as follows:

1. Create a new IDS profile in APM.
2. Update the value of **Global Common ID Attribute** to `uid`.

3.1.1.38 Error When Restarting Oracle Adaptive Access Manager Managed Server After Redeploying Oracle Adaptive Access Manager Applications

This issue occurs when you upgrade Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) or 11*g* Release 1 (11.1.1.7.0) to 11*g* Release 2 (11.1.2.3.0).

After you redeploy Oracle Adaptive Access Manager applications, when you restart the servers, the following error is displayed:

```
Error:
ADF error seen in std-out of managed servers.
"<Sep 25, 2014 9:17:24 PM MDT> <Error> <oracle.adf.share.ADFContext>
<BEA-000000>  <ADF detected an ADFContext leak.
Please see the documentation for more information about handling ADFContext leak
s.
For more information about the leaking ADFContext please enable logging for
oracle.adf.share.ADFContext at FINEST level.
>"
```

This is an harmless error.

3.1.1.39 Warning While Upgrading Oracle Entitlements Server 11.1.1.5.0 Binaries to 11.1.2.3.0

When you upgrade Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) binaries to 11.1.2.3.0 using the Oracle Identity and Access Management 11.1.2.3.0 installer, the following warning is displayed:

```
OUI-10221:The install touches a component that is patched by interim patches
'Interim Patch# 14801327'. The interim patches affect other components not
included in the install.
You may rollback the interim patches 'Interim Patch# 14801327' using OPatch
for consistency before performing the upgrade.
You may also choose to ignore this warning and continue with the upgrade. If
you choose to continue, the conflicting patches will be removed from the
inventory. However, some files that are not updated during the upgrade may be
left behind. Contact Support to check applicability and availability of
interim patches 'Interim Patch# 14801327' for this install.
Do you want to ignore the patch conflicts and continue with the upgrade?
```

This warning can be ignored.

3.1.1.40 Double Authentication Required for OAAM Admin User After Upgrading OAM-OAAM Integrated 11.1.1.7.0 Environment

After you upgrade Oracle Access Manager (OAM) - Oracle Adaptive Access Manager (OAAM) integrated 11*g* Release 1 (11.1.1.7.0) environment to 11*g* Release 2 (11.1.2.3.0), double authentication required for OAAM admin user.

To resolve this issue, validate that the providers ordering is correct, by verifying the steps described in "Creating Oracle Access Manager Identity Asserter" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management* for 11*g* Release 1 (11.1.1.5.0).

3.1.1.41 OIM Middle Tier Online Upgrade Fails When Upgrading 11.1.1.7.0 OIM-OAM-OAAM Integrated Environment

When you perform Oracle Identity Manager middle tier upgrade on OIM-OAM-OAAM integrated 11*g* Release 1 (11.1.1.7.0) environment, the upgrade fails with the following exception:

```
SEVERE: Exception while seeding OIM Resource Policies in OAM
oracle.idm.automation.impl.oim.resource.seed.exception.OIMResourceSeedException:
Exception while getting Application Domains
```

The workaround for this issue is as follows:

1. Modify the `OAM_DOMAIN/config/config.xml` file to add `enforce-valid-basic-auth-credentials` tag within the `<security-configuration>` tag as shown in the following example:

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-c
   redentials
   ```

2. Specify the OAM admin username for the property `oam.admin.username` in the `oim_upgrade_input.properties` file located at `ORACLE_HOME/server/bin/`.

   ```
   oam.admin.username=oamadminuser
   ```

3.1.1.42 Registration and Track Registration Links Not Working After Upgrading OIM-OAM-OAAM Integrated 11.1.1.7.0 Environment

After upgrading OIM-OAM-OAAM integrated 11g Release 1 (11.1.1.7.0) environments to 11.1.2.3.0, the registration and track registration links may not work.

The workaround for this issue is to verify that the following OAAM properties with OIM registration URLs set correctly:

- `bharosa.uio.default.signon.links.enum.selfregistration.url=http://OIM_HOST:OIM_PORT/identity/faces/register?&backUrl=OIM_HOST:OIM_PORT/identity`
- bharosa.uio.default.signon.links.enum.trackregistration.url=`http://OIM_HOST:OIM_PORT/identity/faces/register?&backUrl=OIM_HOST:OHS_PORT/identity`

3.1.1.43 Human Workflow Error While Moving From Test to Production After Upgrading Oracle Identity Management 11*g* Release 1 Environments

After you upgrade Oracle Identity Manager 11*g* Release 1 (11.1.1.7.0) or 11*g* Release 1 (11.1.1.5.0) environments to Oracle Identity Manager 11g Release 2 (11.1.2.3.0), when you move from test to production, the following human workflow error is logged when you run the `pasteConfig` command:

```
UserConfigDataMigrationException:

oracle.bpel.services.workflow.util.tools.wfUserConfigDataMigrator.
UserConfigDataMigrationException: ORABPEL-30511.

Verification Service cannot resolve user identity.
User weblogic cannot be found in the identity repository.
Workflow Context token cannot be null in request.
at
oracle.bpel.services.workflow.util.tools.wfUserConfigDataMigrator.impl.TaskPay
loadFlexFieldMappingMigrator.importHandler(TaskPayloadFlexFieldMappingMigrator.jav
a:338)
```

The workaround for this issue is as follows:

1. Update the versions of `oim` and `OIMMetadata` in the `config-path.properties` file located at *`DOMAIN_HOME`*`/init-info/config-path.properties` as described below:
   - Change `oim\#11.1.1.3.0` to `oim\#11.1.2.0.0`
   - Change `OIMMetadata\#11.1.1.3.0` to `OIMMetadata\#11.1.2.0.0`
2. Add the following entries to the *`DOMAIN_HOME`*`/init-info/config-path.properties` file, if not present already. When adding the following entries, replace *`<OIM_ORACLE_HOME_DIR_NAME>`* with the actual directory name of the OIM Oracle Home.

   ```
   oracle.idm.ipf\#11.1.2@11.1.2=oracle.dogwood.top_11.1.1.7.0_<OIM_ORACLE_HOME_DI
   R_NAME>_ORACLE_HOME
   oracle.idm.ids.config.ui\#11.1.2@11.1.2=oracle.dogwood.top_11.1.1.7.0_<OIM_ORAC
   LE_HOME_DIR_NAME>_ORACLE_HOME
   oracle.iam.console.identity.self-service.ear\#V2.0=oracle.oim.suite_11.1.1.7.0_
   <OIM_ORACLE_HOME_DIR_NAME>_ORACLE_HOME
   oracle.iam.console.identity.sysadmin.ear\#V2.0=oracle.oim.suite_11.1.1.7.0_<OIM
   _ORACLE_HOME_DIR_NAME>_ORACLE_HOME
   oracle.iam.ui.custom\#11.1.1@11.1.1=oracle.oim.suite_11.1.1.7.0_<OIM_ORACLE_HOM
   E_DIR_NAME>_ORACLE_HOME
   oracle.iam.ui.model\#1.0@11.1.1.5.0=oracle.oim.suite_11.1.1.7.0_<OIM_ORACLE_HOM
   E_DIR_NAME>_ORACLE_HOME
   oracle.iam.ui.oia-view\#11.1.1@11.1.1=oracle.oim.suite_11.1.1.7.0_<OIM_ORACLE_H
   OME_DIR_NAME>_ORACLE_HOME
   oracle.iam.ui.view\#11.1.1@11.1.1=oracle.oim.suite_11.1.1.7.0_<OIM_ORACLE_HOME_
   DIR_NAME>_ORACLE_HOME
   oracle.idm.msm.ui.library\#11.1.2@11.1.2=oracle.oim.suite_11.1.1.7.0_<OIM_ORACL
   E_HOME_DIR_NAME>_ORACLE_HOME
   ProvCallback=oracle.oim.suite_11.1.1.7.0_<OIM_ORACLE_HOME_DIR_NAME>_ORACLE_HOME
   Reqsvc=oracle.oim.suite_11.1.1.7.0_<OIM_ORACLE_HOME_DIR_NAME>_ORACLE_HOME
   SCIM\ REST\ service\ for\
   OIM=oracle.oim.suite_11.1.1.7.0_<OIM_ORACLE_HOME_DIR_NAME>_ORACLE_HOME
   SodCheckService=oracle.oim.suite_11.1.1.7.0_<OIM_ORACLE_HOME_DIR_NAME>_ORACLE_H
   OME
   ```

3. Save the `config-path.properties` file.
4. Modify the *`DOMAIN_HOME`*`/oim_domain/config/config.xml` file as below:
   - `<name>OIMMetadata#11.1.1.3.0</name>` as `<name>OIMMetadata#11.1.2.0.0</name>`
   - `<name>oim#11.1.1.3.0</name>` as `<name>oim#11.1.2.0.0</name>`
5. Re-run the `copyConfig` and `pasteConfig` commands.

3.2 Migration Issues

This section describes the issues related to the following scenarios:

- Migrating Oracle Access Manager 10*g* to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.3.0)
- Migrating Oracle Adaptive Access Manager 10*g* to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.3.0)
- Migrating Oracle Single Sign-On 10*g* to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.3.0)
- Migrating Sun OpenSSO Enterprise 8.0 to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.3.0)
- Migrating Sun Java System Access Manager 7.1 to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.3.0)
- Migrating Oracle Identity Analytics 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.3.0).
- Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.3.0)
- Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.3.0)
- Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.3.0)

3.2.1 Migration Issues and Workaround

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

- osso.conf Files may be Copied to Alternate File Location If Upgrading Oracle Single Sign-On 10g Fails
- Server Logs and Assessment Report for Certain Scenarios Show Only English Messages
- Registering Policy Agent 2.2 Using RREG Fails Due to Unavailability of Agent Template
- Assessment Report for OAM 10g Incremental Migration Shows Artifacts that are not Selected
- Assessment Report for OAM 10g Delta Migration Shows Artifacts that are not Selected
- Oracle Access Management 11g Release 2 (11.1.2.0.0) Coexistence, Upgrade, and Migration Supplement

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

This issue occurs when you upgrade Oracle Single Sign-On 10*g* to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.3.0). If errors occurs during the execution of the Upgrade Assistant which require you to re-run the process, there is a possibility that required `osso.conf` files will not be generated, in the location specified in the Upgrade Assistant Summary screen, at the end of the process.

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

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

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

Known issue.

The server logs and assessment report shows only English messages when you migrate the following components to Oracle Access Management Access Manager 11g Release 2 (11.1.2.3.0):

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

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

This issue occurs when you register Policy Agent 2.2 in Oracle Access Management 11.1.2.3.0 Server using Remote Registration tool (RREG), during migration. This is because of the unavailability of the agent template.

The workaround for this issue is as follows:

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

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

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

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

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

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

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

   - **For 2.2 J2EE Agent:**

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

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

   - **For 2.2 Web Agent:**

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

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

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

This issue occurs when you migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.3.0. When you perform incremental migration in `evaluate_only` mode, the assessment report contains the following:

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

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

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

This issue occurs when you migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.3.0. When you perform delta migration, all host identifiers and authentication schemes appear in the assessment report, and the delta migration tries to create all host identifiers and authentication schemes again.

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

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

Oracle Fusion Middleware Migration Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) discusses how to migrate various Single Sign-On and Access Management environments to Oracle Access Management 11*g* Release 2 (11.1.2.3.0). You should use this guide for information about upgrade, migration, and coexistence procedures.

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

My Oracle Support document ID 1473025.1

4

Oracle Fusion Middleware Administration

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

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

4.1 General Issues and Workarounds

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

- Section 4.1.1, "Problems Using Oracle Database 12.2 with This Release"
- Section 4.1.2, "Clarification About Path for OPMN"
- Section 4.1.3, "Fusion Middleware Control May Return Error in Mixed IPv6 and IPv4 Environment"
- Section 4.1.4, "Limitations in Moving from Test to Production"

4.1.1 Problems Using Oracle Database 12.2 with This Release

When you use Oracle Database 12.2.*, you may run into the following issues:

- When you create an MDS database schema using RCU or upgrade the MDS database schema using Patch Set Assistant against Oracle Database 12.2, the operation may fail.

  You may receive the error `ORA-28104: input value for statement_types is not valid`. This is because, as part of a security fix beginning with Oracle Database 12.2, for the DBMS_RLS.ADD_POLICY procedure, statement types of INSERT and UPDATE_CHECK with a value of FALSE (the default value) are no longer allowed. It results in an ORA-28104 error while registering Virtual Private Database policies.

  This error is returned to avoid giving the impression that Virtual Private Database policy are enforced for INSERT statements, which is not the case.

  To workaround this, configure the system with `"_allow_inserts_with_UPDATE_CHECK"` set to True, by executing the following SQL command:

  ```
  ALTER SYSTEM SET "_allow_insert_with_update_check"=TRUE scope=spfile
  ```

Then, re-run RCU or the Patch Set Assistant to create or upgrade the MDS database schema.

- When you use Oracle Fusion Middleware with Oracle Database 12.2.*, you may encounter the following error:

  ```
  ORA-00932: inconsistent datatypes: expected SYS.AQ$_JMS_MESSAGE got
  SYS.AQ$_JMS_MESSAGE
  ```

  The error occurs because during enqueue and dequeue of AQ$_JMS_MESSAGE type, the version number sent to the database server maybe inconsistent. This happens when TOID (the type's unique identifier) for AQ$_JMS_MESSAGE type in type$ is a user-defined TOID and not a fixed SYSTEM defined TOID.

  To workaround this error, install the following patch, which replaces the ojdbc6.jar file used by Oracle Fusion Middleware:

  `https://updates.oracle.com/download/21663638.html`

  For Oracle Fusion Middleware 11*g*, select Release 11.1.1.7.0.

- When you install Oracle Fusion Middleware Release 11*g*R1 or Release 11*g*R2 products with Oracle Database 12.2.0.1, you may run into following error:

  ```
  ORA-28040: No matching authentication protocol
  ```

  This occurs because there is no 11*g* verifier for the proxy user.

  Use the following workaround to create the 11*g* Verifier and allow the connection to the 12.2.0.1 Oracle Database from the Oracle Fusion Middleware installation to proceed:

  1. Set ORACLE_HOME to the Oracle Database 12.2.0.1 Oracle home.
  2. Add the following line to the sqlnet.ora file (in *ORACLE_HOME*/network/admin):

     ```
     SQLNET.ALLOWED_LOGON_VERSION=11
     ```

  3. Connect to the database as sys as sysdba user and execute the following SQL commands:

     ```
     ALTER SYSTEM set sec_case_sensitive_logon=FALSE scope=spfile;
     shutdown immediate;
     startup;
     alter user sys identified by sys_password;
     alter user system identified by sys_password;
     ```

  If you want to use latest DB security features, you should not set SQLNET.ALLOWED_LOGON_VERSION=11. You can apply one of the two workarounds.

  Workaround 1: If Weblogic server is installed in MW_HOME, then perform the following:

  1. Set RCU_HOME environment variable. For example:

     Unix: `RCU_HOME=/stage/rcu/rcuHome; export RCU_HOME`

     Windows: `set RCU_HOME=\stage\rcu\rcuHome`

  2. Make a copy of `RCU_HOME/jdbc/lib/ojdbc6.jar`.
  3. Replace `RCU_HOME/jdbc/lib/ojdbc6.jar` with copy from WL_HOME:

Unix: `cp $WL_HOME/server/lib/ojdbc6.jar $RCU_HOME/jdbc/lib/`

Windows: `copy %WL_HOME%\server\lib\ojdbc6.jar %RCU_HOME%\jdbc\lib`

Workaround 2: Patch RCU with the DBCPUjul2015 patch:

1. Download the patch from the following location. It is in the form of a zip file. Unzip it.

   https://updates.oracle.com/download/20803573.html

2. Because the patch is based on Oracle Database 11.1.0.7 release, apply it on a 11.1.0.7.0 Oracle Database. In the directory in which you unzipped the patch, enter the following commands:

   ```
   setenv ORACLE_HOME oracle home of 11.1.0.7.0 db
   setenv PATH $ORACLE_HOME/OPatch:$PATH
   setenv PATH /usr/ccs/bin:$PATH
   ```

3. Execute following command to apply the patch from the patch unzipped directory:

   ```
   opatch napply -skip_subset -skip_duplicate
   ```

4. After the patch is applied, copy the following files to the *RCU_Home* to the specified directories:

File to Copy from Patched Database	Copy to This Location
ORACLE_HOME/jdbc/lib/ojdbc*.jar	*RCU_HOME*/jdbc/lib/ojdbc*.jar
ORACLE_HOME/lib/libclntsh.so.11.1	Copy to this location, renaming the file: *RCU_HOME*/lib/libclntsh.so.11.1 *RCU_HOME*/lib/libclntsh.so.10.1 *RCU_HOME*/lib/libclntsh.so
ORACLE_HOME/sqlplus/lib/*	Replace RCU_HOME/sqlplus/lib/*

Now RCU is patched with the security patch and can be used to install Oracle Fusion Middleware schemas.

4.1.2 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.

4.1.3 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.

4.1.4 Limitations in Moving from Test to Production

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

- After you run the extractMovePlan script, the move plan version shows 11.1.1.9. This does not cause any problems.
- If you upgraded Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.x or 11.1.1.7.x) to Adaptive Access Manager 11.1.2.3.0, the component versions of some packages packages still show 11.1.1.5.x. or 11.1.1.7.x. Those packages are:

  ```
  oracle.dogwood.top
  oracle.idm.oinav
  oracle.sdp.client
  oracle.oaam.suite
  oracle.oaam.oaam_admin
  oracle.oaam.oaam_server
  oracle.oaam.oaam_offline
  ```

  To resolve this, you must run the domain updater utility (com.oracle.cie.domain-update_1.0.0.0.jar). This step updates the domain-info.xml.. To upgrade the necessary Oracle Adaptive Access Manager packages to 11.1.2.3.0, complete the following steps:

1. Go to the directory *ORACLE_HOME*/oaam/upgrade. The domain updater utility com.oracle.cie.domain-update_1.0.0.0.jar file is located in this directory.
2. Upgrade the packages listed from 11.1.1.5(7).x to 11.1.2.3.0 by running the following command:

   ```
   java -cp
   $MW_HOME/utils/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
   _1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater DOMAIN_HOME
   PACKAGE_NAME:11.1.1.7.0,:11.1.2.3.0
   ```

   For example:

   ```
   java -cp
   /scratch/Oracle/Middleware/utils/config/10.3/config-launch.jar:./com.oracle
   .cie.domain-update_1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater
   /scratch/Oracle/Middleware/user_projects/domains/OAAMDomain
   oracle.dogwood.top:11.1.1.7.0,:11.1.2.3.0
   ```

3. Repeat the previous step for the other packages that show the version 11.1.1.5 or 11.1.1.7.

- If you have an IDS store configured in the source environment, and you plan to retain the same ID store host and port in the target environment without moving it, the pasteConfig script returns the following error:

  ```
  Specified host already configured in adapter
  ```

  To work around the problem, in the generated moveplan.xml, under configGroup LIBOVD_ADAPTERS, look for the configProperty representing the Identity Store that you do not plan to move. Comment out the entire section corresponding to the configProperty for your Identity Store in the move plan before you run the pasteConfig script.

- 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_Cor
  e_Application_Server.txt file
  ```

  Add the following entries:

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

- When you are moving Oracle Virtual Directory, the Oracle instance name in the source environment cannot be the same as the Oracle instance name in the target environment. The Oracle instance name in the target must be different than the name in the source.

- After you move Oracle Virtual Directory from one host to another, you must add a self-signed certificate to the Oracle Virtual Directory keystore and EM Agent wallet on Host B. Take the following steps:

  a. Set the ORACLE_HOME and JAVA_HOME environment variables.

  b. Delete the existing self-signed certificate:

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

  c. Generate a key pair:

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

  d. Export the certificate:

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

  e. Add a wallet to the EM Agent:

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

  f. Stop and start the Oracle Virtual Directory server.

  g. Stop and start the EM Agent.

- When you are moving Oracle Platform Security and you are using an LDAP store, the LDAP store on the source environment must be running and it must be accessible from the target during the pasteConfig operation.

- If you have configured WebGate with Oracle HTTP Server Release 11.1.1.6, you must apply the following patch to Oracle HTTP Server before you use the movement scripts:

  ```
  13897557
  ```

- The movement scripts do not support moving any releases of Oracle Identity Manager prior to *Release 11.1.2.1* to another environment, either through the movement scripts or manual steps. In addition, if any release of Oracle Identity Manager prior to *Release 11.1.2.1* is part of the source environment of other components, the movement scripts for that environment will fail.

- After you move Oracle Adaptive Access Manager, the database schema user name for Oracle Adaptive Access Manager will be changed only if OPSS data is not migrated as part of the copyConfig operation (specified using the opssdataexport parameter).

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

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

  In this case, take the following steps:

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

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

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

  You can ignore these errors.

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

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

  You can ignore these errors.

- The copyConfig script may return the following warnings:

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

You can ignore these warnings.

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

  ```
  portNumber
  SID
  serverName
  ```

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

- When you execute the pasteConfig script on an environment containing Oracle Adaptive Access Manager and a valid domain is does not exist, the pasteConfg steps are skipped and the script returns the following error:

  ```
  Not valid OAAM Domain. Skipping OAAM-specific copy configuration steps.
  ```

  The message should read:

  ```
  Not valid OAAM Domain. Skipping OAAM-specific paste configuration steps.
  ```

- After your run the copyConfig script for a domain containing Access Manager and Oracle Adaptive Access Manager, you may receive the following error, which you can ignore:

  ```
  javax.management.InstanceNotFoundException: java.lang:type=Runtime
  at weblogic.rjvm.ResponseImpl.unmarshalReturn(ResponseImpl.java:237)
  at weblogic.rmi.internal.BasicRemoteRef.invoke(BasicRemoteRef.java:223)
  at
  javax.management.remote.rmi.RMIConnectionImpl_1036_WLStub.getAttribute(Unknown
  Source)
  ```

- When you move a Web tier environment, the copyBinary script may return the following message:

  ```
  Warning Message  :1
    Nov 20, 2014 10:47:57 - WARNING - CLONE-20266   Unable to archive a file.
    Nov 20, 2014 10:47:57 - CAUSE - CLONE-20266   The file
  "/scratch/oracle/webtier6400/network/log/cgisock.9465" did not have
  sufficient permission to access.
    Nov 20, 2014 10:47:57 - ACTION - CLONE-20266   Correct the permission of
  above file and run copyBinary again.
  ```

  You can safely ignore this message.

4.2 Configuration Issues and Workarounds

There are no know configuration issues at this time

4.3 Documentation Errata

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

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

4.3.1 Documentation Errata for the *Administrator's Guide*

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

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

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

- Section 4.3.2.1, "JRockit SDK Not Certified for IDM"

4.3.2.1 JRockit SDK Not Certified for IDM

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

5 Oracle Access Management

This chapter describes issues associated with Oracle Access Management.

It includes the following topics:

- General Issues and Workarounds
- Configurations and Workarounds
- Oracle Access Management Console Issues
- Documentation Errata

5.1 General Issues and Workarounds

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

- General Issues and Workarounds: Access Manager
- General Issues and Workarounds: Security Token Service
- General Issues and Workarounds: Identity Federation
- General Issues and Workarounds: Mobile and Social
- General Issues and Workarounds: Access Portal Service

5.1.1 General Issues and Workarounds: Access Manager

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

- 10G & 32 BIT 11G WebGates Not Supported with SHA1/SHA2 Certificates (Cert Mode)
- Login Issue with Active Directory Over SSL
- SSO Global Logout Fails With Resource Secured By Public Policy
- Behavior Impact for Non-OIC (Oracle Identity Connect) Clients
- Specify Registered/Allowed Grant Types to Request OAuth Token
- IdmConfigTool Creates Weblogic Authentication Provider With Invalid Configuration
- OAM 11.1.2.2 WebGate Agents Not Supported with OAM 11.1.2.3 Server
- Access SDK Client Only Needs oamsdk-api.jar

- Oracle Access Management Console Only Displays 1000 Users in Search
- Anonymous User Must be Defined in Integrated OAM-OAAM Environment
- Names of Certain Access Manager Artifacts Will Not Be Localized
- Partial String + Wild Card (*) Doesn't Work with Authorization Rules Search
- Intermittent Issue with OAM and Coherence
- No Error Message Displayed When Login Page is Tunneled for DCC
- OAM OTP Mail for SFA Is Not Localized
- Can't Search GROUP When Active Directory Is Identity Store
- DCC Webgate Must be Configured to Tunnel when Using Federation

5.1.1.1 10G & 32 BIT 11G WebGates Not Supported with SHA1/SHA2 Certificates (Cert Mode)

If Oracle Access Management Access Manager 11.1.2.3.0 server is configured in Cert mode with SHA1/SHA2 certificate, 10g WebGate and 11.1.2.1.0/11.1.2.2.0 (32bit) WebGates are not supported.

5.1.1.2 Login Issue with Active Directory Over SSL

A login issue occurs with Active Directory when using an SSL connection. The current workaround for this is to use a non-SSL port for the ActiveDirectoryAuthenticator.

5.1.1.3 SSO Global Logout Fails With Resource Secured By Public Policy

SSO global logout fails if one of the participating resources is secured by OAM public policy. When Enterprise Content Management PS7 is used with OAM R2PS2 and the OAM ID Asserter is added as the authentication provider in which the action type is defined as an OAM_IDENTITY_ASSERTION token (rather than OAM_REMOTE_USER), SSO global logout fails.

5.1.1.4 Behavior Impact for Non-OIC (Oracle Identity Connect) Clients

When a user is authenticated with any Authentication Scheme using the LDAPNoPasswordModule Authentication Module, an authentication level of "0" is set for the user irrespective of the authentication level defined in the Authentication Scheme.

5.1.1.5 Specify Registered/Allowed Grant Types to Request OAuth Token

The registered/allowed grant types must be specified when an OAuth token is requested.

5.1.1.6 IdmConfigTool Creates Weblogic Authentication Provider With Invalid Configuration

By default, `idmConfigTool -configOAM` creates a Weblogic Authentication Provider with the following parameters:

- Static Group Object Class = groupofnames
- Static Member DN Attribute = member
- Static Group DNs from Member DN Filter = (&(member=%M)(objectclass=groupofnames))

If your Oracle Unified Directory (OUD) is using `groupofuniquenames` to define groups and `uniquemember` to define group members, this must be explicitly changed in the Weblogic Authentication Provider for OUD.

5.1.1.7 OAM 11.1.2.2 WebGate Agents Not Supported with OAM 11.1.2.3 Server

After the OAM server is upgraded to 11.1.2.3, the 11.1.1.6 orapki library is no longer available to insert certificates in OAM 11.1.2.2 WebGate agents.

WORKAROUND: After upgrading to OAM 11.1.2.3, run the following command to convert the wallet to a version compatible with components of 11.1.2.3.

```
orapki wallet convert [-wallet [wallet]] [-auto_login_only]
```

5.1.1.8 Access SDK Client Only Needs oamsdk-api.jar

As of this 11.1.2.3.0 release, the Access SDK client only needs to have `oamasdk-api.jar` in the classpath. This enhancement cause resulted in a documentation change. See Section 5.4.2.1, "Access SDK Documentation Update."

5.1.1.9 Oracle Access Management Console Only Displays 1000 Users in Search

When you search users in the identity store using the Oracle Access Management Console (Configuration -> Administration -> User search), a maximum of 1000 users is displayed even when the result contains more than 1000 users.

5.1.1.10 Anonymous User Must be Defined in Integrated OAM-OAAM Environment

Anonymous must be defined as a user in the default UID when coexistence and Multi-Data Center is enabled in an integrated OAM-OAAM environment.

5.1.1.11 Names of Certain Access Manager Artifacts Will Not Be Localized

Because they are values and not strings that can be translated, the names of Authentication Policies, Authentication Schemes, Authentication Modules and Authentication Plugins will not be localized.

WORKAROUND: These names can be edited.

5.1.1.12 Partial String + Wild Card (*) Doesn't Work with Authorization Rules Search

A partial string paired with a wild card (*) does not work when searching User or Groups in Authorization Rules. A notification error is not thrown when this occurs.

5.1.1.13 Intermittent Issue with OAM and Coherence

Normally when the Coherence server is started in SSL mode, it comes up on port 9095. This issue is encountered if Access Manager finds 9095 in use and starts Coherence on 9096. To alleviate this, make sure that port 9095 is open for the Coherence server.

5.1.1.14 No Error Message Displayed When Login Page is Tunneled for DCC

For an OAM-OAAM integrated environment (using TAP and the DCC to work, the following configurations must be done.

- Set the DCC app domain "/oam/**" to unprotected.
- Set "/favicon.ico" as an excluded resource.

5.1.1.15 OAM OTP Mail for SFA Is Not Localized

There is no globalization support for OTP mail in SFA. Although the mail subject and content can be edited in `AdaptiveAuthenticationPlugin` and `AdaptiveAuthenticationModule`, it applies to all users.

5.1.1.16 Can't Search GROUP When Active Directory Is Identity Store

If using Active Directory as your identity store, change the group objectclass to "group" rather than the default "groupofuniquenames".

5.1.1.17 DCC Webgate Must be Configured to Tunnel when Using Federation

Detached Credential Collector (DCC) HTTP Reverse Proxy feature has been introduced in the 11.1.2.2.0 release. This new DCC HTTP Reverse Proxy capability is different from the previous DCC for HTTP-Basic/FORM based login, with the latter not working for the Federation SSO flows (IdP or SP mode).

5.1.2 General Issues and Workarounds: Security Token Service

This topic describes general issues and workarounds for Oracle Access Management Security Token Service. There are none currently listed.

5.1.3 General Issues and Workarounds: Identity Federation

This topic describes general issues and workarounds for Oracle Access Management Identity Federation. There are none currently listed.

5.1.4 General Issues and Workarounds: Mobile and Social

This topic describes general issues and workarounds for Oracle Access Management Mobile and Social. There are none currently listed.

5.1.5 General Issues and Workarounds: Access Portal Service

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

- Application Can Still Be Delegated When Delegation Is Disabled

5.1.5.1 Application Can Still Be Delegated When Delegation Is Disabled

When an Administrator unchecks the delegation option using the Oracle Access Management Console, the Application can still be delegated. The workaround is to use the classic ESSO for enabling and disabling the delegation setting.

5.2 Configurations and Workarounds

This section describes configurations and workarounds organized around specific services. The following topics are included:

- Configurations and Workarounds: Access Manager
- Configurations and Workarounds: Security Token Service
- Configurations and Workarounds: Identity Federation
- Configurations and Workarounds: Mobile and Social

5.2.1 Configurations and Workarounds: Access Manager

This topic describes configurations and workarounds for Oracle Access Management Access Manager (Access Manager). It includes the following.

- Enabling ECID Context For Request Tracking
- Create A Server Entry for oam_policy_mgr1

5.2.1.1 Enabling ECID Context For Request Tracking

11.1.2.3 WebGate agents can send the execution context identifier (ECID) as a value of 'ECID-context' to the OAM server and receive a response containing the identifier in return. The ECID can help in end to end debugging of requests sent from the WebGate to OAM and returned responses. To enable ECID context set the following user-defined parameter to true in the 11g WebGate profile.

```
sendECIDResponse=true
```

5.2.1.2 Create A Server Entry for oam_policy_mgr1

Using the Oracle Access Management Console, create a server entry for the oam_policy_mgr1 node if it is targeted on a different machine than the AdminServer machine. Navigate through Configuration -> server instances from the Launch Pad. The hostname and port should match that of the oam_policy_mgr1 managed server node. Use the SSL Port, if enabled. The oam_policy_mgr1 node should only be started after creation of this server entry.

5.2.2 Configurations and Workarounds: Security Token Service

There are no configurations and workarounds for Oracle Access Management Security Token Service.

5.2.3 Configurations and Workarounds: Identity Federation

This topic describes configurations and workarounds for Oracle Access Management Identity Federation. It includes the following.

5.2.3.1 Enabling Federation with Mobile and Social

After Oracle Access Management is installed and configured with Mobile and Social, the Federation Service should be enabled but is not. To enable the Federation Service:

1. Login to the Oracle Access Management Console as Administrator.
2. Navigate through Configuration to access the Available Services.
3. Disable and re-enable the Mobile and Social Service.

   This action will enable the Federation Service.

5.2.4 Configurations and Workarounds: Mobile and Social

There are no configurations and workarounds for Oracle Access Management Mobile and Social.

5.3 Oracle Access Management Console Issues

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

- WebGate for OHS 12c Should Be Configured as 11g WebGates

5.3.1 WebGate for OHS 12c Should Be Configured as 11g WebGates

A WebGate is available for OHS 12c however the Oracle Access Management Console only lists 10g and 11g options. At this time, 12c WebGates should be configured as you would an 11g WebGate.

5.4 Documentation Errata

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

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

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

5.4.1 Administrator's Guide for Oracle Access Management

There are no documentation errata for Administrator's Guide for Oracle Access Management.

5.4.2 Developer's Guide for Oracle Access Management

This topic describes modifications made to the *Developer's Guide for Oracle Access Management*.

5.4.2.1 Access SDK Documentation Update

Due to changes in the oam-java-asdk.zip, the About Installing Access SDK section in chapter 2 of the *Developer's Guide for Oracle Access Management* has been modified.

6 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

6.1 General Issues and Workarounds

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

- Application Role Search Results are Wrong After Search External Role/Users from IDS Profile
- Attribute Default Value is Missing When Creating New Identity Directory Service Profile in and Upgraded 11g Release 2 (11.1.2.3) Environment

6.1.1 Application Role Search Results are Wrong After Search External Role/Users from IDS Profile

When using simple search in the Oracle Entitlements Server Administration Console to search for External Roles and Users of an Application bound to an Identity Directory Service profile, the search results for the Application Roles are incorrect. The issue occurs when the bound Application is not the first item in the Application drop-down list and you did not change the Application manually when you searched for Application Roles. To work around this issue, choose the application you want to search in drop-down box of simple search panel.

6.1.2 Attribute Default Value is Missing When Creating New Identity Directory Service Profile in and Upgraded 11g Release 2 (11.1.2.3) Environment

If you want to create an Identity Directory Service profile in an 11g Release 2 (11.1.2.3) environment that had been upgraded from 11g Release 2 (11.1.2.1), you must create the new IDS profile in the Oracle Entitlements Server Administration Console, and in the User section, enter `uid` in the Global Common ID Attribute field.

In 11g Release 2 PS1, the Global Common ID Attribute field did not exist. In 11g Release 2 (11.1.2.3) the Global Common ID Attribute value is required. If you do not enter a value in this field, an error message results when you try to create the Identity Directory Service profile.

6.2 Configuration Issues and Workarounds

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

- Running ./oesPassword.sh –initenroll Fails the First Time
- The WCC-OES Connector Fails to Install During Oracle WebCenter Content and Oracle Entitlements Server Integration in 11.1.2.3.0
- PD-Client Not Deployed to Administration Server If Managed Server is Configured

6.2.1 Running ./oesPassword.sh –initenroll Fails the First Time

When saving the identity/trust store password into the credential store, the `./oesPassword.sh -initenroll` command fails for Security Modules in controlled-push mode that use a third party digital certificate. The following error occurs:

```
oracle.security.jps.service.policystore.PolicyStoreException:
oracle.security.jps.service.policystore.PolicyStoreException:
java.security.UnrecoverableKeyException: Password must not be null
```

To work around this issue, you must run `./oesPassword.sh -initenroll` again to successfully save the password into the credential store.

6.2.2 The WCC-OES Connector Fails to Install During Oracle WebCenter Content and Oracle Entitlements Server Integration in 11.1.2.3.0

The WCC-OES Connector fails to install during Oracle WebCenter Content and Oracle Entitlements Server integration. To work around this issue, you must perform the following steps before installing the WCC-OES Connector ("Installing the WCC-OES Connector" in *Administering Oracle Entitlements Server*):

1. Back up `$OESCLIENT_HOME/oessm/ucmconnector/components/UCM_OES_Environment.cfg`.
2. Update `UCM_OES_Environment.cfg` to:

```
<?cfg jcharset="UTF8" encoding="UTF-8"?>
applicationName=UCM Application
crudResourceType=UCM CRUD Operation Resource Type
searchResourceType=UCM Pre-Search Query Resource Type
```

3. Copy it to the folder `$wcc_domain/ucm/cs/custom/UCMOESConnector/`.

6.2.3 PD-Client Not Deployed to Administration Server If Managed Server is Configured

The PD Client is deployed to the Managed Servers by default if you choose the **Oracle Entitlement Server Weblogic Security Module** template and configure the Managed Server for the domain when you run `config.sh`.

To work around this issue, when you run `config.sh` (located in *`OES_CLIENT_HOME`*`/oessm/bin)`, in the **Target Deployments to Clusters or Servers** page, click **AdminServer**, and then, choose the application **oracle.oes.client.pd.ssl#11.1.1.3.0** so that the PD Client is deployed to the Administration Server. You can also unchecked the Managed Servers from the target servers.

6.3 Documentation Errata

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

- Administering Oracle Entitlements Server
- Developer's Guide for Oracle Entitlements Server

6.3.1 Administering Oracle Entitlements Server

There are no issues to document for *Administering Oracle Entitlements Server*.

6.3.2 Developer's Guide for Oracle Entitlements Server

There are no issues to document for *Developer's Guide for Oracle Entitlements Server*.

7 Oracle Adaptive Access Manager

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

- General Issues and Workarounds
- Multi-Language Support Issues and Limitations
- Documentation Errata

7.1 General Issues and Workarounds

This section describes general issues and workarounds.

The following topics are included:

- Section 7.1.1, "Search for Device by Last Used On and with Registered Set as True Filters Returns No Results"
- Section 7.1.2, "ADF Exceptions When Starting the Admin and OAAM Admin Servers"
- Section 7.1.3, "OAAM Admin Log Contains Stack Trace of Canceling a Temporary Allow"
- Section 7.1.4, "Warnings and Error When Logging Out of the OAAM Admin Console"
- Section 7.1.5, ""Last Used On" Column Does Not Sort in Fingerprint Details Page"
- Section 7.1.6, "Altering the Schedule Parameters Does Not Affect Next Recurrence"

7.1.1 Search for Device by Last Used On and with Registered Set as True Filters Returns No Results

If you go to the OAAM Admin Console Sessions page, User Details, and Device tab, and search for a device by **Last Used On** date range, no results are returned if **Registered** is set as `True`.

7.1.2 ADF Exceptions When Starting the Admin and OAAM Admin Servers

After installing the Identity and Access Management Suite, ADF exceptions may appear in the OAAM output log when you start the Administration and OAAM Admin Servers. These exceptions do not impact functionality.

7.1.3 OAAM Admin Log Contains Stack Trace of Canceling a Temporary Allow

When you cancel a Temporary Allow, stack traces similar to the following example may appear in the OAAM Admin server log:

```
[2014-03-11T17:05:56.816-07:00] [oaam_admin_server1] [NOTIFICATION] []
[oracle.oaam] [tid: [ACTIVE].ExecuteThread: '4' for queue:
'weblogic.kernel.Default (self-tuning)'] [userId: csrm1] [ecid:
0000KInb1oEF0FGpIwH7if1J5wtY0001bm,0] [APP: oaam_admin#11.1.2.0.0] [DSID:
0000KIn_KpSF0FGpIwH7if1J5wtY0001_i] removeOverride().
vtUser=localUserId={10001}
extUserId={6_df4102a6a41ad6fed09942c3b1cf05a5a45796ab92436adf9bb6ee0c99965a1a}

@ loginId={usercsr} groupId={1} isValid={true} createTime={Fri Mar 07
16:17:38 @ PST 2014} updateTime={Tue Mar 11 17:05:41 PDT 2014} firstLoginTime={Fri
Mar 07 16:17:38 PST 2014} notes={null}
cache={G:84|O:2=2,1=2|F:10001=10003,10002=10003,10006=10007,10007=10007} ,
runtime=1, action=Block[[java.lang.Throwable
at
com.bharosa.vcrypt.dataaccess.util.VCryptCacheUtil.removeOverride(VCryptCacheUtil.
java:204)
at com.bharosa.vcrypt.tracker.rules.util.RulesUtil.removeFromUserCache(RulesUtil.
java:692)
at
com.bharosa.vcrypt.tracker.rules.util.RulesUtil.deleteOverride(RulesUtil.java:728)
at com.bharosa.vcrypt.tracker.rules.util.RulesUtil.clearOverrides(RulesUtil.java:
405)
at com.bharosa.vcrypt.tracker.rules.util.RulesUtil.clearOverrides(RulesUtil.java:
394)
at com.bharosa.vcrypt.customercare.CaseActions.clearTempAllow(CaseActions.java:31
5)
at oracle.oaam.server.admin.cases.impl.CustomerCareManagerImpl.actOnCase(Customer
CareManagerImpl.java:4015)
at
oracle.oaam.server.admin.cases.impl.CustomerCareManagerImpl.performCaseAction(Cust
omerCareManagerImpl.java:3851)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:
25)
at java.lang.reflect.Method.invoke(Method.java:597)
at
oracle.oaam.server.admin.impl.AdminInterceptorProxy.invoke(AdminInterceptorProxy.j
ava:74)
at $Proxy131.performCaseAction(Unknown Source)
at
oracle.oaam.model.customercare.uview.CaseActionVOImpl.doCaseAction(CaseActionVOImp
l.java:344)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
```

The stack trace does not impact functionality.

7.1.4 Warnings and Error When Logging Out of the OAAM Admin Console

When you try to log out of the OAAM Administration Console, you might encounter warnings and an error similar to the following example in the Oracle Adaptive Access Manager server log:

```
[2014-02-21T15:50:28.689-08:00] [oaam_admin_server1] [WARNING]
```

```
[ADF_FACES-00007] [oracle.adf.view.rich.render.RichRenderer] [tid:
[ACTIVE].ExecuteThread: '11' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: ruleAdmin1] [ecid:
0000KHMqrkmF0FGpIwH7if1J1y0Q00006I,0] [APP: oaam_admin#11.1.2.0.0] [DSID:
0000KHMpfB5F0FGpIwH7if1J1y0Q000068] Attempt to synchronized unknown key:
viewportSize.
[2014-02-21T15:50:28.726-08:00] [oaam_admin_server1] [WARNING] []
[oracle.adf.share.ADFContext] [tid: [ACTIVE].ExecuteThread: '17' for queue:
'weblogic.kernel.Default (self-tuning)'] [userId: ruleAdmin1] [ecid:
0000KHMqrlqF0FGpIwH7if1J1y0Q00006J,0] [APP: oaam_admin#11.1.2.0.0] [DSID:
0000KHMpfB5F0FGpIwH7if1J1y0Q000068] Automatically initializing a
DefaultContext for getCurrent.[[
Caller should ensure that a DefaultContext is proper for this use.
Memory leaks and/or unexpected behaviour may occur if the automatic
initialization is performed improperly.
This message may be avoided by performing initADFContext before using
getCurrent().
For more information please enable logging for oracle.adf.share.ADFContext at
FINEST level.
]]
[2014-02-21T15:50:28.728-08:00] [oaam_admin_server1] [WARNING] []
[oracle.adf.share.http.ServletADFContext] [tid: [ACTIVE].ExecuteThread: '17'
for queue: 'weblogic.kernel.Default (self-tuning)'] [userId: ruleAdmin1]
[ecid: 0000KHMqrlqF0FGpIwH7if1J1y0Q00006J,0] [APP: oaam_admin#11.1.2.0.0]
[DSID: 0000KHMpfB5F0FGpIwH7if1J1y0Q000068] Found
oracle.adf.share.DefaultContext sticking to oldContext, while the current
application is oaam_admin(11.1.2.0.0)
[2014-02-21T15:50:28.741-08:00] [oaam_admin_server1] [WARNING] []
[oracle.adf.share.http.ServletADFContext] [tid: [ACTIVE].ExecuteThread: '17'
for queue: 'weblogic.kernel.Default (self-tuning)'] [userId: ruleAdmin1]
[ecid: 0000KHMqrlqF0FGpIwH7if1J1y0Q00006J,0] [APP: oaam_admin#11.1.2.0.0]
[DSID: 0000KHMpfB5F0FGpIwH7if1J1y0Q000068] Found
oracle.adf.share.DefaultContext sticking to oldContext, while the current
application is oaam_admin(11.1.2.0.0)
[2014-02-21T15:50:28.743-08:00] [oaam_admin_server1] [ERROR] []
[oracle.adf.share.ADFContext] [tid: [ACTIVE].ExecuteThread: '17' for queue:
'weblogic.kernel.Default (self-tuning)'] [userId: <WLS Kernel>] [ecid:
0000KHMqrlqF0FGpIwH7if1J1y0Q00006J,0] ADF detected an ADFContext leak.[[
Please see the documentation for more information about handling ADFContext
leaks.
For more information about the leaking ADFContext please enable logging for
oracle.adf.share.ADFContext at FINEST level.
```

The OAAM Server log is located in the following directory:

```
WL_HOME/user_projects/domains/domainName/servers/serverName/logs/serverName-diagno
stic.log
```

You can ignore the warnings and error. They do not impact any functionality.

7.1.5 "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.

7.1.6 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.

7.2 Multi-Language Support Issues and Limitations

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

- Section 7.2.1, "OAAM Admin Console Is Non-Responsive When an Unsupported Language is Set in the Browser"
- Section 7.2.2, "Save Search in Properties Page Fails with Some Thai Characters"

7.2.1 OAAM Admin Console Is Non-Responsive When an Unsupported Language is Set in the Browser

When an unsupported language is set in the browser, the OAAM Admin Console may become non-responsive and the Navigation Tree menu and toolbar may not be displayed.

7.2.2 Save Search in Properties Page Fails with Some Thai Characters

When you try to save a search in a properties page with a name containing Thai characters that are in \u0E31 or \u0e35 format, an error similar to the following example may appear in the server log file:

```
<Error> <oracle.adfinternal.view.faces.config.rich.RegistrationConfigurator>
<BEA-000000> <ADF_FACES-60096:Server Exception during PPR, #1
oracle.jbo.JboException: JBO-29114 ADFContext is not setup to process
messages for this exception. Use the exception stack trace and error code to
investigate the root cause of this exception. Root cause error code is
JBO-29000. Error message parameters are
{0=oracle.xml.parser.v2.XMLDOMException, 1=invalid character \u0e35 in name}
at oracle.jbo.server.Serializer.passivate(Serializer.java:270)
at oracle.jbo.server.DBSerializer.passivateRootAM(DBSerializer.java:293)
at oracle.jbo.server.DBSerializer.passivateRootAM(DBSerializer.java:268)
```

7.3 Documentation Errata

This section contains documentation errata for *Oracle Fusion Middleware Administering Oracle Adaptive Access Manager*.

7.3.1 Table and Column Combinations Needed to Derive Email/SMS Challenges for Specified Time

To derive email/SMS challenges for a specified time, use the `VT_SESSION_ACTION_MAP` table and `action` and `action_list` columns.

In `VT_SESSION_ACTION_MAP` table, the actions and actions list are stored in the following `action` and `action_list` columns:

DB name	Data type	Description
MAP_ID	NOT NULL NUMBER(16)	Map ID
CREATE_TIME	TIMESTAMP(6)	Date/time of the creation of the object
RUNTIME_TYPE	NOT NULL NUMBER(6)	Type of runtime
ACTION	VARCHAR2(256)	Actions for this runtime and session
ACTION_LIST	VARCHAR2(256)	List of action.

To obtain the actions for a given time range, use `create_time`.

To obtain actions for the challenge runtime, filter by `runtime_type` = *`number_for challenge_runtime`*.

8 Oracle Mobile Security Suite

This chapter describes issues associated with Oracle Mobile Security Suite (OMSS).

It includes the following topics:

- General Issues and Workarounds
- Configuration Issues and Workarounds

8.1 General Issues and Workarounds

This section is organized by component.

- General Issues and Workarounds
- General Issues and Workarounds: Mobile Security Manager (MSM)
- General Issues and Workarounds: Mobile Security Access Server (MSAS)
- General Issues and Workarounds: Secure Workspace App for iOS
- General Issues and Workarounds: Secure Workspace App for Android
- General Issues and Workarounds: App Containerization Tool for iOS
- General Issues and Workarounds: App Containerization Tool for Android

8.1.1 General Issues and Workarounds

This section documents issues that are not component specific. It includes the following topic:

- Transfer to Production (T2P) is not Currently Supported for OMSS PS3
- Windows is not Supported

8.1.1.1 Transfer to Production (T2P) is not Currently Supported for OMSS PS3

Moving Oracle Mobile Security Suite artifacts from a test environment to a production environment is not supported. After testing, administrators should deploy Oracle Mobile Security Suite in the production environment and manually recreate configurations and policies in the new environment.

8.1.1.2 Windows is not Supported

This release of Oracle Mobile Security Suite does not support the Windows platform.

8.1.2 General Issues and Workarounds: Mobile Security Manager (MSM)

This section includes the following topics:

8.1.2.1 Distribution Details Do Not Immediately Appear When Uploading an Android App Binary

When uploading an Android App binary to the Mobile Security Manager App Catalog, the apps details (package name, version, etc) will not immediately be populated on the current screen. Once you save the app and view it again the app details will be present.

8.1.2.2 Users with an Asterisk Character in their User Name are Not Mapped to Roles

If a user account in LDAP has an asterisk character (*) in its user name, then it will not be mapped to roles in Mobile Security Manager correctly. The workaround is to avoid using the asterisk character in user names.

8.1.2.3 Deselecting Device Details from the Policy Applicable to a Given Device Does not Result in the Removal of some MDM Policy Elements on the Device

Mobile Security Manager only enforces mobile device management (MDM) configuration, policies, and restrictions when **Specify device details for this policy** is selected in the Mobile Security Policy definition. If a given device has been registered with MDM using an applicable policy that has the device details specified, but then subsequently the policy is updated to deselect **Specify device details for this policy**, the associated MDM device configuration is not automatically removed and it is still possible to send commands (such as, **Lock**, **Wipe**, **Sync**) to the device.

8.1.2.4 A Single Microsoft Exchange Server is Supported for Push Notifications

The Mobile Security Manager server setting for Microsoft Exchange push notifications is global across all mobile security policies. It is not possible to configure a different Microsoft Exchange server setting for different mobile security policies.

8.1.2.5 Searching Policies by Roles is Case Sensitive

Searching Mobile Security Policies by the name of the assigned mobile roles is a case-sensitive search, while searching Mobile Security Policies by other attributes, such as the policy name, is not. The workaround is to search policies using case-sensitive role names.

8.1.2.6 Not Possible to Cancel an App Upload In Progress

When uploading an app binary to the Mobile Security Manager App Catalog, it is not possible to cancel the upload once it is in progress. Clicking **Cancel** will close the current dialog, but the app will finish uploading in the background.

8.1.2.7 User and Role Searches Display a Maximum of 1000 Results

When you search for users or roles in Mobile Security Manager, a maximum of 1000 users or roles is displayed even when the search matches more than 1000 results. The workaround is to update the search criteria so that the search matches less than 1000 results.

8.1.3 General Issues and Workarounds: Mobile Security Access Server (MSAS)

This section includes the following topics:

- JPS-06514 and JPS-06619 Warning Messages in MSAS Log Files
- Deleting a MSAS Instances Does Not Remove OAuth Clients and WebGate Configuration from OAM
- Error Using Same Logical MSAS Instance ID After OAM Test-to-Production (T2P)
- MSAS Console UI Does Not Display Properly on Mobile Devices
- OMSS Console UI Suggests an RSA 1024-Bit Key By Default
- MSAS Console Does Not Provide Host Header Configuration Option for Reverse Proxies
- The WLST displayIdentityProfile Command Includes TERM_CHAR in the Output
- Using the Same Name for Different URLs in a Proxy Application Causes Unexpected Runtime Behavior
- SSO to Oracle Access Manager Distributed Credential Collector is Not Supported

8.1.3.1 JPS-06514 and JPS-06619 Warning Messages in MSAS Log Files

The MSAS log files contain warning messages such as the following:

```
WARNING: JPS-06514 Opening of file based keystore failed.
WARNING: JPS-06619 Key store file keystores.xml integrity check failed.
```

Messages with the codes "WARNING: JPS-06514" and "WARNING: JPS-06619" can be safely ignored.

8.1.3.2 Deleting a MSAS Instances Does Not Remove OAuth Clients and WebGate Configuration from OAM

When `configMSAS.sh` is used to configure a MSAS instance, it will attempt to automatically register OAuth clients and a WebGate configuration for the MSAS instance in Oracle Access Manager. When that MSAS instance is later deleted, it does not automatic remove the previously registered OAuth clients and WebGate configuration. The workaround is to delete the OAuth clients and WebGate configuration manually using the OAM console UI.

8.1.3.3 Error Using Same Logical MSAS Instance ID After OAM Test-to-Production (T2P)

Oracle Access Manager and Oracle Mobile Security Suite are installed together in this release. When the OAM Test-to-Production (T2P) process is followed to transfer the OAM configuration from a source environment to a destination environment, it also transfers some configuration elements for the Mobile Security Access Server. This creates a conflict in the destination environment, such that performing the standard Oracle Mobile Security Suite configuration process in the destination environment will fail if the same logical MSAS instance ID is chosen in the destination environment as that which was previously used in the source environment. The workaround is to choose a different logical MSAS instance ID in the destination environment and not reuse the logical MSAS instance ID that which was used in the source environment.

8.1.3.4 MSAS Console UI Does Not Display Properly on Mobile Devices

The MSAS console UI does not display properly on mobile devices. To view the MSAS console UI, the workaround is to use a desktop web browser that is certified to work with the OAM Policy Manager console.

8.1.3.5 OMSS Console UI Suggests an RSA 1024-Bit Key By Default

A number of screens in the Oracle Mobile Security Suite console UI suggest an RSA 1024-bit key by default for new public key creation. The standard Oracle security recommendation is to use RSA 2048-bit minimum key-length keys. The workaround is to change the default selection to use RSA 2048-bit keys or larger.

8.1.3.6 MSAS Console Does Not Provide Host Header Configuration Option for Reverse Proxies

The MSAS console does not provide an option to switch the host header between MSAS and the backend, which only impacts JWT client policies attached on reverse proxies (on invoke). To prevent the JWT audience restriction check from failing due to this issue, set the `audience.uri` property to `None` for attached JWT client policies.

8.1.3.7 The WLST displayIdentityProfile Command Includes TERM_CHAR in the Output

The display output of `displayIdentityProfile` command includes `TERM_CHAR` in the output in place of new line characters. These extraneous `TERM_CHAR` can be ignored.

8.1.3.8 Using the Same Name for Different URLs in a Proxy Application Causes Unexpected Runtime Behavior

When you create a proxy application, do not use the same proxy name for multiple different URLs. Doing so will cause unexpected behavior at runtime.

8.1.3.9 SSO to Oracle Access Manager Distributed Credential Collector is Not Supported

Oracle Mobile Security Suite supports SSO to Oracle Access Manager when the OAM login page is exposed using the Embedded Credential Collector mode. SSO to the OAM login page is *not* supported when it is exposed using the Distributed Credential Collector mode.

8.1.4 General Issues and Workarounds: Secure Workspace App for iOS

This section includes the following topics:

- Unable to Play Videos Online
- No Audio for Video Files When Vibrate Mode is Enabled
- Catalog Apps Appear on Secure Workspace App Home Page When Min OS Version Higher Than the Mobile Device

- Secure Workspace Falls Back to English With Unsupported Region
- Customizable Workspace Name is Not Localized in the Device Language
- User can Toggle the Turn off Passcode Setting on a Managed Device
- In iOS Settings, the Workspace App may Need a Moment to Appear

8.1.4.1 Unable to Play Videos Online

Trying to play an online video file hosted on a website in the Secure Browser results in an error. The workaround is to download the video file locally and then play it.

8.1.4.2 No Audio for Video Files When Vibrate Mode is Enabled

There is no audio while playing local video files in the Secure Browser if the hardware vibrate mode has been enabled on the iOS device. The workaround is to turn off vibrate mode.

8.1.4.3 Catalog Apps Appear on Secure Workspace App Home Page When Min OS Version Higher Than the Mobile Device

If the **Install on Homepage** policy setting is enabled, apps will appear on the Secure Workspace app homepage even if they should be blocked because the device OS does not meet the minimum required by the **Min OS Version** policy setting. The workaround is to not set **Install on Homepage** for mobile apps with a **Min OS Version** restriction, and to instead allow users to install the mobile apps from the dynamic catalog, where the **Min OS Version** restriction is properly applied.

8.1.4.4 Secure Workspace Falls Back to English With Unsupported Region

If the configured device language does not match one of the languages that the app is localized for, the Secure Workspace app reverts to English. The app also reverts to English if the device language is set to a supported language, but the region is unsupported. The workaround is to either set the device language to a supported language and a supported region, or to not configure the region at all.

8.1.4.5 Customizable Workspace Name is Not Localized in the Device Language

When customizing the Secure Workspace app with a different app name, only a single name in a single language is supported. If different names are desired for different languages, then the workaround is to create a separate customized version of the app for each language.

8.1.4.6 User can Toggle the Turn off Passcode Setting on a Managed Device

After registering a managed device, the user can select the "Turn Passcode off" setting, however, the device forces the user to reset the passcode again. Due to the limitations of the iOS 7.*x* MDM API, the "Turn Passcode off" setting cannot be completely disabled.

8.1.4.7 In iOS Settings, the Workspace App may Need a Moment to Appear

The list of apps under Settings load dynamically in iOS 9. Consequently, the Workspace app may take a moment to appear in the list of apps on the iOS Settings screen.

8.1.5 General Issues and Workarounds: Secure Workspace App for Android

This section includes the following topics:

- Progress Dialog Dismissed Temporarily While Logging In
- Existing Tabs Close When Opening a vApp in the Secure Browser
- Customizable Workspace Name is Not Localized in the Device Language
- Talkback Accessibility Feature on Android Devices Does Not Properly Announce Password Characters

8.1.5.1 Progress Dialog Dismissed Temporarily While Logging In

During the Secure Workspace app login process when MDM is not enabled the "Logging in" progress dialog will be dismissed temporarily and then reappear. There is no functional impact to this temporary dismissal.

8.1.5.2 Existing Tabs Close When Opening a vApp in the Secure Browser

Opening a virtual app in the Secure Browser will cause any previously opened browser tabs to be closed.

8.1.5.3 Customizable Workspace Name is Not Localized in the Device Language

When customizing the Secure Workspace app with a different app name, only a single name in a single language is supported. If different names are desired for different languages then the workaround is to create a separate customized version of the app for each language.

8.1.5.4 Talkback Accessibility Feature on Android Devices Does Not Properly Announce Password Characters

When Talkback is enabled and headphones are in use, Talkback should announce the characters in the password field. On many Android devices, however, Talkback says "dot" instead of speaking the character name. This is not a Secure Workspace bug but a known limitation that affects many Android devices.

8.1.6 General Issues and Workarounds: App Containerization Tool for iOS

This section includes the following topics:

- Streaming of Video Not working
- Socket-Level Secure Networking Not Supported
- Saving Images to Local Gallery Cannot Be Restricted
- Xamarin Apps with UI Storyboards do not Containerize Properly
- App Containerization Tool for iOS Not Localized
- To Avoid Touch ID Crashes, Use the 11.1.2.3.1 Tool to Re-Containerize Apps That Were Containerized With the Older Version 3 Tool

8.1.6.1 Streaming of Video Not working

Trying to play an online video file hosted on a website in a containerized app results in an error. The workaround is to download the video file locally and then play it.

8.1.6.2 Socket-Level Secure Networking Not Supported

Secure networking for apps directly using socket-level communication primitives is not supported.

8.1.6.3 Saving Images to Local Gallery Cannot Be Restricted

It is not possible to restrict the ability to save images from a containerized app presenting the **Save Image** feature of QLPreviewController, even if the **Save image to local gallery** restriction is enabled on Mobile Security Manager.

8.1.6.4 Xamarin Apps with UI Storyboards do not Containerize Properly

A Xamarin app that uses a UI storyboard will show a blank screen or crash after it has been containerized. The workaround is to not use UI storyboards when writing Xamarin apps.

8.1.6.5 App Containerization Tool for iOS Not Localized

The App Containerization tool is not localized. All text is displayed in English regardless of the locale set in the OSX terminal window.

8.1.6.6 To Avoid Touch ID Crashes, Use the 11.1.2.3.1 Tool to Re-Containerize Apps That Were Containerized With the Older Version 3 Tool

Apps with version 3.0.*n* containerization crash upon launching if the iOS Touch ID feature is enabled. To fix this issue, re-containerize apps using the 11.1.2.3.1 App Containerization Tool. Until all containerized apps are upgraded to 11.1.2.3.1 containerization, turn Touch ID off.

8.1.7 General Issues and Workarounds: App Containerization Tool for Android

This section includes the following topics:

- Some Non-Containerized Apps Still Appear when File Share is Restricted
- Redirect from Container Policy is Not Implemented
- Socket-Level Secure Networking Not Supported
- Apps Exposing Document Providers are Not Listed When Containerized
- Homescreen Widgets of Containerized Apps Do Not Load
- App Containerization Tool for Android Not Localized

8.1.7.1 Some Non-Containerized Apps Still Appear when File Share is Restricted

When the Secure Workspace policy is set to restrict file sharing, some non-containerized apps may still appear in the list of available apps on Android. Attempting to select one of these non-containerized apps will, however, result in encrypted data being accessed by the app. There is no leakage of un-encrypted data.

8.1.7.2 Redirect from Container Policy is Not Implemented

The Secure Workspace policy to allow or disallow redirects from web pages displayed within the Secure Workspace app to other apps using custom URL schemes is not implemented on Android.

8.1.7.3 Socket-Level Secure Networking Not Supported

Secure networking for apps directly using socket-level communication primitives is not supported.

8.1.7.4 Apps Exposing Document Providers are Not Listed When Containerized

Apps that implement the document provider interface of the Android storage access framework will not appear in the **Open From** list in other mobile apps after being containerized.

8.1.7.5 Homescreen Widgets of Containerized Apps Do Not Load

When you install a containerized app on Android that support widgets, and then drag one of its widgets to the Android home screen, it results in a "Problem Loading Widget" error when the widget is opened.

8.1.7.6 App Containerization Tool for Android Not Localized

The App Containerization tool is not localized. All text will be displayed in English regardless of the locale set in the OSX terminal window.

8.2 Configuration Issues and Workarounds

This section is organized by component.

- Configuration Issues and Workarounds: Mobile Security Manager (MSM)
- Configuration Issues and Workarounds: Mobile Security Access Server (MSAS)

8.2.1 Configuration Issues and Workarounds: Mobile Security Manager (MSM)

This section includes the following topic:

- Patch Requirements for WebLogic 10.3.6.0.10

8.2.1.1 Patch Requirements for WebLogic 10.3.6.0.10

Oracle Mobile Security Suite 11g Release 2 (11.1.2.3.0) requires the following patches to be applied on top of WebLogic 10.3.6.0.10 after installation.

- 13856604: NEW TIMEOUT PROPERTY REQUIRED FOR HTTPRESPONSE INSTEAD OF COMPLETEMESSAGETIMEOUT
- 15865825: DISABLE BASIC AUTH FOR OWSM WHILE KEEP BACKWARD COMPATIBILITY
- 14809365: HTTP BASIC AUTHENTICATION FOR WLS WS STACK

To obtain a patch from My Oracle Support (formerly OracleMetaLink), go to the following URL, click **Patches and Updates**, and search for the patch number:

https://support.oracle.com/

8.2.2 Configuration Issues and Workarounds: Mobile Security Access Server (MSAS)

This section includes the following topic:

- idmConfigTool Fails When Logical MSAS Instance ID Does Not Exist
- Short Name for OAM / OAuth Host Must Be Used for SSL Configuration with the WebLogic Server Demo Identity Certificate

8.2.2.1 idmConfigTool Fails When Logical MSAS Instance ID Does Not Exist

The idmConfigTool `-configOMSS mode=OMSAS` command will fail with the following error if the logical MSAS instance ID present in the idmConfigTool properties file does not match the logical MSAS instance ID present in the configMSAS.sh properties file when configMSAS.sh was previously executed.

```
(1/4) Configuring OMSAS Identity Profile Error
[oracle.wsm.cli.CommandLineException: WSM-15013 : No session to abort.]
```

When this failure occurs, the IDS profile for Mobile Security Access Server may be created and result in a further error if the idmConfigTool properties file is subsequently updated to use the correct logical MSAS instance ID, and idmConfigTool `-configOMSS mode=OMSAS` is executed again. The workaround is either to update the idmConfigTool properties file to use a new IDS profile name, or delete the previously created IDS profile using WLST commands.

8.2.2.2 Short Name for OAM / OAuth Host Must Be Used for SSL Configuration with the WebLogic Server Demo Identity Certificate

The Oracle Access Manager configuration for SSL can use the WebLogic Server demo identity certificate by default. This demo identity certificate only includes the short name of the server host, not the fully-qualified domain name. For MSAS to connect to Oracle Access Manager over SSL (including the OAuth server) when the demo identity certificate is used, it is necessary for MSAS to be configured with the short name of the Oracle Access Manager and/or OAuth server host, and not the fully-qualified domain name.

This applies to the `OAM_HOST` and `OAUTH_HOST` properties used by `configMSAS.sh`, and the OAuth2 Confidential Client and OAuth2 Mobile Client authentication endpoints, which can be configured in the MSAS console by opening the **Environments -> Instances -> <*gateway instance*> -> Authentication Endpoints** page and updating the **OAuth2 Confidential Client: Endpoint** and **OAuth2 Mobile Client: Endpoint** parameters.

9 Oracle Privileged Account Manager

This chapter describes issues associated with Oracle Privileged Account Manager.

This information includes the following topics:

- What's New in Oracle Privileged Account Manager 11g Release 2 (11.1.2.3.0)
- General Issues and Workarounds
- Configuration Issues and Workarounds
- Documentation Errata

9.1 What's New in Oracle Privileged Account Manager 11*g* Release 2 (11.1.2.3.0)

Oracle Privileged Account Manager 11*g* Release 2 (11.1.2.3.0) has the following key new features:

- Section 9.1.1, "Support for Connector Servers"
- Section 9.1.2, "Support for New Targets"
- Section 9.1.3, "Support for Windows Session Recording Using the Windows Agent"
- Section 9.1.4, "Enhanced Session Recording Capabilities"
- Section 9.1.5, "Enhanced Password Checkout Capabilities"
- Section 9.1.6, "Support for Resource Groups"
- Section 9.1.7, "Enhanced Reporting Capabilities"
- Section 9.1.8, "Enhanced Plug-In Framework"
- Section 9.1.9, "Enhanced Usage Policies"
- Section 9.1.10, "Improved UI in the Oracle Privileged Account Manager Console"

9.1.1 Support for Connector Servers

Support has been added for the use of connector servers. Users can configure and manage connector servers in Oracle Privileged Account Manager to work with different connectors and their associated targets.

9.1.2 Support for New Targets

Support has been added for the use of additional targets. Users can configure Oracle Privileged Account Manager to use and work with the Windows, SSH, SAP UM, and SAP UME targets.

9.1.3 Support for Windows Session Recording Using the Windows Agent

Oracle Privileged Account Manager provides a session recording playback for Windows targets. This feature is capable of reading the session data from the Oracle Privileged Account Manager Server and replaying it as a video. This enhanced session recording functionality makes it possible to replay the session even from the execution of a specific event of interest. For every event, a clickable link is provided, which enables the user to play the session video from that point. This functionality is made available through the use of an agent configured for Windows targets. This agent for Windows targets or Windows agent is deploy directly on the target with which Oracle Privileged Account Manager interacts. The agent enables the recording and playback of events.

9.1.4 Enhanced Session Recording Capabilities

Oracle Privileged Account Manager provides a session transcript for SSH sessions. The transcript contains a region where the transcript text is loaded and another region which contains an outline of all the commands issued to the target system along with the timestamps. Each command in the outline is clickable link and when clicked, it points to the relevant region of the transcript where the command was used or occurs.

9.1.5 Enhanced Password Checkout Capabilities

Oracle Privileged Account Manager provides the ability to directly copy a password to a clipboard when an account is checked out. Therefore, the need to display the password on the screen in plain text is reduced. A user can click a button in the UI to copy the password to the clipboard. The user can also clear the copied password from the clipboard using the clear clipboard functionality, after the password has been used.

9.1.6 Support for Resource Groups

Oracle Privileged Account Manager provides support for administrators to create, modify, and delete resource groups which contain a group of resources. This allows administrators to delegate their administration privileges on resource groups to other users and roles. Oracle Privileged Account Manager also provides support for managing delegated administration in Oracle Privileged Account Manager interfaces such as REST APIs, Oracle Privileged Account Manager Console, and the Oracle Privileged Account Manager command line tool.

9.1.7 Enhanced Reporting Capabilities

Oracle Privileged Account Manager provides enhanced reporting capabilities that present data visualizations such as bar graphs and pie charts, comprehensive reports about account name, target name, target type, user, checkout type, checkout date, recording and other vital data about actions performed in Oracle Privileged Account Manager.

9.1.8 Enhanced Plug-In Framework

Oracle Privileged Account Manager provides additional filtering rules to help the manageability of and reduce the logic required in plug-in implementation. The support for retry operations also provides fault tolerance during network unavailability, host down, and similar situations. While configuring plug-ins, the display of required custom attributes and defaults using the create-like function enables users to create similar or configure new plug-ins easily.

9.1.9 Enhanced Usage Policies

Oracle Privileged Account Manager provides support for administrators to limit the actions that a user with access to a session is capable of performing. These limits or constraints can be applied at different levels. The constraints holds control over SSH or SCP sessions, Interactive or Non-Interactive modes within SSH sessions, and command-level actions. Administrators can specify replacements for commands and also enable these constraints by configuring or extending the usage policies.

9.1.10 Improved UI in the Oracle Privileged Account Manager Console

The user interface (UI) of the Oracle Privileged Account Manager console has been improved to present a simplified design and minimalistic design elements. The new UI enables ease of access and clear presentation of data. The UI also features changes within the console to accommodate the addition of new features within this release of Oracle Privileged Account Manager.

9.2 General Issues and Workarounds

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

- Section 9.2.1, "No Translation (Messages or Help) Support for OPAM Command Line Tools"
- Section 9.2.2, "Deprecated Features for Oracle Privileged Account Manager Restful API"
- Section 9.2.3, "Thread Count Continuously Increases During Oracle Privileged Session Manager Session Checkouts"
- Section 9.2.4, "Unlimited Tablespace Privilege Missing When Using Oracle Database 12.1"
- Section 9.2.5, "Session Checkout Does Not Appear In "My Checkouts""
- Section 9.2.6, "A User With an Application Configurator Role Cannot Duplicate an Active Plug-In"
- Section 9.2.7, "Issues After Upgrading From Oracle Privileged Session Manager 11g Release 2 Patchset 1 to Oracle Privileged Session Manager 11g Release 2 Patchset 3"

9.2.1 No Translation (Messages or Help) Support for OPAM Command Line Tools

Oracle Privileged Account Manager command-line tool messages and help were not translated in the Oracle Privileged Account Manager 11.1.2.0.0 release.

Translation support for the Oracle Privileged Account Manager command-line tool messages and help will be provided after the 11.1.2.0.0 release.

9.2.2 Deprecated Features for Oracle Privileged Account Manager Restful API

The following table lists the Oracle Privileged Account Manager RESTful APIs that were available in the Oracle Fusion Middleware 11g Release 2 (11.1.2.1.0) release and then deprecated in 11g Release 2 (11.1.2.2.0). In addition, this table lists the new, equivalent APIs and provides links to topics in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager* that describe how to use the new APIs.

Deprecated API (11gr2 11.1.2.1.0)	New API (11gr2 11.1.2.2.0)	Refer to This Topic
`Show Service Account Password` in the Target Resource	`Show Service Account Password` in the Target Resource	"Show Service Account Password" in the "Target Resource" section.
`Show Password` in the Account Resource	`Show Password` in Account Resource	"Show Password" in the "Account Resource" section.
`Show Password History` in the Account Resource	`Show Password History` in Account Resource	"Show Password History" in the "Account Resource" section.
`Search Accounts` in the UI Resource	`Search Accounts` in Account Resource	"Search Accounts" in the "Account Resource" section.
`Search Assigned Accounts` in the UI Resource	`Search Assigned Accounts` in Account Resource	"Search Assigned Accounts" in the "Account Resource" section.
`Get All Checked Out Accounts` in the UI Resource	`Get All Checked Out Accounts` in Account Resource	"Get All Checked Out Accounts" in the "Account Resource" section.

9.2.3 Thread Count Continuously Increases During Oracle Privileged Session Manager Session Checkouts

To prevent thread counts from continuously increasing as Oracle Privileged Session Manager session checkouts progress, you must implement the following idle connection timeouts for each Unix target node so that when a connection has been idle for 20 minutes, it will be closed:

```
ClientAliveInterval 600
ClientAliveCountMax 2
```

Where the **`ClientAliveInterval`** value is in seconds.

For example, on Linux, you must edit the `/etc/ssh/sshd_config` file to add these parameters.

> **Note:** For more information about the `ClientAliveInterval` and `ClientAliveCountMax` keywords, refer to the `sshd_config` UNIX man page.

9.2.4 Unlimited Tablespace Privilege Missing When Using Oracle Database 12.1

Oracle Privileged Account Manager operations fail with a database error when you use Oracle Database 12.1.0.1 or higher. This error is displayed in the Oracle Privileged Account Manager server logs and is similar to the following:

```
<Error> <oracle.idm.opam> <BEA-000000>
<OPAMSQLManager.executeUpdateStatementSQLException occurred SQLErrorCode=1950
SQLErrorMesg=ORA-01950: no privileges on tablespace 'DEV_OPAM_BINSTORE'>
```

Oracle Database removed the `Unlimited Tablespace` privilege that was assigned to the `Resource` DB role, starting with the 12.1 release. The removal of this privilege has caused issues for Oracle Privileged Account Manager operations. For a description of the Oracle Database 12.1 release changes, refer to the following:

http://docs.oracle.com/cd/E16655_01/network.121/e17607/release_changes.htm#DBSEG941

Workaround: Login to Oracle Database using SQLPLUS as the `SYS` user. Run the following SQL command to grant unlimited tablespace to the Oracle Privileged Account Manager schema user:

```
grant unlimited tablespace to <opam_schema>;
```

For example, if the Oracle Privileged Account Manager schema name is *dev_opam*, then you would run the following command:

```
grant unlimited tablespace to dev_opam;
```

9.2.5 Session Checkout Does Not Appear In "My Checkouts"

Session Checkouts will not appear in the My Checkouts list unless you use the same (case sensitive) username to log in to the Oracle Privileged Account Manager GUI Console that you used to initiate the session.

9.2.6 A User With an Application Configurator Role Cannot Duplicate an Active Plug-In

When user logs in as with the app_config role and duplicates an existing active plug-in, it is not possible to save the new plug-in. This is because the status `active` is carried over and is not an option to change. The user who logs in with the app_config role does not have the privilege to change the status.

Workaround: To duplicate as a user with Application Configurator role, you must manually create a new plug-in and copy or type the required values.

9.2.7 Issues After Upgrading From Oracle Privileged Session Manager 11*g* Release 2 Patchset 1 to Oracle Privileged Session Manager 11*g* Release 2 Patchset 3

After upgrading Oracle Privileged Session Manager from Release 2 Patchset 1 (R2PS1) to Release 2 Patchset 3 (R2PS3), issues occur while configuring OPAM Session manager and configuring OPAM Console Application if any name other than "opam_server1" is used for the server managed by Oracle Privileged Account Manager (OPAM-managed server).

The Oracle Privileged Account Manager GUI Console and Oracle Privileged Account Manager session manager will not be deployed on the OPAM-managed server. There is no functional loss from pre-upgrade state. However, the new session manager functionality will not be available and the Oracle Privileged Account Manager console application will be available only on the Admin Server.

Workaround: Perform the following procedures to workaround this issue:

- To deploy the Session Manager application from the Oracle Privileged Account Manager GUI Console, perform the following procedure:
  1. Login to Weblogic console.
  2. Click **Deployments** and then click **Install.**
  3. Add the following:

```
$ORACLE_HOME/opam/modules/opamsessionmgr.ear_11.1.2/
```

4. Select **opamsessionmgr.ear.**
5. Select **OPAM Managed Servers** as deployment targets.
6. Click **Finish.**

- To target the oinav application on an OPAM-managed server, perform the following procedure:

  1. Login to Weblogic console.
  2. Click **Deployments** and expand **OINAV(11.1.1.3.0).**
  3. Click the **Targets** tab, select **OINAV(11.1.1.3.0) Enterprise Application** and click **Change Targets.**
  4. Select **OPAM Managed Servers** and click **Yes.**

9.3 Configuration Issues and Workarounds

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

- Section 9.3.1, "Use Absolute Paths While Running configureSecurityStore.py With -m Join"
- Section 9.3.2, "The configureSecurityStore.py Script Fails on Windows 8.1 64-Bit"

9.3.1 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 `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`.

9.3.2 The configureSecurityStore.py Script Fails on Windows 8.1 64-Bit

The "configureSecurityStore.py" script fails on Windows 8.1 Enterprise 64-bit during the installation of Oracle Privileged Account Manager.

To work around this issue, after configuring the Oracle Privileged Account Manager domain with the "config.bat" batch file, apply Patch 17342539. To obtain the patch, go to following URL, click **Patches and Updates**, and search for the patch number:

`https://support.oracle.com/`

You must download and extract the contents within the patch, and perform the procedure provided in the "README.txt" file. After performing the procedure, rerun "configureSecurityStore.py" script file.

9.4 Documentation Errata

There are no documentation errata items for the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager* 11g Release 2 (11.1.2.3.0), Part Number E52312-01.

10

Oracle Identity Manager

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

- Section 10.1, "Patch Requirements"
- Section 10.2, "What's New in Oracle Identity Manager 11g Release 2 (11.1.2.3.0)"
- Section 10.3, "General Issues and Workarounds"
- Section 10.4, "Configuration Issues and Workarounds"
- Section 10.5, "Multi-Language Support Issues and Limitations"
- Section 10.6, "Documentation Errata"

10.1 Patch Requirements

This section describes patch requirements for Oracle Identity Manager 11*g* Release 2 (11.1.2.3). It includes the following sections:

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

- Section 10.1.1, "Obtaining Patches From My Oracle Support (Formerly OracleMetaLink)"
- Section 10.1.2, "Patch Requirements for Oracle Database 11g (11.1.0.7)"
- Section 10.1.3, "Patch Requirements for Oracle Database 11g (11.2.0.1.0)"
- Section 10.1.4, "Patch Requirements for Oracle Database 11g (11.2.0.2.0)"
- Section 10.1.5, "Patch Requirements for Oracle Database 11g (11.2.0.3.0)"
- Section 10.1.6, "Patch Requirements for Oracle Database 11g (11.2.0.4.0)"
- Section 10.1.7, "Patch Requirements for Oracle Database 10g (10.2.0.4)"
- Section 10.1.8, "Patch Upgrade Requirement"
- Section 10.1.9, "Patch Requirement for BI Publisher 11.1.1.9.0"
- Section 10.1.10, "Patch Requirement for SOA 11.1.1.9.0"
- Section 10.1.11, "Patch Requirement for SSL with JDK 7u40 or Later"
- Section 10.1.12, "Obtaining the Latest Bundle Patch"

10.1.1 Obtaining Patches From My Oracle Support (Formerly OracleMetaLink)

To obtain a patch from My Oracle Support (formerly OracleMetaLink), go to following URL, click **Patches and Updates**, and search for the patch number:

`https://support.oracle.com/`

10.1.2 Patch Requirements for Oracle Database 11g (11.1.0.7)

Table 10–1 lists patches required for Oracle Identity Manager 11*g* Release 2 (11.1.2) configurations that use Oracle Database 11*g* (11.1.0.7). Before you configure Oracle Identity Manager 11*g*, be sure to apply the patches to your Oracle Database 11*g* (11.1.0.7).

Table 10–1 Required Patches for Oracle Database 11g (11.1.0.7)

Platform	Patch Number and Description on My Oracle Support
UNIX / Linux	7614692: BULK FEATURE WITH 'SAVE EXCEPTIONS' DOES NOT WORK IN ORACLE 11G
	7000281: DIFFERENCE IN FOR ALL STATEMENT BEHAVIOR IN 11G
	8327137: WRONG RESULTS WITH INLINE VIEW AND AGGREGATION FUNCTION
	8617824: MERGE LABEL REQUEST ON TOP OF 11.1.0.7 FOR BUGS 7628358 7598314
	8545377: ORA-1780 RAISED WHEN CURSOR_SHARING=FORCE
Windows 32 bit	8689191: ORACLE 11G 11.1.0.7 PATCH 16 BUG FOR WINDOWS 32 BIT
Windows 64 bit	8689199: ORACLE 11G 11.1.0.7 PATCH 16 BUG FOR WINDOWS (64-BIT AMD64 AND INTEL EM64T)
Oracle Solaris on SPARC 64-bit	8545377: ORA-1780 RAISED WHEN CURSOR_SHARING=FORCE

Note: The patches listed for UNIX/Linux in Table 10–1 are also available by the same names for Solaris SPARC 64 bit.

10.1.3 Patch Requirements for Oracle Database 11*g* (11.2.0.1.0)

Table 10–2 lists the required patch for Oracle Identity Manager 11*g* Release 2 (11.1.2.3) configurations that use Oracle Database 11*g* (11.2.0.1.0).

Table 10–2 Required Patch for Oracle Database 11g (11.2.0.1.0)

Platform	Patch Number and Description on My Oracle Support
Linux x86 64-bit	8545377: ORA-1780 RAISED WHEN CURSOR_SHARING=FORCE

10.1.4 Patch Requirements for Oracle Database 11*g* (11.2.0.2.0)

If you are using Oracle Database 11*g* (11.2.0.2.0), make sure that you download and install the appropriate version (based on the platform) for the RDBMS Patch Number 9776940. This is a prerequisite for installing the Oracle Identity Manager schemas.

Table 10–3 lists the patches required for Oracle Identity Manager 11*g* Release 2 (11.1.2) configurations that use Oracle Database 11*g* Release 2 (11.2.0.2.0). Make sure that you download and install the following patches before creating Oracle Identity Manager schemas.

Table 10–3 Required Patches for Oracle Database 11g (11.2.0.2.0)

Platform	Patch Number and Description on My Oracle Support
Linux x86 (32-bit) Linux x86 (64-bit) Oracle Solaris on SPARC (64-bit) Oracle Solaris on x86-64 (64-bit)	RDBMS Patch#13004894.
Microsoft Windows x86 (32-bit)	Bundle Patch 2 [Patch#11669994] or later. The latest Bundle Patch is 4 [Patch# 11896290].
Microsoft Windows x86 (64-bit)	Bundle Patch 2 [Patch# 11669995] or later. The latest Bundle Patch is 4 [Patch# 11896292].
All platforms	Patch 12419331: Database PSU 11.2.0.2.3 on top of 11.2.0.2.0 Base Release.

If this patch is not applied, then problems might occur in user and role search and manager lookup. In addition, search results might return empty result.

10.1.5 Patch Requirements for Oracle Database 11*g* (11.2.0.3.0)

Table 10–4 lists the patches required for Oracle Identity Manager 11*g* Release 2 (11.1.2.3) configurations that use Oracle Database 11g (11.2.0.3.0).

Table 10–4 Required Patches for Oracle Database 11g (11.2.0.3.0)

Platform	Patch Number and Description on My Oracle Support
Linux x86 64-bit	14019600: MERGE REQUEST ON TOP OF 11.2.0.3.0 FOR BUGS 13004894 13370330 13743357
Solaris, HP-UX, IBM AIX:	14019600: MERGE REQUEST ON TOP OF 11.2.0.3.0 FOR BUGS 13004894 13370330 13743357
Microsoft Windows 32-bit	13783452: ORACLE 11G 11.2.0.3 PATCH 4 BUG FOR WINDOWS 32 BIT
Microsoft Windows 64-bit	13783453: ORACLE 11G 11.2.0.3 PATCH 4 BUG FOR WINDOWS (64-BIT AMD64 AND INTEL EM64)

10.1.6 Patch Requirements for Oracle Database 11*g* (11.2.0.4.0)

Table 10–5 lists the patch required for Oracle Identity Manager 11*g* Release 2 (11.1.2.3) configurations that use Oracle Database 11*g* (11.2.0.4.0).

Table 10–5 Required Patch for Oracle Database 11g (11.2.0.4.0)

Platform	Patch Number and Description on My Oracle Support
All platforms	17501296: UNABLE TO DELETE ROWS FROM TABLE WITH TEXT INDEX AFTER UPGRADE TO 11.2.0.4

10.1.7 Patch Requirements for Oracle Database 10*g* (10.2.0.4)

In Oracle Database 10*g*, problems are encountered when creating materialized view using CONNECT_BY_ROOT clause. This is because the CONNECT_BY_ROOT operator is not available in Oracle Database 10*g* (10.2).

To resolve this issue, use the patches listed in Table 10–6:

Table 10–6 Required Patches for Oracle Database 10g (10.2.0.4)

Oracle Database Release	Patch Number and Description on My Oracle Support
10.2.0.4	8239552: BLR BACKPORT OF BUG 6908967 ON TOP OF 10.2.0.4.0 (BLR #113173)
10.2.0.4	8545377: ORA-1780 RAISED WHEN CURSOR_SHARING=FORCE

10.1.8 Patch Upgrade Requirement

While applying the patch provided by Oracle Identity Manager, the following error is generated:

```
ApplySession failed: ApplySession failed to prepare the system.
```

OPatch version 11.1.0.8.1 must be upgraded to version 11.1.0.8.2 to meet the version requirement.

See "Obtaining Patches From My Oracle Support (Formerly OracleMetalink)" for information about downloading OPatch from My Oracle Support.

10.1.9 Patch Requirement for BI Publisher 11.1.1.9.0

For information about patch requirement for BI Publisher 11.1.1.9.0, see Section 1.6.1, "Mandatory Patches Required for Installing Oracle Identity Manager.".

10.1.10 Patch Requirement for SOA 11.1.1.9.0

For information about patch requirement for SOA 11.1.1.9.0, see Section 1.6.1, "Mandatory Patches Required for Installing Oracle Identity Manager.".

10.1.11 Patch Requirement for SSL with JDK 7u40 or Later

In an Oracle Identity Manager environment in which SSL is enabled, JDK 7u40 or later is used, and SSL is configured by using the default setting as described in section "Enabling SSL for Oracle Identity Manager By Using Default Setting" of *Administering Oracle Identity Manager*, apply Oracle WebLogic Server patch 13964737.

10.1.12 Obtaining the Latest Bundle Patch

You must download and apply the latest Bundle Patch for Oracle Identity Manager 11*g* Release 2 (11.1.2.3). To do so:

1. Log in to My Oracle Support web site at the following URL:

   `https://support.oracle.com`

2. Click the **Knowledge** tab.
3. Search the article titled `Master Note on Fusion Middleware Proactive Patching - Patch Set Updates (PSUs) and Bundle Patches (BPs) (Doc ID 1494151.1)`.
4. Download and apply the appropriate Bundle Patch by following the instructions in the article. The row for 'Oracle Identity Manager (OIM) 11gR2' in the Proactive Patch Table provides information about the Bundle Patches for the current release of Oracle Identity Manager.

10.2 What's New in Oracle Identity Manager 11*g* Release 2 (11.1.2.3.0)

Oracle Identity Manager 11g Release 2 (11.1.2.3.0) has the following key new features:

- Section 10.2.1, "Improved Self Service UI"
- Section 10.2.2, "Access Catalog with Guided Navigation"
- Section 10.2.3, "Temporal Grants for New and Existing Access"
- Section 10.2.4, "Self Capabilities"
- Section 10.2.5, "Simplified Admin Roles"
- Section 10.2.6, "Role Lifecycle Management"
- Section 10.2.7, "Identity Audit Policy Management"
- Section 10.2.8, "Enhanced Auditing"
- Section 10.2.9, "Enhanced Password Policy Management"
- Section 10.2.10, "SCIM-Based REST Services"
- Section 10.2.11, "Simplified Workflow Policies"
- Section 10.2.12, "Simplified SSO Integration"

10.2.1 Improved Self Service UI

The simplified tiled user interface of Oracle Identity Manager presents end-users with quick access to the self service functions they need to do their jobs. Users can see what access they have, manage their information, and reset their passwords without having to do unnecessary navigation. Managers and empowered users can access their work items easily, with the ubiquitous notification icons providing them a clear picture of their work.

10.2.2 Access Catalog with Guided Navigation

The access request feature has been further simplified to enable end-users to get the access they need to do their jobs in a simple and user-friendly manner. Users are guided through the access request process and are presented with the relevant access in an easy to understand manner via the access catalog. The guided navigation and intelligent forms ensure that end-users are able to browse and, if required, search for access using keyword search. The access catalog presents end-users with relevant business information that helps them make a decision about the access they need.

10.2.3 Temporal Grants for New and Existing Access

As part of requesting for new access (or modifications to existing access), users can set start and end dates so that access is granted at the right time and revoked when the requirement is over. Empowered users can modify the grant duration for pending as well as provisioned access.

10.2.4 Self Capabilities

Administrators have a requirement to control the actions that end-users can perform in Oracle Identity Manager, either on themselves or on others. In earlier releases, there is no ability for an administrator to control the end-user actions as this function is handled by a combination of admin roles and approval policies.

In this release, administrators can make use of the self capabilities feature and specify rules that determine which action users can perform on themselves. To control the actions that users can perform on others, administrators can leverage the custom admin roles feature.

10.2.5 Simplified Admin Roles

Oracle Identity Manager allows you to define custom admin roles. As part of creating these admin roles, you can assign functional capabilities to the admin role, specify members and membership rules, and organizations that the admin role members can manage. The system-defined admin roles of 11g Release 2 (11.1.2.2.0) are present for backward compatibility only and should be considered deprecated. It is recommended to move to the new admin role model as soon as possible. To make use of the new admin role functionality, you must also enable the workflow policies feature.

With the introduction of this feature, Oracle Identity Manager no longer requires the use of Authorization Policy Manager (APM) and does not support policy customizations based on Oracle Entitlement Server (OES).

10.2.6 Role Lifecycle Management

Oracle Identity Manager allows empowered users to create, modify, approve, and certify business roles. Users composing new business roles or modifying existing roles can define business-friendly metadata, control membership, and specify which organizations have access to the role. They can also associate one or more access policies, which are collections of application entitlements, with the role. Access policies abstract out the complexities associated with application entitlements from business users, simplifying the role modeling and composition process. The application-specific access policy model also encourages reuse across roles simplifying the overall process.

As part of role composition or approval, users can see the impact of their actions, including potential compliance violations in a simple graphical manner. They can see which users will be impacted, whether there are other roles similar to the one being worked on, and whether any compliance policies are violated.

The use of this feature requires you to be licensed for its use.

10.2.7 Identity Audit Policy Management

Ensuring compliance with security controls across applications and enforcement of these controls are a key part of regulatory compliance. This requires you to define access controls that span applications and the ability to enforce these in real-time when access is being granted or modified, but also in a detective manner, for access that has already been granted. Oracle Identity Manager makes it possible for organizations to meet their compliance objectives by allowing business users to define audit policies. Audit policies specify what type of access a user may or may not have. For example, a user who has access to both Accounts Payables and Accounts Receivables is violating Sarbanes-Oxley guidelines. This is known as a Segregation of Duties (SoD) violation. Oracle Identity Manager allows organizations to define SoD policies that can be enforced during access request and can also be used to scan existing access to identify toxic combinations of access privileges, known as policy violations. Oracle Identity Manager identifies the violations and initiates a workflow allowing remediators, who could be business manager or administrators to fix these violations. This process is known as remediation. All actions taken by remediators are recorded and a comprehensive audit trail is maintained.

The use of this feature requires you to be licensed for its use.

10.2.8 Enhanced Auditing

This release of Oracle Identity Manager introduces a lightweight auditing engine which is used by user, role, and organization management, and other components excluding provisioning. Unlike the existing audit engine, it does not depend on audit snapshots and JMS and is synchronous in operation. This audit engine is the strategic choice, and the current audit engine will be deprecated in the next release of the product.

10.2.9 Enhanced Password Policy Management

This release of Oracle Identity Manager provides a common password policy management framework between Oracle Identity Manager and Oracle Access Manager (OAM). It also introduces the concept of a challenge policy, which allows you to specify whether challenge questions are system-defined or end-user defined (or a combination of both). You can specify different password policies for different organizations, allowing granular control of passwords and challenge questions.

10.2.10 SCIM-Based REST Services

Representational State Transfer (REST) services is the standard approach for creating scalable web services over HTTP. System for Cross-Domain Identity Management (SCIM) is the standard used to represent users and groups and provides a REST API for all necessary CRUD operations. This release of Oracle Identity Manager exposes several services as SCIM-based REST services. The SPML XSD-based SOAP web service is deprecated in favor of SCIM-based REST Services. It is recommended to move to the new REST services as soon as possible.

10.2.11 Simplified Workflow Policies

Approval policies are used in Oracle Identity Manager to determine the approval workflow to be launched for a particular action. This feature has been deprecated in favor of workflow policies. Functionally, workflow policies are equivalent to approval policies but perform better, expose additional configuration options, and conform to the UI of this release. You can continue using approval policies if you are upgrading to this release of Oracle Identity Manager. However, you cannot leverage the simplified admin roles capabilities. You must work with workflow policies only for a fresh deployment of Oracle Identity Manager.

If you are upgrading to Oracle Identity Manager 11*g* Release 2 (11.1.2.3), then it is recommended that you convert the approval policies to workflow policies as soon as possible.

10.2.12 Simplified SSO Integration

The recommended approach of Oracle Identity Manager to Single Sign On (SSO) is to use WebLogic plug-ins (Identity Asserters or Authenticators). These plug-ins are provided by Web Access Management solutions, such as OAM or SiteMinder. This release of Oracle Identity Manager supports a simplified single sign on integration by using HTTP Header variables. This approach requires you to configure a HTTP Server similar to Oracle HTTP Server or Apache HTTP Server as a reverse proxy for Oracle Identity Manager, and install and configure the vendor-provided web server plug-in.

10.3 General Issues and Workarounds

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

10.3.1 Background Color of Buttons Not Showing in Internet Explorer 9

If you are using Microsoft Internet Explorer 9, then the green background color for some action buttons in Oracle Identity Self Service are not displayed correctly.

To workaround this issue, upgrade to Internet Explorer 10 or higher. Otherwise, use Mozilla Firefox or Google Chrome.

10.3.2 Status Attribute Cannot be Included in the Denied Attributes List

If Identity Status is included in the list of Denied Attributes, then the functional capabilities added to an admin role do not work as expected. Identity Status cannot be included in the list of Denied Attributes.

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

10.3.3 Advanced Search Parameters Do Not Reset After Switching to Basic Search

When you switch from basic to advanced search and fill in search criteria and then switch back to basic search again, the basic search still has the criteria from the advanced search. It is now no longer a basic search. However, this is not apparent to the user because all the parameters from the advanced search are not displayed.

10.3.4 Error While Using Notification

UMS client object is pooled in Oracle Identity Manager. The following exception can be logged while using notification:

```
Class/Method: UCPPool/returnConnectionToPool encounter some problems: Failed to
release connection back to the UCP Pool, pooledconnection is null.
```

This exception can be safely ignored because it does not result in any notification message loss.

10.3.5 Form Data Not Displayed in Email Notifications

When requesting for account/entitlement, email notification is sent to the approver. The task details embedded in the email does not display the form data of the application instance or entitlement.

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

10.3.6 Export/Import of Roles with UDF Values Does Not Work

When you export and import the roles consisting of role UDFs and catalog UDFs by using the Deployment Manager, the catalog UDFs are imported with values but the role UDF values are not imported properly.

To workaround this issue, manually update the role after import.

10.3.7 Export/Import of Role with History Does Not Work

When you export and import a role by using the Deployment Manager, the role history is not imported properly. Fresh role history is created in the imported environment and is displayed for the Attributes and Membership Rules subtabs. But new history is not displayed for the following subtabs:

- Hierarchy
- Access Policy
- Organizations
- Role Membership
- Certification

This is a know issue, and a workaround for this is not available.

10.3.8 Export/Import of Roles with Parent Roles Does Not Work

When you export and import a role with parent and child roles by using the Deployment Manager, the child roles are displayed in the **Inherited By** subtab of the Hierarchy tab. But the parent roles are not displayed in the **Inherits From** subtab. In addition, parent roles cannot be selected as dependency during the export.

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

10.3.9 Modifying Display Name of Default Roles Not Supported

Modifying the values of the Display Name attribute for default roles, for example OPERATORS, ALL USERS, and SELF OPERATORS, is not supported.

In addition, if any client, such as API Client, UI, or the Deployment Manager, passes the display name attribute in the Role VO to the role modification API, then the operation fails even if the display name passed is same as the display name of the role in the system. As a result, import of exported default roles via the Deployment Manager fails because of this limitation, and the following error is logged:

```
Caused by: oracle.iam.platform.kernel.ValidationFailedException:
IAM-3056150:Cannot change the base value for the display name of an Oracle
Identity Manager system role.:
at
oracle.iam.identity.utils.Utils.createValidationFailedException(Utils.java:1066)
at
oracle.iam.identity.utils.Utils.createValidationFailedException(Utils.java:1049)
at
oracle.iam.identity.rolemgmt.utils.RoleManagerUtils.createValidationFailedExceptio
n(RoleManagerUtils.java:3242)
at
oracle.iam.identity.rolemgmt.utils.RoleManagerUtils.createValidationFailedExceptio
n(RoleManagerUtils.java:3251)
at
oracle.iam.identity.rolemgmt.impl.handlers.role.RoleValidationHandler.validateOOTB
Roles(RoleValidationHandler.java:731)
at
oracle.iam.identity.rolemgmt.impl.handlers.role.RoleValidationHandler.validate(Rol
eValidationHandler.java:441)
at
oracle.iam.identity.rolemgmt.impl.handlers.role.RoleValidationHandler.validate(Rol
eValidationHandler.java:285)
at
oracle.iam.platform.kernel.impl.OrchestrationEngineImpl.validate(OrchestrationEngi
neImpl.java:307)
at oracle.iam.request.impl.RequestEngine.triggerOperation(RequestEngine.java:4783)
at oracle.iam.request.impl.RequestEngine.doOperation(RequestEngine.java:4472)
at oracle.iam.impl.OIMServiceImpl.doOperation(OIMServiceImpl.java:43)
at
org.springframework.aop.support.AopUtils.invokeJoinpointUsingReflection(AopUtils.j
ava:307)
at
org.springframework.aop.framework.ReflectiveMethodInvocation.invokeJoinpoint(Refle
ctiveMethodInvocation.java:182)
at
org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMet
hodInvocation.java:149)
at
oracle.iam.platform.utils.DMSMethodInterceptor.invoke(DMSMethodInterceptor.java:35
)
at
org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMet
hodInvocation.java:171)
at
org.springframework.aop.framework.JdkDynamicAopProxy.invoke(JdkDynamicAopProxy.jav
a:204)
at $Proxy355.doOperation(Unknown Source)
at oracle.iam.identity.utils.Utils.invokeUnifiedService(Utils.java:3831)
at
oracle.iam.identity.rolemgmt.impl.RoleManagerImpl.modify(RoleManagerImpl.java:4196
)
```

To workaround this issue, right-click the default role in the import selection summary screen of the Deployment Manager, and click **Remove** to remove the specific role from the import selection. Then, import the rest of the artifacts.

10.3.10 Approval Tasks Cannot Be Signed Using Some Web Browsers

Approval tasks cannot be digitally signed when Google Chrome, Microsoft Internet Explorer, or Mozilla Firefox web browsers are used. When Firefox is used, this issue is encountered only with recent versions of Firefox.

Only Firefox web browser is supported for digitally signing tasks. To sign with Firefox, make the following setting:

1. Navigate to the following URL:

   https://addons.mozilla.org/en-US/firefox/addon/signtextjs/

2. Click **Add to Firefox** to install the add-on for electronic signing.
3. Restart the browser.

10.3.11 Filtering By Organization Name Not Supported

Sorting or filtering by the Organization Name column in the Available Roles tab of role details is not supported.

10.3.12 Cannot Filter By Attribute ID

Using SCIM REST service, filtering on the attribute ID is not supported for root search.

10.3.13 Cannot Filter By Meta.ResourceType

Using SCIM REST service, filtering on the attribute `meta.resourceType` is not supported.

10.3.14 Cannot Sort By Password Policies

When using SCIM REST API to retrieve password policies, the returned resources cannot be sorted.

10.3.15 Incorrect Error Codes for Some Operations

For some operations, the HTTP error code returned in a SCIM response is not same as defined by the SCIM specification, for example:

- POST operation on user that already exists returns HTTP error code `400` instead of `409`.
- Deleting an organization that is already deleted returns HTTP error code `400` instead of `404`.
- Request with no authorization returns HTTP error code `500` instead of `401`.
- POST, PATCH, and PUT operations on password policies with no authorization return error code `500` instead of `401`.
- PUT operation on unknown password policy returns incorrect error code `500`.
- PATCH operation on read-only attributes returns incorrect error code.
- Unsupported operation for ServiceProviderConfigs returns incorrect error code instead of `403`.
- Disabling and enabling a user with no authorization returns incorrect error code instead of `401`.
- GET operation on attribute that is not searchable returns incorrect error code.
- PATCH replace a read-only attribute returns incorrect error code.
- DELETE operation in unknown notification templates and system properties return incorrect error codes.
- PUT group is unknown owner returns incorrect error code.

10.3.16 Root Search on meta.resourceType Fails

Root search with filter on `meta.resourceType` using SCIM REST service fails, and error code `500` is returned.

10.3.17 Root Search with No Resource Fails

Root search with no resource specified using SCIM REST service fails, and error code `500` is returned.

10.3.18 Error Thrown on Sorting by Description Column on Lookup Type

When you click the Description column in the search results of the Lookup Type form to sort by description, the sorted result is not displayed, and the following error is displayed in Oracle Identity Manager server locale:

```
ORA-00932: inconsistent datatypes: expected - got CLOB
```

10.3.19 More Link in Auto-suggest for Catalog Advanced Search Does Not Work

In catalog advanced search, when you select the entity type as entitlement, you can select the application instance from the Application combo box. Alternatively, if you type the first few characters of the application instance name in the Application combo box, application instance names that match the characters are displayed along with a More link. However, clicking the More link has no effect.

10.3.20 Error While Customizing the Summary Page of the Create Role Wizard

The following error is thrown while customizing a catalog UDF added as read-only attribute in the Summary page of the Create Role wizard, when the Catalog Attributes section is expanded:

```
OracleJSP error: java.io.FileNotFoundException:
```

> **Note:** Set the `init-param` debug mode to `true` to see the complete exception message.

To workaround this issue, collapse the Catalog Attributes section of the Summary page in the Create Role wizard, and then click **Customize**.

The Summary page of the Create Role wizard displays the attributes that have already been added while creating the role. Therefore, you cannot add any extra catalog attribute in the Summary page that are not present in the Catalog Attributes section of the Attributes page. Therefore, if you want to add the read-only label for the catalog UDF, then add the UDF on the Catalog Attributes section of the Attributes page, go to the Display Options of that UDF, and set the **Read Only** property by using the Expression Builder. To do so, use the following expression:

```
 #{!pageFlowScope.editable}
```

The same UDF is displayed in the Summary page as read-only, and there is no need to add the extra read-only attribute on the summary page for the UDF.

10.3.21 Error While Provisioning Application Instance with New Field

When you create a new field in the application instance form, and in the same session, try to provision the application instance using Identity Self Service to any user, an error page is displayed.

To workaround this issue, logout and login to Identity Self Service.

10.3.22 Risk Levels Cannot Be Customized

In this release of Oracle Identity Manager, risk levels cannot be customized.

10.3.23 Delay in Displaying Pending Approvals Count

Display of the pending approvals count in the Self Service home page in Oracle Identity Self Service is delayed when large number of tasks are waiting for approval, which is approximately 34000 tasks.

To resolve this issue:

1. Create the index in SOA schema by running following SQL query:

```
CREATE INDEX WFTASKSTATENSPC ON
 WFTASK("STATE","IDENTITYCONTEXT","TASKNAMESPACE",
 "ACQUIREDBY","AGGREGATIONTASKID")';
```

2. Collect the statistics from all database schemas.
3. Restart all servers.

10.3.24 Loading of Technical Glossary Does Not Work With Oracle Database 11.2.0.1.0

With Oracle Database version 11.2.0.1.0, loading of Technical Glossary does not work as expected. The following `Internal ORA-00600` error is logged when trying to seed hierarchical entitlement data in Oracle Identity Manager database:

```
<ORA-00600: internal error code, arguments:
[kzxcInitLoadLocal-7], [64131],
          [ORA-64131: XMLIndex Metadata: failure during the looking up of the
dictionary
           ORA-30966: error detected in the XML Index layer
           ORA-31011: XML parsing failed], [], [], [], [], [], [], [], [], []

          ORA-00600: internal error code, arguments: [kzxcInitLoadLocal-7],
[64131], [ORA-64131: XMLIndex Metadata: failure during the looking up of the
dictionary
          ORA-30966: error detected in the XML Index layer
          ORA-31011: XML parsing failed ], [], [], [], [], [], [], [], [], []
```

To workaround this issue:

1. Login to the database as SYS DB user, and run the following queries:

   ```
   DROP INDEX XDB.PRIN_XIDX;
   DROP INDEX XDB.SC_XIDX;
   ```

2. Seed hierarchical entitlement data into Oracle Identity Manager database.
3. Run the following query from Oracle Identity Manager user to check whether the seeded data has entered the catalog hierarchical table:

   ```
   SELECT COUNT(1) FROM CATALOG_HIERARCHICAL_ATTR;
   ```

   The data is successfully seeded to the `CATALOG_HIERARCHICAL_ATTR` table.

10.3.25 Error Thrown While Setting Challenge Questions for the First Time

When you login to Oracle Identity Self Service for the first time, and while setting the challenge questions and answers, you try to set the question with length more than 55 characters, the following error is displayed:

```
Error
Unexpected exception caught: {0}, msg={1}

Error
JTA transaction unexpectedly rolled back (maybe due to a timeout); nested
exception is weblogic.transaction.RollbackException: setRollbackOnly called on
transaction

Error
setRollbackOnly called on transaction
```

This issue is applicable for administrator-defined challenge questions as well as challenge questions defined by the password policy. In addition, the same error is displayed when you try to set challenge questions and answers from the My Information page of Identity Self Service.

10.3.26 SCIM OIM Webapp Does Not Support Some Characters in UDF Names

SCIM OIM webapp accepts UDF names only with alphanumeric characters. If a UDF is created with an underscore (_) or dash (-) character in its name, then the SCIM OIM webapp does not work after the UDF is created.

To workaround this issue, the UDF definition in Oracle Identity Manager metadata must be fixed, as follows:

1. Export OIM metadata, as described in "Migrating User Modifiable Metadata Files" in *Developing and Customizing Applications for Oracle Identity Manager*.

   Specify the export directory in toLocation: `/tmp/mds`, and the metadata documents to export in docs: `/file/User.xml,/db/identity/entity-definition/Role.xml,/db/identity/entity-definition/Organization.xml`.

2. Depending on the UDF you created, edit the User.xml, Role.xml, or Organization.xml file, and look for the SCIM definition of the UDF, which is similar to the following:

   ```
   <metadata>
     <name>scim</name>
     <value>UDF_NAME</value>
     <category>properties</category>
   </metadata>
   ```

3. In the sample, remove the _ or dash - character from the UDF name (*UDF_NAME*).

   The new UDF name must be unique in the metadata file to avoid name conflict. For example, if you want to replace `MY_UDF_NAME` with `MYUDFNAME`, then make sure that `MYUDFNAME` is not already defined in the metadata as a SCIM attribute (UDF or not). If it is already defined, then find a unique name, such as `MYUDFNAMEUNIQUE`.

4. Import the modified XML file, as described in "Migrating User Modifiable Metadata Files" in *Developing and Customizing Applications for Oracle Identity Manager*.

   Specify the import directory in fromLocation: `/tmp/mds`, and the metadata documents to import in docs: `/file/User.xml,/db/identity/entity-definition/Role.xml,/db/identity/entity-definition/Organization.xml`.

5. Restart Oracle Identity Manager.

10.3.27 Local Part of Email Must Be Less Than Or Equal To 64 Characters

During user creation from the Identity Self Service, the local part of the email ID must be less than or equal to 64 characters. The local part is denoted as `localpart@domain.com`.

If the local part of the email ID consists of more than 64 characters, then user creation fails with the following error:

```
****attribute mail is not valid.
Please enter valid value for attribute mail
```

10.3.28 Inbox View Names Not Displayed Correctly

In an upgraded deployment of Oracle Identity Manager, the Inbox view names are not displayed correctly. For example, the view names are displayed as MANUAL_PROVISIONING_VIEW, PENDING_APPROVALS_VIEW, PENDING_CERTIFICATIONS_VIEW, and PENDING_VOILATIONS_VIEW instead of Manual Provisioning, Pending Approvals, Pending Certifications, and Pending Violations respectively.

To display the Inbox view names correctly, set the value of the WorkflowCustomClasspathURL attribute, as follows:

1. Login to Oracle Enterprise Manager.
2. Expand **Weblogic Domain**, ***DOMAIN_NAME***.
3. Right-click the domain name, and select **System MBean Browser**.
4. Go to **Application Defined MBeans**, **oracle.as.soainfra.config**, **server:*SOA_SERVER***, **WorkflowConfig**, **human-workflow**.
5. Check the value of the `WorkflowCustomClasspathURL` attribute. Verify that the path to the `adflibPendingApprovalsUI.jar` file is correct. If the path is not correct, then change the path correctly.
6. Save the changes.

10.3.29 Error on Opening Deployment Manager in Chrome Version 42

When you use Google Chrome Version 42, the Deployment Manager window does not open and displays the following error:

```
"This Plugin is not supported".
```

To workaround this issue:

1. In the address bar of the Google Chrome browser, enter `chrome://flags`.
2. In the page that loads, search for `#enable-npapi`.

   Alternatively, you can enter `chrome://flags/#enable-npapi` in the address bar to load the page directly.
3. Click the **Enable** link under **Enable NPAPI**.
4. Restart the browser.

10.3.30 Approvals Via Actionable Email Not Processed After Upgrade

After upgrading Oracle Identity Manager to 11g Release 2 (11.1.2.3.0), approvals done via actionable mails are not processed because of the following error:

```
"Overlapping access point specification".
```

To fix this issue, remove access points from the database. To do so:

1. Login to Oracle Enterprise Manager.
2. On the left pane, expand **User Messaging Service**.
3. Right-click **usermessagingserver**, and select **Messaging Client Applications**.

   The table that is displayed contains an entry with the SOA domain under the Name column. All the access points are listed in the Access Point column. Check how many and what access points are registered.

4. To deregister an access point, select the row, and then click **De-register**.
5. Restart SOA Managed Server, which will register the access point again.

10.3.31 System Properties Replaced with Password Policy Fields

In this release of Oracle Identity Manager, the `XL.MAXLOGINATTEMPTS` and `XL.MAXPASSWORDRESETATTEMPTS` system properties have been removed.

The function of the `XL.MAXLOGINATTEMPTS` system property has been replaced with the `Maximum Incorrect Login attempts counter` field in the password policy details page.

The function of the `XL.MAXPASSWORDRESETATTEMPTS` system property has been replaced with the `Lock User After Attempts` field in the Challenge Options section of the password policy details page.

For information about these fields, see "Managing Password Policies" in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager*.

10.3.32 Task Flows Created on Oracle Identity Manager 11*g* Release 2 (11.1.2.2) Not Applicable to Oracle Identity Manager 11*g* Release 2 (11.1.2.3)

If you have upgraded from Oracle Identity Manager 11*g* Release 2 (11.1.2.2) to Oracle Identity Manager 11*g* Release 2 (11.1.2.3), then the existing task flows cannot be used on Oracle Identity Manager 11*g* Release 2 (11.1.2.3). Because the UI of Oracle Identity Manager 11*g* Release 2 (11.1.2.3) changed, the existing task flows are outdated.

You should rewrite your own task flows for using them in 11*g* Release 2 (11.1.2.3). For information about creating task flows, see *Developing and Customizing Applications for Oracle Identity Manager*.

10.3.33 Scope of Immediate Attribute Limited to the Specific Actions

When the Justification field is customized to be required and the value of the field is not set, displaying other UI pages does not work and validation error happens for the empty value of the Justification field.

The problem can be resolved after disabling the ADF attribute `Immediate` of the Justification field. The scope of the ADF attribute `Immediate` is limited to the scope of specific actions, such as Submit or Next.

10.3.34 Unauthenticated SSL Not Supported by OWSM Policy

When OWSM multi_token_noauth_over_ssl_rest_service_policy is configured, all access must be over SSL. However, Oracle REST Self Service APIs allow unauthenticated access over HTTP even though OWSM multi_token_noauth_over_ssl_rest_service_policy is configured.

10.3.35 Deployment Manager Import/Export Not Supported on Edge and Safari Browsers

Import or export by using the Deployment Manager is not supported on Edge and Safari browsers. This is because Edge and Safari browsers do not support Java plug-ins or any other plug-ins, and Java plug-in is required for the Deployment Manager import/export to work. This is also stated in the following FAQ:

`https://www.java.com/en/download/faq/win10_faq.xml`

Therefore, use the Internet Explorer or other browsers for Deployment Manager import/export.

10.3.36 Connector Upgrade Not Supported on Edge and Safari Browsers

Upgrading any connector is not supported on Edge and Safari browsers because of the plug-in issue described in Section 10.3.35, "Deployment Manager Import/Export Not Supported on Edge and Safari Browsers".

Therefore, use the Internet Explorer or any other browsers for connector upgrade.

10.3.37 oimclient.jar Needs Update and ipf.jar for Some passwordmgmt VOs

Custom client applications using the previous version of the oimclient.jar will get an error similar to the following:

```
"oracle.iam.passwordmgmt.vo.Challenge; local class incompatible:
stream classdesc serialVersionUID = 7026677945288353246, local class
serialVersionUID = -5258470952025280257"
```

To resolve this issue, update the client application to use the new version of the oimclient.jar included with this release in *OIM_ORACLE_HOME*/server/client/oimclient.zip, and include the additional *OIM_ORACLE_HOME*/modules/oracle.idm.ipf_11.1.2/ipf.jar in the lib/classpath.

10.4 Configuration Issues and Workarounds

Currently, there are no configuration issues to note.

10.5 Multi-Language Support Issues and Limitations

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

- Section 10.5.1, "SOA-Based Notification Fails for Non-ASCII Administrator User"
- Section 10.5.2, "Oracle Identity Manager Help Displayed in Browser Language"
- Section 10.5.3, "Values for Organization Type and Status Displayed in English"
- Section 10.5.4, "Task Status Option Values Not Displayed Per Browser Language Setting"
- Section 10.5.5, "Data Populated By Default Not Translatable"
- Section 10.5.6, "Locale Drop Down is Not Displayed in Browser Language"

10.5.1 SOA-Based Notification Fails for Non-ASCII Administrator User

SOA-based notification is not working when a notification is sent to the user whose name contains non-ASCII characters. The notification e-mail body contains the following:

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

The following error is logged:

```
Caused By: javax.security.auth.login.FailedLoginException:
```

```
[Security:090304]Authentication Failed: User 0318~A~A~Y~A
javax.security.auth.login.FailedLoginException:
[Security:090302]Authentication Failed: User 0318~A~A~Y~A denied
        at
weblogic.security.providers.authentication.LDAPAtnLoginModuleImpl.login(LDAPAt
nLoginModuleImpl.java:261)
        at
com.bea.common.security.internal.service.LoginModuleWrapper$1.run(LoginModuleW
rapper.java:110)
        at java.security.AccessController.doPrivileged(Native Method)
        at
com.bea.common.security.internal.service.LoginModuleWrapper.login(LoginModuleW
rapper.java:106)
        at sun.reflect.GeneratedMethodAccessor1382.invoke(Unknown Source)
        at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.j
ava:25)
        at java.lang.reflect.Method.invoke(Method.java:597)
        at
javax.security.auth.login.LoginContext.invoke(LoginContext.java:769)
        at
javax.security.auth.login.LoginContext.access$000(LoginContext.java:186)
        at
javax.security.auth.login.LoginContext$4.run(LoginContext.java:683)
        at java.security.AccessController.doPrivileged(Native Method)
        at
javax.security.auth.login.LoginContext.invokePriv(LoginContext.java:680)
```

To resolve this issue:

1. Go to the My Oracle Support web site at:

   https://support.oracle.com/

2. Search and apply patch 18398295.
3. Restart all servers.

10.5.2 Oracle Identity Manager Help Displayed in Browser Language

If you set different languages as the browser language and as the value of the ORA_FUSION_PREFS cookie, then Oracle Identity Manager UI is displayed in the language set by the ORA_FUSION_PREFS cookie, but Oracle Identity Manager Help is displayed in the browser language.

For example, if you set the browser language as Japanese, and set ORA_FUSION_PREFS=German, then Oracle Identity Manager UI is displayed in German, but Oracle Identity Manager Help is displayed in Japanese.

10.5.3 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 for any selected suborganization in the Children tab of Organization Details page in Oracle Identity Self Service.

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

10.5.4 Task Status Option Values Not Displayed Per Browser Language Setting

The following Task Status option values are displayed in English on the Provisioning Tasks page instead of the browser language setting:

- Pending
- Rejected

10.5.5 Data Populated By Default Not Translatable

All data that is populated by default in Oracle Identity Self Service cannot be translated. For example, the name of the default password policy, which is `Default Password Policy`, displayed in the Password Policies page of Identity Self Service is in English irrespective of the browser language setting.

10.5.6 Locale Drop Down is Not Displayed in Browser Language

When you set the browser language to any one of the following, the Locale drop down in either My Information or Preferences in Identity Self Service is displayed in English and not according to the browser language setting:

- Arabic (ar)
- Czech (cs)
- Danish (da)
- Dutch (nl)
- Hebrew (he)
- Hungarian (hu)
- Norwegian (no)
- Romanian (ro)
- Slovak (sk)
- Turkish (tr)

10.6 Documentation Errata

Currently, there are no documentation issues to note.

11

Oracle Identity Management Integration

This chapter describes issues associated with Oracle Identity Management integrations.

Oracle Identity Management consists of a number of products, which can be used either individually or collectively.

This chapter contains the following topics:

- Integrating Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager
- Integrating Access Manager and Oracle Adaptive Access Manager

11.1 Integrating Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager

This section contains issues related to the integration of Oracle Access Management Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager. It contains the following topics:

- Section 11.1.1, "Lock User is Unable to Unlock Self in an Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager Integrated Environment"
- Section 11.1.2, "Invalid Class Exception When Password Policy Fails"
- Section 11.1.3, "The OAAM Login Page Does Not Show the Appropriate Error Message After the User is Locked Out"
- Section 11.1.4, "Forgot Password Link Is Available to Users that are not Registered"

11.1.1 Lock User is Unable to Unlock Self in an Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager Integrated Environment

In an Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager integrated environment, when an end user is locked in OIM and LDAP by providing multiple incorrect passwords, and he provides valid credentials in the OAAM login page, the user is denied access and an error message similar to the following is displayed:

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

The locked user is not redirected to an account locked page with the **Forgot your password** link that enables him to use the Forgot Password flow to unlock himself. To perform self unlock, the user must click the **Forgot Password** link in the Password input page.

In an Access Manager and Oracle Identity Manager integrated environment, the locked user is redirected to an account locked page with the **Forgot your password** link available to him.

11.1.2 Invalid Class Exception When Password Policy Fails

In an OAAM 11g Release 1 PS2 (11.1.1.3) and OIM 11g Release 2 PS1 (11.1.2.1) integrated environment or OAAM Release 2 PS1 (11.1.2.1) and OIM Release 1 PS2 (11.1.1.3) integrated environment, when the end user enters a password that violates the default password policy in the Expired, Forgot, or Change Password flow, the following message is displayed:

```
An error occurred while attempting to change your password. Please try again
```

An invalid class exception similar to the following example is shown in error log file:

```
<Apr 13, 2013 5:06:09 AM CST> <Error> <oracle.oaam> <BEA-000000>
<failed to changePassword(john.doe@example.com)
javax.ejb.EJBException: Problem deserializing error response; nested
exception is:
java.io.InvalidClassException:
oracle.iam.identity.exception.IdentityException; local class incompatible:
stream classdesc serialVersionUID = 1935467088360363654, local class
serialVersionUID = -7391301560574640548; nested exception is:
java.io.InvalidClassException:
oracle.iam.identity.exception.IdentityException; local class incompatible:
stream classdesc serialVersionUID = 1935467088360363654, local class
serialVersionUID = -7391301560574640548
at weblogic.ejb.container.internal.RemoteBusinessIntfProxy.unwrapRemoteException(
RemoteBusinessIntfProxy.java:121)
at weblogic.ejb.container.internal.RemoteBusinessIntfProxy.invoke(RemoteBusinessI
ntfProxy.java:96)
at $Proxy163.changePasswordx(Unknown Source)
at oracle.iam.identity.usermgmt.api.UserManagerDelegate.changePassword(Unknown
Source)
...etc
Caused By: java.io.InvalidClassException:
oracle.iam.identity.exception.IdentityException; local class incompatible:
stream classdesc serialVersionUID = 1935467088360363654, local class
serialVersionUID = -7391301560574640548
        at java.io.ObjectStreamClass.initNonProxy(ObjectStreamClass.java:562)
        at
java.io.ObjectInputStream.readNonProxyDesc(ObjectInputStream.java:1582)
...etc
```

The password related flows work if a valid password that adheres to the defined password policy is provided. The error does not affect the flow.

11.1.3 The OAAM Login Page Does Not Show the Appropriate Error Message After the User is Locked Out

OAAM Server treats the user that is disabled in the identity store as an invalid user. When such a user tries to log in using the OAAM server, the user may see a message similar to one that is displayed for an invalid user, such as the following example:

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

11.1.4 Forgot Password Link Is Available to Users that are not Registered

The OAAM password page shows a link to initiate the Forgot Password flow irregardless of whether the user is registered or not.

11.2 Integrating Access Manager and Oracle Adaptive Access Manager

This section contains issues related to the integration of Oracle Access Management Access Manager and Oracle Adaptive Access Manager. It contains the following topics:

- Section 11.2.1, "Access Manager and Oracle Adaptive Access Manager Integrations Using OAAMBasic and OAAMAdvanced Schemes Deprecated"
- Section 11.2.2, "OAAM Redirects from HTTPS to HTTP When Accessing an SSL-Protected Resource"
- Section 11.2.3, "bharosa.uio.default.is_oam_integrated Must Be Set to False"

11.2.1 Access Manager and Oracle Adaptive Access Manager Integrations Using OAAMBasic and OAAMAdvanced Schemes Deprecated

Oracle Access Management Access Manager and Oracle Adaptive Access Manager integrations using OAAMBasic and OAAMAdvanced authentication schemes are deprecated starting with 11.1.2.2 and will be desupported in 12.1.4 and future releases. The recommendation is to use the Oracle Access Management Access Manager and Oracle Adaptive Access Manager integration using Trusted Authentication Protocol (TAP) instead of OAAMBasic and OAAMAdvanced integrations. For information about Access Manager and Oracle Adaptive Access Manager integration using TAP, see *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

11.2.2 OAAM Redirects from HTTPS to HTTP When Accessing an SSL-Protected Resource

In an OAAM and Access Manager integrated environment, when accessing an SSL-protected resource, OAAM redirects to the login page URL with the http protocol but with the SSL port, resulting in an error. This occurs when the OAAM Server is fronted by Oracle HTTP Server (OHS) using an SSL port and SSL terminates at Oracle HTTP Server.

To work around this issue:

1. Set the following properties (otherwise OAAM will redirect incorrectly to the HTTP port):

```
oaam.uio.oam.cookie.redirect.hostname.attribute=rh
oaam.uio.oam.cookie.redirect.path.attribute=ru
```

> **Note:** These instructions only apply to integrations where TAPScheme is not used.

2. Add the following to the Oracle HTTP Server configuration file that contains the reverse proxy settings, example location: `*WEB_ORACLE_INSTANCE*/config/OHS/component_name/moduleconf/sso_vh.conf`:

```
#######################################################
```

```
## Entries Required by Oracle Adaptive Access Manager
####################################################
   <Location /oaam_server>
      SetHandler weblogic-handler
      WebLogicCluster OAMHOST1.mycompany.com:14300,
OAMHOST2.mycompany.com:14300
      WLProxySSL ON
      WLProxySSLPassThrough ON
   </Location>
```

3. Make sure the WebLogic SSL directives are in the `sso_vh.conf` file.
4. Because the Oracle HTTP Server acts as a proxy for WebLogic, by default certain CGI environment variables are not passed through to WebLogic. These include the host and port. You must tell WebLogic that it is using a virtual site name and port so that it can generate internal URLs appropriately. To do this:
   a. Log in to the WebLogic administration console in the IAMAccessDomain at

      `http://IADADMIN.mycompany.com/console`

   b. Select **Clusters** from the home page or, alternatively, select **Environment** -> Clusters from the Domain structure menu.
   c. Click **Lock and Edit** in the Change Center Window to enable editing.
   d. Click the Cluster Name (**oaam_cluster**).
   e. Select HTTP and enter the following values:

      Frontend Host: sso.mycompany.com (*IAM_LOGIN_URI*)

      Frontend HTTP Port: 80 (*HTTP_PORT*)

      Frontend HTTPS Port: 443 (*HTTP_SSL_PORT*)

      This ensures that any HTTPS URLs created from within WebLogic are directed to port 443 on the load balancer.

   f. Click **Save**.
   g. Select **Clusters** from the home page or, alternatively, select **Environment** > Clusters from the Domain structure menu.
   h. Click the Cluster Name (**oaam_admin_cluster**).
   i. Select HTTP and enter the following values:

      Frontend Host: IADADMIN.mycompany.com (*IAD_DOMAIN_ADMIN_LBRVHN*)

      Frontend HTTP Port: 80 (*HTTP_PORT*)

   j. Click **Save**.
   k. Click **Activate Changes** in the Change Center window.
5. In the WebLogic administration console, click **base_domain** on the left hand navigation and then click the Web Applications tab.
6. Scroll down toward the bottom and select the **WebLogic Plugin Enabled** option.
7. Click **Save**.
8. Log in to the Oracle Access Management Administration Console and check the Access Manager host details. Make sure the host points to the load balancer and is HTTPS.

11.2.3 bharosa.uio.default.is_oam_integrated Must Be Set to False

In an Access Manager and Oracle Adaptive Access Manager 11g Release 2 (11.1.2.3) integrated environment, the property `bharosa.uio.default.is_oam_integrated` must be set to `false`.

12

High Availability and Enterprise Deployment

This chapter describes issues associated with Oracle Fusion Middleware high availability and enterprise deployment. It includes the following section:

- "Configuration Issues and Workarounds"

12.1 Configuration Issues and Workarounds

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

- "Log in to Authorization Policy Manager Fails"
- "NullPointerException Occurs and Policy Does Not Save When OAAM Server Fails Over"
- "NullPointerException Occurs and Transaction Does Not Save When OAAM Server Fails Over"
- "OUD changelog is Configured Incorrectly"

12.1.1 Log in to Authorization Policy Manager Fails

If you have upgraded the Oracle Entitlements Server (OES) Administration Server from version 11g R2 PS1 to 11g R2 PS2 in a high availability cluster environment and you are in the process of configuring high availability, you cannot log into Authorization Policy Manager (APM). When you start the APM Administration Server and managed servers then try to log into the APM console, the system returns the following exception:

```
javax.el.PropertyNotFoundException The class
'oracle.security.apm.ui.bean.ApmMainManagedBean' does not have the property
'roleTemplateEnabled'
```

To log into APM, you must manually redeploy APM in the Administration Console from IDM_HOME.

12.1.2 NullPointerException Occurs and Policy Does Not Save When OAAM Server Fails Over

If you are creating a policy in the Administration Console and one OAAM Server is down and failover occurs, a NullPointerException opens when you click **Apply**. The policy does not save successfully.

To resolve this issue, open the Create Policy page, enter the settings you had entered previously, and click **Apply**.

12.1.3 NullPointerException Occurs and Transaction Does Not Save When OAAM Server Fails Over

If you are creating a transaction in the Administration Console and the OAAM Server is down and failover occurs, a NullPointerException opens when you click **Apply**. The transaction does not save successfully.

To resolve this issue, open the Create Transaction page, enter the settings you had entered previously, and click **Apply**.

12.1.4 OUD changelog is Configured Incorrectly

If you have selected the **Prepare Directory using IDMLCM** option when creating a response file in an Enterprise Deployment with Oracle Unified Directory (OUD), complete the following steps after LCM is deployed successfully:

1. Grant OUD changelog access on LDAPHOST1 and LDAPHOST2. See "Grant OUD changelog Access" in the Enterprise Deployment Guide for Oracle Identity and Access Management guide.
2. Restart LDAPHOST1 and LDAPHOST2.