Oracle® Fusion Middleware

Identity Management Release Notes

11*g* Release 1 (11.1.1.7)

E54961-02

August 2014

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

Oracle Fusion Middleware Identity Management Release Notes, 11*g* Release 1 (11.1.1.7)

E54961-02

Contents

3 Oracle Access Manager

6 Oracle Identity Manager

7 Oracle Internet Directory

8 Oracle Platform Security Services

9 SSL Configuration in Oracle Fusion Middleware

10 Oracle Directory Integration Platform

11 Oracle Virtual Directory

Preface

This preface includes the following sections:

Audience

This document is intended for users of Oracle Fusion Middleware 11*g*.

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

Related Documents

For more information, see these Oracle resources:

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

Conventions

The following text conventions are used in this document:

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

1 Introduction

This chapter introduces Oracle Fusion Middleware Identity Management Release Notes, 11g Release 1 (11.1.1). It includes the following topics:

1.1 Latest Release Information

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

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

1.2 Purpose of this Document

This document contains the release information for Oracle Fusion Middleware 11g Release 1 (11.1.1). It describes differences between Oracle Fusion Middleware and its documented functionality.

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

1.3 System Requirements and Specifications

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

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

1.4 Certification Information

This section contains the following:

1.4.1 Where to Find Oracle Fusion Middleware Certification Information

The latest certification information for Oracle Fusion Middleware 11g Release 1 (11.1.1) is available at the Oracle Fusion Middleware Supported System Configurations Central Hub:

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

1.4.2 Certification Exceptions

This section describes known issues (exceptions) and their workarounds that are associated with Oracle Fusion Middleware 11g certifications. For a list of known issues that are associated with specific Oracle Fusion Middleware 11g Release 1 (11.1.1) components, see the Release Notes for the specific Oracle Fusion Middleware 11g Release 1 (11.1.1) component.

This section contains the following topics:

1.4.2.1 Certification Information for Oracle Fusion Middleware 11g R1 with Oracle Database 11.2.0.1

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

1. Apply patch 8897382 to fix bug 8897382.

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

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

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

```
          ,enabled => 'Y');
     commit;
    end;/
```

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

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

1.4.2.2 Excel Export Issue on Windows Vista Client

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

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

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

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

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

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

1.4.2.4 Restrictions on Specific Browsers

1.4.2.4.1 Internet Explorer Browser Goes Blank When Adding Portlets in Oracle Webcenter If you add portlets in Oracle Webcenter by using Internet Explorer, then the page can go

blank. When it does go blank, a download message appears on the browser's status bar. However, nothing is downloaded and the browser remains blank untill you click the browser's back button. If this problem occurs, the portlets will appear only when you hit the browser's back button. This issue does not occur with Firefox.

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

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

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

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

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

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

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

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

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

1.4.3 Upgrading Sun JDK From 1.6.0_07 to 1.6.0_11

For information, see Section 2.1.6.3, "Upgrading Sun JDK in the Oracle Home Directory." THIS LINK IS BROKEN. I DEACTIVATED IT SO THE BUILD WOULD SUCCEED.

1.4.4 JMSDELIVERYCOUNT Is Not Set Properly

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

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

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

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

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

1.5 Downloading and Applying Required Patches

After you install and configure Oracle Fusion Middleware 11g Release 1 (11.1.1.4.0), there might be cases where additional patches are required to address specific known issues.

Complete the following steps to obtain a patch:

1. Log into the My Oracle Support web site at `https://myoraclesupport.com/`.
2. Click the Patches & Updates tab.
3. Use the Patch Search area to locate patches.
4. On the Patch Search Results page, select a patch and click Download to download the patch.
5. Install the patch by following the instructions in the README file that is included with the patch.

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

For additional patching information, see Section 3.1.1, "Patches Required to Address Specific Upgrade and Compatibility Requirements." THIS LINK IS BROKEN. I DEACTIVATED IT SO THE BUILD WOULD SUCCEED.

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

Oracle Fusion Middleware Product or Component	Bug/Patch Number	Description
Oracle SOA Suite - Oracle BPM Worklist application	9901600	Unless you apply this patch, errors appear in the log files when you access the Event Driven page in the Oracle Business Process Management Worklist application.
Oracle XDK for Java	10337609	This patch fixes the following issue. If you use the XSU utility to insert some data into the database, and the database connection had the connection property called `oracle.jdbc.J2EE13Compliant` set to "true", and the target column was some kind of numeric column, then it is possible for the insert to fail with a the following error: `java.lang.NumberFormatException`

1.6 Licensing Information

Licensing information for Oracle Fusion Middleware is available at:

`http://oraclestore.oracle.com`

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

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

2

Oracle Adaptive Access Manager

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

2.1 General Issues and Workarounds

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

2.1.1 OAAM Sessions is Not Recorded When IP Address from Header is an Invalid IP Address

OAAM sessions were not recorded for some header-based IP addresses.

Header based IP addresses are not accepted by default. To enabled the reading of IP addresses from the header, set `vcrypt.tracker.ip.detectProxiedIP` to `true`. When header IP addresses are enabled, only valid IP addresses are used. If the header contains an invalid IP address, the actual request IP address is used.

2.1.2 Checkpoint Boxes in Session are Displayed with Same Timestamp

The same timestamp is displayed in **Checkpoint** boxes in the Session Details page when multiple transactions are triggered in the same session. This bug has been fixed for OAAM Online.

2.1.3 Autogenerated Agent Cases Display User Specific Data

When an OAAM Agent Case is autogenerated from a Configurable Action, the User Details pane is populated with details of the user for the session where the case was created. An autogenerated Agent case should not contain user-specific data. Only Escalated Agent cases should display user details since they are the only cases specific to a single end user.

2.2 Policy Management Issues and Workarounds

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

2.2.1 Rule Condition Check Current Transaction Using the Filter Conditions Cannot Be Configured for Corresponding Attributes of Two Entity Instances

When two instances of an entity are associated to an OAAM Transaction and a filter condition is set up to compare an attribute of one entity instance with the corresponding attribute of the other entity instance, the OAAM Administration Console can only configure a comparison between the same attribute instead of a comparison between the different attributes.

For example:

Two instances of the `Address` entity are associated with a Transaction, one with the instance name `BillingAddr` and another with the instance name `ShippingAddr`. If the user configures `Check Current Transaction using the filter condition` to compare `Billing.line1` with `ShippingAddr.line1`, after saving the rule, the OAAM Administration Console always shows the instance `--- line1 of BillingAddr` in the dropdown for the attribute the user wants to compare and the dropdown for the attribute the user is comparing to.

2.2.2 Rule Condition to Check Consecutive Transactions Fails Entity Check

The rule condition `TRANSACTION: Check if consecutive Transactions in given duration satisfies the filter conditions` does not trigger. The condition returns `False` and the entity check fails with exceptions in the debug log.

2.2.3 Exclude IP List Parameter for User and Device Velocity Rule Conditions

The `Exclude IP List` parameter was added to the following conditions:

- `Device: Velocity from last login`
- `User: Velocity from last login`

This parameter allows you to specify a list of IP addresses to ignore. If the user's IP address belongs to that list, then this condition always evaluates to `false` and no action and/or alert is triggered. If the user's IP address is not in that list or if the list is null or empty, then the condition evaluates the velocity of the user or the device from the last login. If the velocity of the user or the device from the last login is more than the configured value in the rule, the condition evaluates to `true` and the condition is triggered.

2.2.4 OAAM Offline Displays Only the Last Rule Executed Overwriting Previous

When multiple transactions are run in the same session, only the rule triggered for the last transaction is displayed in OAAM offline. The rules from the previous transactions are overwritten. To fix this bug, you must apply the patch and update the database schema.

2.2.5 User: Check First Login Time Rule Condition Always Triggers

The `User: Check first login time` condition returned the same value regardless of when the user logged in.

2.3 Transaction Issues and Workarounds

This section describes OAAM Transaction issues. It includes the following topics:

2.3.1 OAAM Displays Only the Last Rule Executed and Overwrites Previous Rules

When multiple transactions are triggered in the same session which result in multiple alerts and policies execution, OAAM displays only the most recent alerts and policies triggered and overwrites the alerts and policies from previous transactions.

2.3.2 OAAM Shows Only 25 Transactions in Session Details

When there are more than 25 data elements configured for a transaction, the Session Details displays only transaction details for the first 25 items. The page has no scroll bars for scrolling.

2.3.3 Alerts Are Not Displayed Beyond 25 Transactions

Alerts are not visible for transactions beyond the 25th. If there are more than 25 checkpoint boxes containing alerts, they are not visible in the Session Details, although the data is seen in the database.

2.3.4 OAAM Transaction Cannot Be Created with Numeric Parameter of More than 16 Digits

If a user defines any numeric value more than 16 digits in a transaction field, the transaction creation fails with the error on the server of ORA-01438: value larger than specified precision allowed for this column.

2.3.5 Transactions in Session Details Duplicated After 25

Transactions listed in Session Transactions section of Session Details are duplicated after 25 transactions in a session.

2.3.6 Transaction ID Association with Alert Does Not Work

Transaction ID association with Alert is not working even after passing `transactionId` in `processRules` API. The bug has been fixed for the server-side.

2.3.7 OAAM Console Does Not Display Transaction Status

Transaction status needs to be displayed in the Transaction Details page so that the Fraud team will be able to see if a transaction was attempted but did not complete. This provides information on both the behavior of customers and fraudsters and also of the functioning of the rules. The Fraud team does not believe they can do their job effectively if they cannot tell the transaction status. The workaround is to display the status value for each transaction on the Session Transactions panel along with **Name**, **Transaction Id**, **Description**, and **Timestamp**. The value displayed would be mapped from the property `tracker.transaction.status.enum` (e.g. `1`=Success, `99`=Pending).

2.3.8 Transaction Mapping Substring Error for First Character Value

When the user performs a transaction mapping of the type `SubString`, the first character of the value is missing from the mapping result because the `oaam.transaction.mapping.startindex.min` property was set to `1`. Setting the property to `1` starts the substring operation from the second character of the string. A fix has been made so that this property is assigned to 0 so that the substring operation starts from the first character of the string.

2.3.9 Update Time for Entity Is Updated Without Any Change in Entity Data

When using an entity that is mapped to a Transaction Definition in a transaction, the entity's update time is updated by the OAAM Server even if no changes were made to the entity data (other fields are not updated). Database performance is impacted when this occurs.

2.4 Knowledge-Based Authentication Issues and Workarounds

This section describes Knowledge-Based Authentication issues. It includes the following topics:

2.4.1 Registration Logic Page Does Not Display KBA Logic

The KBA Registration Logic page does not display KBA Logic (Question per menu, Categories per menu, Number of questions the user will register) because the previous out of the box snapshot did not contain the properties for the KBA Registration Logic page. The patch fixes this problem. To effect this fix, the new out of the box snapshot file (`oaam_base_snapshot.zip`) needs to be imported. Note that importing this file will overwrite the existing content in the server.

If you do not want to import the snapshot file, but want to fix the registration logic related issue, you can create the following properties (with default values as shown):

```
challenge.question.registration.groups.categories.count=5
challenge.question.registration.groups.count=3
challenge.question.registration.groups.minimum.questions.per.category.count=1
challenge.question.registration.groups.questions.count=5
```

The patch also fixes the policy overrides in such a way that when the user fails the OTP challenge, the challenge does use KBA as a fallback. If you do not want to overwrite the contents but just import the newer policies, you can import `oaam_policies.zip` as a policies import. Importing the policies does not fix the registration logic related bug.

2.4.2 Answer Logic Abbreviation Resource Was Not Used

Answer Logic checks if the answer provided by the user matches closely to the ones provided during registration. Answer Logic relies abbreviations.

An updated Answer Logic abbreviations resource bundle is available in OAAM 11.1.1.5. In the new resource bundle, the following are considered a match:

Registered Answer	Given Answer
Missus	Mrs
Mister	Mr
Sergeant	Sgt
Mrs	Missus
Mr	Mister
Sgt	Sergeant

2.4.3 Update KBA for FFIEC Compliance

The following KBA questions from previous releases were deleted from the `kba_questions.zip` (English) file and `oaam_base_snapshot.zip` file for Federal Financial Institutions Examination Council (FFIEC) compliance:

Children Category

Delete or deactivate the following 10 questions:

- What year was your oldest child born?
- What year did your oldest child start school?
- What year did your youngest child start school?
- What is your eldest child's middle name?
- What is the first name of your youngest child?
- What year was your youngest child born?
- What is the first name of your oldest child?
- What is your youngest child's birthday?
- What is your youngest child's middle name?
- What is your oldest child's birthday?

Education Category

Delete or deactivate the following 18 questions:

- What year did you graduate from high school?
- What year did you graduate from junior high school?
- What city was your high school in?
- What were your college colors?
- What year did you graduate from grade school?
- What was the mascot of your college?
- What were your high school colors?
- What was the mascot of your high school?
- What is the name of a college you applied to but did not attend?
- In what city was your first elementary school?
- What year did you start high school?
- What year did you start junior high school?
- What year did you start grade school?
- What year did you graduate from college?
- What year did you start college?
- What was your major in college?
- What was the first school you ever attended?
- What city was your college in?

Miscellaneous Category

Delete or deactivate the following 2 questions:

- What is the first name of your closest childhood friend?
- What is your height?

Parents, Grandparents, Siblings Category

Delete or deactivate the following 17 questions:

- What year was your father born?
- What is your father's birthday?
- What is your oldest sibling's nickname?
- In which city was your father born?
- In which city was your mother born?
- What is your parent's current street address number?
- What is your parent's current street name?
- What is your youngest sibling's nickname?
- What is your parent's current ZIP code?
- What year was your mother born?
- What are the last 4 digits of your parent's phone number?
- What is your maternal grandmother's first name?
- What is your paternal grandmother's first name?
- What is the first name of your youngest sibling?
- What is your paternal grandfather's first name?
- What is your mother's birthday?
- What is the first name of your eldest sibling?

Significant Other Category

Delete or deactivate the following 18 questions:

- Where did you go on your honeymoon?
- What year did you get married?
- What year was your significant other born?
- What is your significant other's birthday?
- What date is your wedding anniversary?
- In what city did you meet your spouse for the first time?
- What city was your significant other born in?
- What is the first name of your significant other's mother?
- What is the first name of your significant other's father?
- What is the last name of your significant other's eldest sibling?
- What is the first name of your significant other's youngest sibling?
- What high school did your significant other attend?
- What was the last name of your best man or maid of honor?
- What was the first name of your best man or maid of honor?
- Name of the place where your wedding reception was held.
- What is your spouse's nickname?

- What state was your significant other born in?
- What is the last name of your significant other's youngest sibling?

Sports Category

Delete or deactivate the following 4 questions:

- What is the mascot of your favorite sports team?
- What are the colors of your favorite sports team?
- What team is the biggest rival of your favorite sports team?
- What is your all time favorite sports team?

Your Birth Category

Delete or deactivate the following 9 questions:

- What is the ZIP code where you grew up?
- Who was the US President when you were born?
- How old was your father when you were born?
- How old was your mother when you were born?
- What is the name of the hospital you were born in?
- What is the ZIP code of your birthplace?
- What is the holiday closest to your birthday?
- What state were you born in?
- What city were you born in?

2.4.4 Closing Browser on Image and Security Phrase Registration Page

If the user tries to register his security image and phrase for the first time and during the process, he closes his browser window on the registration and user preferences pages or returns to the login page, the last image and phrase presented are accepted as the default even if he has not explicitly chosen them by clicking the **Continue** button.

A fix has been made so that the image and phrase registration only saves the image and phrase after the user clicks **Continue** on the registration and user preferences pages.

2.4.5 OAAM Change Password Does Not Display Any Validation for Password Fields

The OAAM Change Password page in an OAAM and OIM integration does not display any validation for the Password field. The issues are as follows:

- If the user does not enter a password, but clicks **Submit**, there is no validation that the fields are empty
- If the user enters a new password and then the confirmation password, the password is accepted regardless of whether they are the same or different
- If the user changes his password, the old password is not validated to confirm that it is correct

2.4.6 ORA-01722 Occurs During KBA Update

An `ORA-01722` error can occur when adding a new challenge question.

2.4.7 Registered Questions Are Deleted and Subsequent Challenge Does Not Succeed

If a user's question set contains a deleted question and/or if a user's registered questions contain a deleted question and/or if the KBA registration logic is out of alignment with the user's registered questions and question set (the number of questions/categories and so on), when the user tries to update his question set but cancels or closes the browser window or the session times out without saving, that user's existing questions are deleted from the database. The subsequent challenge does not succeed as the existing questions have been deleted.

This issue has been fixed so that now if a user's registered questions have been deleted in the process of resetting the questions, the user will be asked to re-register new ones on the next login.

2.5 Integration Issues and Workarounds

This section describes OAAM integration issues. It includes the following topics:

- setupOAMTapIntegration.sh Does Not Set oaam.uio.oam.secondary.host.port
- OAAM Does Not Support Juniper Single Sign-On for Authentication and Forgot Password Flow
- Step Up Authentication Changes
- TAP: Incorrect Error Message
- OAAM 11g SOAP Timeout Exception Handling
- OAAM Should Call UserManager.Unlock() in the Forgot Password Workflow

2.5.1 setupOAMTapIntegration.sh Does Not Set oaam.uio.oam.secondary.host.port

The `setupOAMTapIntegration.sh` script does not set the secondary OAM host information (`oaam.uio.oam.secondary.host.port` value) during the configuration of Oracle Adaptive Access Manager for the Oracle Access Manager and Oracle Adaptive Access Manager integration. The workaround is to set the property value through the property editor.

2.5.2 OAAM Does Not Support Juniper Single Sign-On for Authentication and Forgot Password Flow

The OAAM Authentication flow is not invoked when integrated with Juniper SSL. With invoking OAAM, the integration can detect fraud and determine risk during the authentication flow and accordingly strongly authenticate the user using OAAM capabilities like Challenge, Block, and other actions. The Juniper SSL and OAAM integration flow should be as follows:

1. The user tries to access a web application or URL that is secured by Juniper SSL, and Juniper SSL detects whether the user is authenticated or not.
2. If the user is authenticated then he is allowed to proceed to the web application.
3. If the user is not authenticated, he is redirected to the OAAM Server. The OAAM Server displays the User ID page and prompts the user to enter his User ID. Once the user enters his User ID, OAAM evaluates the Pre-Authentication checkpoint policies and checks to see if the user has to be blocked.
4. OAAM then checks to see if the user has registered for an Authentication Pad. If so, it displays the registered Authentication Pad, otherwise it displays a generic text pad.

5. OAAM Server displays the Password page with the Authentication Pad and prompts the user to enter his password. Once the password is entered, it is validated against the user store (the user store can be LDAP, Active Directory, or any active user store). It also identifies the device by running the device identification process.
6. If the credentials are incorrect then OAAM displays an error page and asks the user to enter his credentials again.
7. If the credentials are correct then OAAM evaluates Post-Authentication checkpoint policies. Based on the outcome of the policy OAAM might challenge or block the user.
8. If the outcome of Post-Authentication is ALLOW then OAAM determines if the user has to be registered. Based on the types of registration, OAAM takes the user through registration pages.
9. If the outcome of Post-Authentication is CHALLENGE and if the user is already registered for at least one of the challenge mechanisms, OAAM challenges the user. If the user is able to answer the challenge then he would be allowed to continue to the next step. As the next step OAAM fetches the user attributes from the user store and then creates the SAML response, signs it and then it posts to the Juniper SSL redirection URL. Juniper SSL then takes control, validates the SAML payload, and lets the user access the web application.
10. If the outcome of Post-Authentication is BLOCK then user would be blocked and he would not be able to access the web application.

2.5.3 Step Up Authentication Changes

The Step Up Authentication feature is available with OAAM. Step Up Authentication allows users who have been authenticated by OAM at a lower level to access resources protected by `OAAMTAPScheme` configured at a relatively higher authentication level. When the user tries to access a protected resource that is configured at a higher level, OAAM runs policies to determine how to further authenticate the user so as to gain the required level of authentication needed for access to the protected resource. The user is not taken to the normal login flow since he is already authenticated.

The property to disable/enable Step Up Authentication mode in TAP Integration: By default the Step Up Authentication mode is enabled. However if you want to disable this feature, then set property `oaam.uio.oam.integration.stepup.enabled` as `false`.

Change in behavior for the end user: For an end user using the Access Manager-OAAM TAP Integration, the change in behavior is as follows:

If a user has already been authenticated by Access Manager and he tries to access a resource protected under `TAPScheme` with OAAM as the TAP partner, the user is not taken to the OAAM login flow (since the user is already authenticated). However, OAAM runs its fraud detection policies and might ask challenge questions or block the user depending on the risk evaluated by the policies.

2.5.4 TAP: Incorrect Error Message

In Access Manager-OAAM TAP integration, when an incorrect user name or password is supplied, OAAM shows following error:

```
There was some technical error processing your request.   Please try again
```

The patch fixes this problem: the error message now indicates an invalid user name or password error instead of a technical error.

2.5.5 OAAM 11g SOAP Timeout Exception Handling

The client calling Web services is not getting exceptions for timeouts. As a result the client cannot handle SOAP timeouts in a proper way because it cannot determine whether the exception is a SOAP timeout or any other faults. A fix has been implemented so that a specific error code for timeouts is passed to the client. The client can therefore handle the fault per the information contained in the exception.

The method `handleException()` has introduced a class `VCryptSOAPGenericImpl` which can be overridden to include more error codes based on business requirements. Currently it has been set for `soaptimeout` errors:

```
protected String handleException(String requestName, Exception ex, String
resultXml) {
```

2.5.6 OAAM Should Call UserManager.Unlock() in the Forgot Password Workflow

In the Forgot Password flow executed by OAAM in an Oracle Identity Manager and Access Manager integration, the user is not unlocked when he changes his password. When OAAM executes the `changePassword()` API, Oracle Identity Manager does not automatically unlock the user.

The following steps are needed to enable automatic unlocking of the user on the Oracle Identity Manager side when OAAM executes the `changePassword ()` API during the Forgot Password flow:

1. Log in to the OAAM Administration Console.
2. In the navigation pane, click **Environment** and double-click **Properties**. The Properties search page is displayed.
3. Set `oaam.oim.passwordflow.unlockuser` to `true`.

   By default this property value is set to `false`. By setting this property to `true` OAAM will call the `unlock` API of Oracle Identity Manager in the Change Password task flow.

2.6 Reporting Issues and Workarounds

This section describes OAAM BI Publisher reports and Sessions issues and workarounds. It includes the following topics:

- Alert Message Link in Session Details Page Does Not Open the Alert Details
- OAAM Rules Breakdown Report Does Not Provide Correct Information

2.6.1 Alert Message Link in Session Details Page Does Not Open the Alert Details

When the user tries to access an alert details page from an alert message link in the Session Details page, the page fails to open.

To work around this issue, use the alert message link on the Session Search page.

2.6.2 OAAM Rules Breakdown Report Does Not Provide Correct Information

The `BI Publisher Rules Breakdown` report does not give a summary of the rules which have been triggered by the checkpoint and policy. The values given are not complete or accurate.

For the report to work, run the following script:

```
create or replace view OAAM_FIRED_RULES_VIEW as (
select actionMap.create_time, ruleMaps.rule_map_id, actionMap.request_id,
actionMap.runtime_type,
  sessions.user_id, sessions.node_id, actionMap.action_list
from (select substr(attr_name, 7) ruleInstanceId, case when
length(trim(translate(attr_value, '+-.0123456789', ' '))) is null then
CAST(attr_value AS NUMBER(16)) else null end rule_map_id, fprint_id from
v_fp_map where attr_name like 'RLD_ID%') ruleMaps
 inner join vt_session_action_map actionMap on actionMap.rule_trace_fp_id
=
ruleMaps.fprint_id
 inner join vcrypt_tracker_usernode_logs sessions on sessions.request_id =
actionMap.request_id
  inner join (select substr(attr_name, 11) ruleInstanceId, case when
length(trim(translate(attr_value, '+-.0123456789', ' '))) is null then
CAST(attr_value AS NUMBER(16)) else null end attr_value, fprint_id from
v_fp_map where attr_name like 'RLD_STATUS%') ruleStatus
   on ruleStatus.ruleInstanceId = ruleMaps.ruleInstanceId and
ruleStatus.fprint_id = ruleMaps.fprint_id
 where ruleStatus.attr_value=1
union select ruleLogs.create_time, ruleLogs.rule_map_id,
policySetLogs.request_id, policySetLogs.runtime_type,
  userNodeLogs.user_id, userNodeLogs.node_id, ruleLogs.action_list
from VR_RULE_LOGS ruleLogs
  inner join VR_MODEL_LOGS modelLogs on ruleLogs.MODEL_LOG_ID =
modelLogs.MODEL_LOG_ID
  inner join VR_POLICY_LOGS policyLogs on modelLogs.POLICY_LOG_ID =
policyLogs.POLICY_LOG_ID
 inner join VR_POLICYSET_LOGS policySetLogs on policyLogs.POLICYSET_LOG_ID
=
policySetLogs.POLICYSET_LOG_ID
  inner join VCRYPT_TRACKER_USERNODE_LOGS userNodeLogs on
policySetLogs.REQUEST_ID = userNodeLogs.REQUEST_ID
```

```
 where ruleLogs.status=1);
commit;
```

2.7 Configuration Issues and Workarounds

This section describes the following configuration issues and workarounds:

- Database Archive and Purge Scripts Missing from Installation
- Juniper Login Fails Due to Incorrect CN Value and No UID Attribute in SAML Response

2.7.1 Oracle Linux 6 (OEL6) with the Unbreakable Enterprise Kernel (UEK), Oracle Linux 6 (OEL6) with the Red Hat Compatible Kernel, and Red Hat Enterprise Linux 6 (RHEL6) Certification

OAAM is certified on Oracle Linux 6 (OEL6) with the Unbreakable Enterprise Kernel (UEK), Oracle Linux 6 (OEL6) with the Red Hat Compatible Kernel, and Red Hat Enterprise Linux 6 (RHEL6). Note that OAAM 11g is certified on Oracle Linux 6 but during the installation of Oracle Identity Management (Oracle IdM), the user will see an alert message during the pre-requisite check. This error does not impact the installation and can be ignored. The user can click OK to continue the installation.

Bug 15833450 OAAM 11.1.1.5 is certified on Oracle Linux 6 (OEL6) with the Unbreakable Enterprise Kernel (UEK), Oracle Linux 6 (OEL6) with the Red Hat Compatible Kernel, and Red Hat Enterprise Linux 6 (RHEL6).

2.7.2 Database Archive and Purge Scripts Missing from Installation

Case and monitor data purge scripts are missing from the `oaam_db_purging_scripts.zip` file.

For purging case data, the following scripts need to be included:

- `create_case_purge_proc.sql`

  The `create_case_purge_proc.sql` script is required to set up the archive and purge routines for the Oracle database.

- `exec_sp_purge_case_data.sql`

  The `exec_sp_purge_case_data.sql` is required to perform the archive and purge of case data.

For purging monitor data, the following scripts need to be included:

- `drop_monitor_partition.sql`

  Customers who are using the Oracle table partitioning option and have no reporting database should run the `drop_monitor_partition.sql` script before setting up purging routine for monitor data.

- `exec_v_monitor_purge_proc.sql`

  The `exec_v_monitor_purge_proc.sql` script calls the stored procedures to archive and purge data from device fingerprinting tables.

- `create_v_monitor_purge_proc.sql`

The `create_v_monitor_purge_proc.sql` script creates the `V_MONITOR_DATA_PURGE` table and the stored procedure `SP_V_MON_DATA_PURGE_PROC` to archive and purge data from the transaction table.

2.7.3 Juniper Login Fails Due to Incorrect CN Value and No UID Attribute in SAML Response

After successful authentication, OAAM obtains the user attributes from the user store and sends user attributes in a SAML assertion to Juniper. Juniper is set up to look for attributes to read from the SAML assertion to match the user in its repository. Then it logs the user in to the requested target page or web application.

In this bug, the user is unable to log in to Juniper via OAAM because Juniper fails to identify the user. OAAM did not fetch the correct `cn` (common name) value and it did not set the `uid` (User ID) attribute in the SAML response.

2.8 Customer Care Issues and Workarounds

This section describes customer care and investigation issues. It includes the following topics:

- Investigator Role Overrides CSR Role When Both Roles Are Given to a User
- Scroll Bars Missing from Some Case Management Screens
- Case Search and Case Details Do Not Display Case Disposition
- Wrong User Attributed for Last Notes Added If Two Users Concurrently Update Case Notes
- Manually Created OAAM Agent Cases Cannot Be Searched by Username or User ID
- OAAM Allows Case Ownership Change and Add Notes Actions to Closed Case
- Create Agent Case Configurable Action Displays Wrong Name for Action
- KBA and OTP Failure Counter Reset and Unlock

2.8.1 Investigator Role Overrides CSR Role When Both Roles Are Given to a User

When a user is given both the Investigator and CSR Access roles, the former overrides the access permissions of the latter and the user has only Investigator access and no CSR access. Expected behavior is that a user having both Investigator and CSR access, should be able to perform Investigator and CSR tasks.

2.8.2 Scroll Bars Missing from Some Case Management Screens

Users with low resolution monitors are not able to see details in full in the Case Details page. Details refer to those available based on a user's role. The Case Details page required scroll bars so that a users with low resolution monitors can see all details.

2.8.3 Case Search and Case Details Do Not Display Case Disposition

After an OAAM Agent case is closed with a disposition of `Confirmed Fraud`, the agent can locate the case by searching by deposition but `Confirmed Fraud` is not displayed in the Case search page even after adding **Disposition** as a column to display. When the Case Details page of the same case is opened, the field is empty for **Disposition**.

2.8.4 Wrong User Attributed for Last Notes Added If Two Users Concurrently Update Case Notes

OAAM allows two agents to concurrently access a case, but if the two agents add notes to the case, OAAM saves both agents' notes; however, the second agent's notes are displayed as having been added by the first agent. Concurrent write access to cases is supported: if two agents are accessing the case at the same time, the second agent is made aware that the case is being worked on by another agent with a warning message. When the second agent continues, he is made the owner of the case. Notes are attributed to the correct agent.

2.8.5 Manually Created OAAM Agent Cases Cannot Be Searched by Username or User ID

When an OAAM Agent Case is autogenerated from the Configurable Action, the User Details panel is populated with user details for the session for which the case was created. When manually creating a case and linking to a session, user details are not populated. Subsequent searches of cases by `Username` or `User ID` only locate automatically created cases.

An enhancement has been made so that the Agent case creation page can optionally accept entry of a valid `Username` and/or `User ID` if the `oaam.customercare.agent.case.allow.userinfo` property is set to `true`. If a `Username` and/or `User ID` is entered it is mapped to the Agent case. Agent cases with a mapped `Username` and/or `User ID` are searchable by `Username` and/or `User ID`. These cases display the mapped user identifier in the **Username** and/or **User ID** column on the Cases search page. Only an Agent case that has been escalated from a CSR case displays the User Details section under the Case Details Summary tab.

2.8.6 OAAM Allows Case Ownership Change and Add Notes Actions to Closed Case

After an Agent case is closed, case ownership can still change when accessed by another user. The case owner is changed to the user who accessed the case. OAAM also allows the adding and editing of notes after a case is closed. After an Agent case is closed, no changes should be allowed.

2.8.7 Create Agent Case Configurable Action Displays Wrong Name for Action

When a Configurable Action triggers the `Create Agent Case` action, it is displayed as `Add to IP Watch list` for both the **Name** and **Description** of the action when it is added to an Action group.

2.8.8 KBA and OTP Failure Counter Reset and Unlock

Challenge failure counters are not displayed on the CSR Case Details as in the details pages. Failure counters should be displayed for KBA and OTP as well as for new or custom challenge processors. Also, the `Reset` action does not reset all the counters. An `Unlock` action should reset all counters (KBA and OTP). The following should occur for counters when the `Unlock` action is performed:

- Unlocking KBA resets the KBA and OTP failure counters to 0
- Unlocking OTP resets the KBA and OTP failure counters to 0

The following actions should occur for failure counters when the `Reset` action is performed:

- Resetting KBA resets KBA and OTP failure counters to 0. The user will be required to register challenge questions again
- Resetting CSR KBA resets KBA and OTP failure counters to 0. The user will be required to register challenge questions again
- Resetting OTP resets KBA and OTP failure counters to 0. The user will be required to register OTP again

The following enhancements have been made:

- OAAM Admin Console Case detail and details pages display failure counter, registration, and other information for KBA, OTP, and other custom challenge mechanisms
- OTP failure counters from different channels consolidate failures. For example, if multiple channels are used, the OTP status displays `Locked` if the combined OTP counters are above the threshold. So, if the user fails SMS twice and Email once and threshold is 3, they are locked using the consolidated OTP counter
- The `Reset` action resets all challenge failure counters
- The `Unlock` action is consolidated into an `Unlock User` action instead of separate actions for unlocking KBA and OTP. The `Unlock User` action resets all failure counters
- User name is displayed on the Case Details tab instead of or along with Case ID
- The Threshold value for failure counter can be set in the rule condition, `User: Challenge Channel Failure.`

2.9 Performance Issues and Workarounds

This section describes performance issues. It includes the following topic:

- Out of Memory Error Occurs Scrolling through Sessions Search in OAAM Admin

2.9.1 Out of Memory Error Occurs Scrolling through Sessions Search in OAAM Admin

Scrolling up and down on the Session search page may pass an empty or null input list, which may result in retrieving millions of rows from the database, causing the error, `java.lang.OutOfMemoryError:GC overhead limit exceeded`.

2.10 Device Fingerprinting Issues and Workarounds

This section describes device fingerprinting issues. It includes the following topic:

- Errors Occur When Custom Locale is Used in OAAM .NET

2.10.1 Errors Occur When Custom Locale is Used in OAAM .NET

When the .Net API is used to generate a browser fingerprint that uses a custom locale as part of the login flow, an error occurs: `Culture ID 4096 (0x1000) is not a supported culture.\r\nParameter name: culture.` The issue occurs when the application is using a custom culture because locale is registered with the Microsoft .NET framework and when the OAAM .NET API classes try to construct the `CultureInfo` from the LCID that came into the `HttpSession`, an exception occurs because of the Microsoft .NET framework. The workaround is to change the `oaam/src/dotNET/Bharosa/vCrypt/Common/Util/HttpUtil.cs` line `162` from

`CultureInfo ci = new CultureInfo(context.Session.LCID);` to `CultureInfo ci = new CultureInfo(context.Current.Request.UserLanguages[0]);`

This causes .NET to look up the locale by the name of the locale instead of by the LCID.

2.11 Geolocation Data Loader Issues and Workarounds

This section describes geolocation loader issues. It includes the following topics:

- Upload of Geolocation Data Causes Unique Constraint Violation
- IP Location Data Loader Fails If There is a Blank Line in the File

2.11.1 Upload of Geolocation Data Causes Unique Constraint Violation

When reloading the same location data file, or loading an updated location data file, the data would be loaded correctly, but the log file would show numerous warnings about unique constraint violations which degrades performance.

2.11.2 IP Location Data Loader Fails If There is a Blank Line in the File

The OAAM data loader fails to load IP location data if a blank line is in the data file and does not report the line number. The expected result is for the OAAM data loader to skip the blank line and display a warning message that include the line number.

You can work around this issue by opening the IP location data file, removing the blank line, and saving the file. This issue will be fixed in a future release.

2.12 Multi-Language Support Issues and Workarounds

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

- Session or Cases Page Cannot Open if Browser Language is Italian
- Session Search and Case Search By Date Range Does Not Work in OAAM Admin Console When Browser Language is Brazilian Portuguese or Spanish

2.12.1 Session or Cases Page Cannot Open if Browser Language is Italian

When the browser language is set to Italian, the user cannot open pages with calendars in the OAAM Administration Console, such as the Session or Cases page. A pop-up window with the following error message is displayed:

```
java.lang.IllegalArgumentException:
Illegal pattern character 'g'
```

2.12.2 Session Search and Case Search By Date Range Does Not Work in OAAM Admin Console When Browser Language is Brazilian Portuguese or Spanish

Searching sessions and cases by date range does not work in the OAAM Administration Console when the browser language is set to Brazilian Portuguese or Spanish. When the user opens the calendar in the Session or Cases page in the Spanish or Brazilian Portuguese locale, the year value is always shown as `1970` and cannot be modified to the correct year. As a result, the search does not work and the expected data cannot be returned in the search results.

3

Oracle Access Manager

This chapter describes issues associated with Oracle Access Manager 11*g* Release 1 (11.1.1). It includes the following topics:

3.1 Patch Requirements

This section describes patch requirements for Oracle Access Manager 11*g* Release 1 (11.1.1). It includes the following sections:

See Also:

- Oracle Technology Network for details about the latest supported versions and platforms:

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

- *Oracle Fusion Middleware Patching Guide* for details about the latest patch set
- My Oracle Support at the following URL for the latest Oracle Access Manager 11*g* Release 1 (11.1.1) bundle patches and related release notes:

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

3.1.1 Plain Text Credentials Exposed in Diagnostic Logs when Creating an Identity Store

To work around this issue:

1. Go to **My Oracle Support** at

http://support.oracle.com

2. Click the **Patches & Updates** tab, and search for **bug 9824531**.Download the associated patch and install it by following the instructions in the README file included with the patch.
3. On the **Patches & Updates** tab, search for **bug 9882205**. Download the associated patch and install it by following the instructions in the README file included with the patch.

3.2 General Issues and Workarounds

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

3.2.1 Resource Protected By Federation Shown Without Authentication

When accessing a page protected by the new Oracle Access Manager integrated Federation feature with the Internet Explorer browser, the browser's delete cookies option does not delete cookies and, therefore, authentication will not be requested. This is a browser specific issue.

Workaround: Delete the browsing history using Tools-> Internet Options-> Browsing History (make sure Cookies is selected) and close all instances of Internet Explorer. When accessing the OAM protected page again; authentication will be requested.

3.2.2 SSO Authentication Screen Does Does Not Appear If Using Oracle Traffic Director

The Host Identifier attribute takes a value equal to the name of the resource being protected when a policy is defined. When a WebGate intercepts a request for access to

the resource, it checks the request for an address. If the address is on the Host Identifiers list, it is mapped to the Host Identifier name and all policies and rules applicable to it can be applied. In this situation, if Oracle HTTP Server is fronted by Oracle Traffic Director (load balancer), an exception acknowledging that all required hosts and ports have not been added to the list is thrown. Use the following steps to update the Host Identifier list.

1. Launch the Oracle Access Manager Conosle.
2. Click the Policy Configuration tab on the left.
3. Click Host Identifiers in the Policy Configuration pane.

   The Host Identifiers page appears.
4. Find the appropriate host identifier using the search functionality.
5. Select the appropriate host identifier from the search results and click Edit.
6. Type the name of the host in the Name field.
7. (Optional) Type a short description in the Description field.
8. Enter all variations for identifying this host in the Host Name Variations field.

   A default port number will not be added if one is not provided.
9. Click Save and restart the Oracle Access Manager administration and managed servers.

3.2.3 Issues Registering the OSSO Plugin

The OSSO Plugin is for iPlanet and IIS when a customer does not wish to use OHS. It must be registered with OID/SSO 10.1.2.3 or 10.1.4.3 which have been discontinued as of 2011.

3.2.4 Modify Authentication Scheme When Upgrading OAM 11.1.1.5 to OAM 11.1.1.7

For any Oracle Access Manager customer that upgrades from OAM 11.1.1.5 to OAM 11.1.1.7 and uses a custom login page, remove the `redirect=true` entry from Challenge Parameters in the AnonymousScheme authentication scheme or the Login Page will not work. Details are in MOS Note 1548551.1.

3.2.5 RemoteRegistrationServerException Seen After PasteConfig IDM (T2P)

Even when pasteConfig goes through successfully, a RemoteRegistrationServerException is logged. If you can access the Oracle Access Manager console and see all the agents, this exception is benign and can be ignored.

3.2.6 System Error Page Displayed After Login

After successfully logging in to a page with a longer URL, an Oracle Access Manager system error page might be displayed; access to the same page would not have resulted in this in previous releases. Accessing the page with a longer URL a second time may clear this condition.

3.2.7 T2P Paste Config Operation Fails With Exception

When trying to complete the paste config portion of the Test to Production procedure, the following exception may occur:

```
javax.management.RuntimeMBeanException:
javax.management.RuntimeMBeanException: Configuration MBean not initialized.
```

There is currently no workaround for this issue.

3.2.8 Creating Policies For Webgate 11g

Oracle Identity Manager and Oracle Access Manager integrations support Webgate 11g. Follow this procedure to create policies for Webgate 11g.

1. Modify the value for WEBGATE_TYPE in the `idmConfigTool configOAM` and `idmConfigTool configOIM` property files.
   - ohsWebgate11g (for Webgate 11)
   - ohsWebgate10g (for Webgate 10)
2. Log in to the Oracle Access Manager console.
3. Select the Policy Configuration tab.
4. Expand Application Domains - IAM Suite
5. Click Resources.
6. Click Open.
7. Click New resource.
8. Provide values for the following:
   - Type: HTTP
   - Description: OAM Credential Collector
   - Host Identifier: IAMSuiteAgent
   - Resource URL: /oam
   - Protection Level: Unprotected
   - Authentication Policy: Public Policy
9. Click Apply.

3.2.9 Sending Valid Cookie For Embedded BI Content

When embedded BI content and Oracle Access Manager are on different physical machines or accessed from different ports on the same machine, the BI proxy on the application's container needs to authenticate itself to the Oracle Access Manager server in order to access the protected BI content. To ensure that the valid OAMAuthnCookie is sent to the Webgate, `filterOAMAuthnCookie=false` should be set in the User Defined Parameters section of the Webgate's configuration profile. Restart the server after the modification for the new parameter value to take effect.

3.2.10 Incorrect SSO Agent Date/Time Shown to User

The default start date on the Create OAM Agent page is based on the Oracle Access Manager server date/time. The date/time shown to the end user is based on the Oracle Access Manager server time zone rather than on the user's machine.

3.2.11 Initial Messages After Webgate Registration Are Not Shown in the User's Locale

After Webgate registration, the description fields in the initial messages for related components are not shown in the user's locale.

The description field does not support Multilingual Support (MLS).

3.2.12 Single-Click to Open Child Node is Not Supported in the Navigation Tree

Single-click to open a child node in the navigation tree is not supported, but double-click is supported.

3.2.13 User Credential for Registration Tool Does Not Support Non-ASCII Characters on Native Server Locale

The user credential for the Oracle Access Manager registration tool `oamreg.sh/oamreg.bat` does not support non-ASCII characters on the Linux Non-UTF8 server locale and the Windows native server.

3.2.14 Turkish and Greek Character Issues on Oracle Access Manager Authentication Page

In some cases if a user has Turkish, German, or Greek special characters in the user name and the login name only differs in the special characters, he might pass authentication because of case mappings and case-insensitivity.

Some internationalization characters should have special capitalization rule so that characters do not convert back to the lower case.

For example, there is the case with SS and ß in German, where ß only exists as a lower case character. When performing "to Upper" against ß, ß will be changed to SS. And if the upper case text is then converted back to lower case, the SS becomes ss and not the original ß.

3.2.15 Oracle Access Manager Authentication Does Not Support Non-ASCII Passwords on Locales Other than UTF8

When the server locale is not UTF-8 and using WebLogic Server embedded LDAP as an identity store, the SSO Authentication page does not support Non-ASCII passwords.

3.2.16 Error Message of Create Agent Shows as Server Locale

When an administrator creates an agent with the same name as one that already exists, the language of the error message displayed is based on the server locale rather than on the browser locale.

3.2.17 Referrals in LDAP Searches

Oracle Access Manager 11g Release 1 (11.1.1) cannot operate directly with LDAP servers returning referrals.

The workaround is to use Oracle Virtual Directory.

3.2.18 Non-ASCII Resources Require OHS To Restart To Make Protection Take Effect

When you add a resource with a non-ASCII name to the protected authentication policy, it will require the 11g OHS Server to restart to make the protection take effect, whereas in adding resources with English characters, protection takes effect in real time without having to restarting the OHS Server.

3.2.19 Non-ASCII Characters on Success/Failure URL Results in Garbled Redirect URL

If an on success or on failure URL configured for an authentication policy contains non-ASCII characters in the URL specified, then the URL specified will be garbled when it is used during a user authentication. This will happen only when the authentication scheme is Basic Authentication and the end user's browser is the Simplified Chinese version of IE8 running on the Chinese version of Windows.

3.2.20 Resource with Non-ASCII Characters Cannot Be Protected by an OSSO Agent

The OSSO Agent cannot protect a resource because it does not encode the entire resource URL to UTF-8 format.

To work around this issue, use the Webgate Agent instead of the SSO Agent.

Webgate is able to convert the entire resource URL to UTF-8 format.

3.2.21 Error in Administration Server Log from Console Logins

If you log in to the Oracle Access Manager Console as an administrator and then log in to the Console as an administrator in a new browser tab, the following error appears in the administration logs:

```
------------------------------------------------------------
<May 20, 2010 10:12:47 AM PDT> <Error>
<oracle.adfinternal.view.page.editor.utils.ReflectionUtility> <WCS-16178>
<Error instantiating class -
oracle.adfdtinternal.view.faces.portlet.PortletDefinitionDTFactory>
------------------------------------------------------------
```

The error message does not impact functionality.

3.2.22 Application Domain Subtree in the Navigation Tree Is Not Rendered and Does Not Respond to User Actions

If the Application Domain subtree on the navigation tree does not render or respond to user interface actions over a period of time, it may be the result of multiple refreshes.

To work around these issues, restart the administration server and log in to the Oracle Access Manager Console again.

3.2.23 editWebgateAgent Command Does Not Give An Error If Invalid Value is Entered

The WLST command `editWebgateAgent` does not give an error when a invalid value is entered for the **state** field in both online and offline mode. The Oracle Access Manager Console does show the **state** field value as neither **enabled** nor **disabled**, though it is a mandatory field.

3.2.24 WLST Command displayWebgate11gAgent In Offline Mode Displays the Webgate Agent Entry Twice

In the offline mode, the WLST command, `displayWebgate11gAgent`, displays the 11*g* Webgate Agent entry in the System Configuration tab twice.

3.2.25 Message Logged at Error Level Instead of at INFO When Servers in Cluster Start

When starting Oracle Access Manager servers in a cluster, the following message is displayed:

```
<Jun 22, 2010 3:59:41 AM PDT> <Error> <oracle.jps.authorization.provider.pd>
<JPS-10774> <arme can not find state.chk file.>
```

The correct level of the message is `INFO`, rather than `Error`.

3.2.26 Help Is Not Available for WLST Command registeroifdappartner

The Help command is not available for the WLST command, `registeroifdappartner`.

The online and offline command registers Oracle Identity Federation as a Delegated Authentication Protocol (DAP) Partner.

For information, refer to "registerOIFDAPPartner" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Syntax

```
registerOIFDAPPartner(keystoreLocation="/scratch/keystore"
logoutURL="http://<oifhost>:<oifport>/fed/user/sploosso?doneURL=
http://<oamhost>:< oam port>/ngam/server/pages/logout.jsp",
rolloverTime="526")
```

Parameter Name	Definition
keystoreLocation	Location of the Keystore file. The file generated at the OIF Server. (mandatory)
logoutURL	The OIF Server's logout URL. <mandatory>
rolloverInterval	The Rollover Interval for the keys used to enc/decrypt SASSO Tokens (optional)

Example

```
The following invocation illustrates use of all parameters.

registerOIFDAPPartner(keystoreLocation="/scratch/keystore",
logoutURL="http://<oifhost>:<oifport>/fed/user/sploosso?doneURL=http://<oamhost>:
<oam port>/ngam/server/pages/logout.jsp", rolloverTime="526")
```

3.2.27 User Must Click Continue to Advance in Authentication Flow

In a native integration with Oracle Adaptive Access Manager, the resource is protected by an Oracle Access Manager policy that uses the Basic Oracle Adaptive Access Manager authentication scheme.

When a user tries to access a resource, he is presented with the username page.

After he enters his username, he must click **Continue** before he can proceed to the password page. He is not taken to this page automatically.

The workaround is for the user to click **Continue**, which might allow him to proceed to the password page.

3.2.28 OCSP-Related Fields are Not Mandatory

In the X509 authentication modules, the following OCSP-related fields are no longer mandatory:

- OCSP Server Alias
- OCSP Responder URL
- OCSP Responder Timeout

If OCSP is enabled

The OCSP-related fields should be filled in by the administrator. If they are not filled, there will not be an error from the Console side.

It is the responsibility of the administrator to provide these values.

If OCSP is not enabled

The OCSP-related fields need not be filled in this case. If there are values for these fields, they will be of no consequence/significance, as OCSP itself is not enabled.

In the default out of the box configuration, the OCSP responder URL is `http://ocspresponderhost:port`. If you make changes to other fields and leave this as is, you will see a validation error, since this value is still submitted to the back end and at the Console, the layer port should be a numeric field. You can either modify the field, with the port being a numeric field or delete the entire value.

3.2.29 Database Node is Absent in the Console

Under the Data Sources node of the System Configuration tab, Common Configuration section, there is no Databases node in Oracle Access Manager 11g (11.1.1.5).

3.2.30 Online Help Provided Might Not Be Up To Date

Online help is available in the Oracle Access Manager Console, but you should check OTN to ensure you have the latest information.

3.2.31 Oracle Access Manager Audit Report AUTHENTICATIONFROMIPBYUSER Throws a FROM Keyword Not Found Where Expected Error

The Oracle Access Manager audit report **AuthenticationFromIPByUser** uses an Oracle Database 11.2.0 feature and will not work with older versions of database. The following error is displayed if an older version is used:

```
ORA-00923: FROM keyword not found where expected
```

3.2.32 Disabled: Custom Resource Types Cannot be Created

For Oracle Access Manager 11g, creating custom resource types should not be attempted. In the initial release, the buttons to create/edit/delete resource types were available.

With Oracle Access Manager 11g (11.1.1.7) these command buttons are disabled. Oracle provided resource types include:

- HTTP (includes HTTPS)
- TokenServiceRP (Resources for representing Token Service Relying Party)
- wl_authen (Resources for representing WebLogic Authentication schemes)

3.2.33 Use of a Non-ASCII Name for a Webgate Might Impact SSO Redirection Flows

When using the OAM Server with WebGates and when the Webgate ID is registered with a non-ASCII name, the OAM Server may reject that authentication redirect as an invalid request.

To work around this redirection issue, use an ASCII name for the Webgate.

Note: Resources are protected and error messages do not occur when the administration server and oracle access servers are started on UTF-8 locales.

The redirection issue only occurs on native server locales (Windows and Non-UTF8 Linux server locales)

3.2.34 Authentication Module Lists Non-Primary Identity Stores

In the user interface under the Authentication Module, only the primary identity store should be selected in the list since only primary identity stores can be used for authentication/authorization. Currently, the Oracle Access Manager Console allows you to select identity stores that are not primary.

3.2.35 Unable to Stop and Start OAM Server Through Identity and Access Node in Fusion Middleware Control

The following Oracle Access Manager operations are not supported through using the **oam_server** node under **Identity and Access** in Fusion Middleware Control:

- Start up
- Shut down
- View Log Messages

However, these operations are supported per the Oracle Access Manager managed server instance through using the **oam_server** node (for the specific server) under **Application Deployments** in Fusion Middleware Control.

3.2.36 AdminServer Won't Start if the Wrong Java Path Given with WebLogic Server Installation

WebLogic Server installation on Windows 64-bit platform can be successful with 32-bit JAVA_HOME (jdk1.6.0_23). On Windows 64-bit platform, the path to 32-bit JAVA_HOME (c:\program files (x86)\java\jdkxxx) is not correctly handled by the startWeblogic.cmd.

- If you launch the install shield with setup.exe, you are asked for the path of the 64-bit JAVA_HOME. If you provide the 32-bit JAVA_HOME (jdk1.6.0_24) path, the install shield is not launched.
- If you execute config.cmd from \Middleware\Oracle_IDM1\common\bin, the path to the 32-bit JAVA_HOME (jdk1.6.0_24) is used. Following successful installation, however, you cannot start AdminServer.

Workaround: Oracle recommends replacing SUN_JAVA_HOME to use the path with the shorter name (c:\progra~2\java\jdkxxxx).

- On Windows, the shorter names can be seen by executing "dir /X".
- Alternatively, you can set Windows command shell variable JAVA_HOME to path with shorter name and execute startWeblogic.cmd within that. For example:

```
>set JAVA_HOME=c:\progra~2\java\jdkXXX

>startweblogic.cmd
```

3.2.37 Changing UserIdentityStore1 Type Can Lock Out Administrators

An Identity Store that is designated as the System Store should not be edited to change the store type (from Embedded LDAP to OID, for instance) nor the connection URLs.

If you do need to change the Identity Store that is designated as the System Store should not be edited to change the store type, Oracle recommends that you create a new Identity Store and then edit that registration to mark it as your System Store.

3.2.38 Page Layouts and Locales

The layout of the single sign-on (SSO) Login Page, Impersonation Consent page, Logout Page, Impersonation Error page, and Login Error Page do not change for Arabic and Hebrew locales.

3.2.39 Some Pages Are Not Correctly Localized

The date formats of "Creation Instant" and "Last Access Time" on the Session Management Search page are not correctly localized.

3.2.40 Non-ASCII Query String Issues with Internet Explorer v 7, 8, 9

Due to a limitation with the Internet Explorer browser, resources with Non-ASCII query string when if you directly type or paste the resource URL.

3.2.41 Oracle Virtual Directory with SSL Enabled

With Oracle Virtual Directory as the user identity store, no errors are seen after changing its registration to use the SSL port, checking the SSL box, and testing the connection (Test Connection button). However, authentication fails (even though non-SSL port is fine). The first time Test Connection goes through and any subsequent time it results in Socket Timeout exception from the Oracle Virtual Directory side.

Workaround: Disable NIO for the SSL port as follows:

1. Stop Oracle Virtual Directory. For example:

```
$ORACLE_INSTANCE/bin/opmnctl stopproc ias-component=ovd1
```

2. Edit the a LDAP SSL listener section of listener.os_xml to add `<useNIO>false</useNIO>`, as follows:

```
$ORACLE_INSTANCE/config/OVD/ovd1/listener.os_xml

<ldap version="20" id="LDAP SSL Endpoint">
<port>7501</port>
<host>0.0.0.0</host>
.........
.........
```

```
<tcpNoDelay>true</tcpNoDelay>
<readTimeout>180000</readTimeout>
</socketOptions>
<useNIO>false</useNIO>
</ldap>
```

3. Save the file.
4. Test the connection several times to confirm this is working.

3.2.42 Query String Not Properly Encoded

There is no encoding on the query string from Webgate when % is not followed by a sequence of characters that form a valid URL escape sequence. In this case, Oracle Access Manager etains % as % in the decoded string and the following error occurs:

```
No message for The Access Server has returned a status that is unknown to the
Access Gate .Contact your website administrator to remedy this problem.
```

Workaround:

11g Webgate: To specify the '%' character in a query string, you must specify '%25' instead of '%'.

10g Webgate: The 11g Webgate workaround applies to only the anonymous scheme. For other authentication schemes, there is currently no workaround.

3.3 Configuration Issues and Workarounds

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

- Section 3.3.13, "Finding and Deleting Sessions Using the Console"
- Section 3.3.14, "Non-ASCII Users with Resource Protected by Kerberos Authentication Scheme"

3.3.1 For mod-osso Value for RedirectMethod Should be "POST"

For Webgate to support long URLs, the following code sample was added under `oam-config.xml`:

```
<Setting Name="AgentConfig" Type="htf:map">
   <Setting Name="OSSO" Type="htf:map">
        <Setting Name="RedirectMethod"Type="xsd:string">GET</Setting>
        <Setting Name="Delimiter" Type="xsd:string">AND</Setting>
   </Setting>
```

For `mod-osso`, the value for `RedirectMethod` should be `POST`, however, the values shipped out of the box is `GET`. Follow these steps to perform the modification, as this change needs to be performed manually and there is no user interface or WLST commands available to do so.

1. Stop the Oracle Access Manager Console and managed servers.
2. Enter cd `DOMAIN_HOME/config/fmwconfig`
3. Enter vi `oam-config.xml`
4. Go to the following line in `oam-config.xml`:

   ```
   <Setting Name="AgentConfig" Type="htf:map">
      <Setting Name="OSSO" Type="htf:map">
           <Setting Name="RedirectMethod"Type="xsd:string">GET</Setting>
   ```

   Modify `GET` to `POST` as follows:

   ```
   <Setting Name="RedirectMethod"Type="xsd:string">POST</Setting>
   ```

5. Save the changes and start the AdminServer and managed servers.

3.3.2 User Wrongly Directed to the Self-User Login after Logging Out of the Oracle Identity Manager Administration Console

The user is directed to the self-user login after logging out of the Oracle Identity Manager Administration Console.

To be redirected correctly, the logout must work properly.

The workaround for logout with 10g Webgate is to:

1. Copy `logout.html` (for example, from `Oracle_IDM1/oam/server/oamsso/logout.html`) to `webgate_install_dir/oamsso`.
2. Update logout URL in the file to `http://oam_server:oam_server/ngam/server/logout`.
3. If redirection to specific page has to occur after logout, change the logout URL to `http://oam_server:oam_server/ngam/server/logout?doneURL=http://host:port/specifipage.html`.

3.3.3 11g Webgate Fails to Install with Compact Configuration

A compact configuration is an installation with all identity management components on a machine with limited hardware capacity.

On trying to install the 11g Webgate with compact configuration, the following error occurs during the configure step:

```
Configuring WebGate...
There is an error. Please try again.
Preparing to connect to Access Server. Please wait.
Client authentication failed, please verify your WebGate ID.
cp: cannot stat
`$ORACLE_HOME/ohs/conf/aaa_key.pem':
No such file or directory
cp: cannot stat
`$ORACLE_HOME/ohs/conf/aaa_cert.pem':
No such file or directory
cp: cannot stat
`$ORACLE_HOME/ohs/conf/aaa_chain.pem':
```

The error occurs because the following entries were not initialized in `oam-config.xml` during the installation:

```
<Setting Name="oamproxy" Type="htf:map">
<Setting Name="sslGlobalPassphrase" Type="xsd:string">changeit</Setting>
<Setting Name="SharedSecret" Type="xsd:string">1234567812345678</Setting>
</Setting>
```

To initialize `oam-config.xml` properly:

1. Delete the `OAM` entry from CSF repository by performing the following steps:
   a. Start the WebLogic Scripting Tool:

      oracle_common/*oracle_common*/common/bin/wlst.sh

   b. In the WLST shell, enter the command to connect to the domain and then enter the requested information.

      A sample is given below.

      ```
      wls:/offline> connect ()
      Please enter your username [weblogic] :
      Please enter your password [welcome1] :
      Please enter your server URL [t3://localhost:7001] :
      Connecting to t3://localhost:7001 with userid weblogic ...
      Successfully connected to Admin Server 'AdminServer' that belongs to domain
      'imdomain86'.
      ```

   c. Change to `domainRuntime`.

      A sample is given below.

      ```
      wls:/imdomain86/serverConfig> domainRuntime ()
      Location changed to domainRuntime tree. This is a read-only tree with
      DomainMBean as the root.
      ```

   d. Check whether an entry exists in the CSF repository with the map name as `OAM` and key as `jks`.

      A sample is given below.

      ```
      wls:/imdomain86/domainRuntime> listCred(map="OAM_STORE",key="jks")
      {map=OAM_STORE, key=jks}
      Already in Domain Runtime Tree
      .
      [Name : jks, Description : null, expiry Date : null]
      PASSWORD:1qaldrk3eoulhlcmfcqasufgj2
      ```

.

e. Delete the `OAM` map entry from the CSF repository.

```
wls:/imdomain86/domainRuntime> deleteCred(map="OAM_STORE",key="jks")
{map=OAM_STORE, key=jks}
Already in Domain Runtime Tree
.
```

f. Exit from wlst shell.

A sample is given below.

```
wls:/imdomain86/domainRuntime> exit ()
.
.
.
```

2. Go to *DOMAIN_HOME*/config/fmwconfig and delete the file `.oamkeystore`.

   A sample [on linux] is given below.

```
[aime@pdrac09-5 fmwconfig]$ rm .oamkeystore
.
```

3. Stop the Managed Server and Admin Server.
4. Start the AdminServer.
5. Verify `oam-config.xml`.
6. Start Managed Server.

Steps to verify `oam-config.xml`:

1. Go to *DOMAIN_HOME*/config/fmwconfig/oam-config.xml.
2. Verify that all the WebLogic Server server instances are configured under **DeployedComponent** > **Server** > **NGAMServer** > **Instance**
3. Verify that the OAM Managed Server protocol, host and port are available at:

   DeployedComponent > **Server** > **NGAMServer** > **Profile** > **OAMServerProfile** > **OAMSERVER**
4. Verify that the SSO CipherKey is generated and available at:

   DeployedComponent > **Server** > **NGAMServer** > **Profile** > **ssoengine** > **CipherKey**
5. Verify that the `oamproxy` entries for `SharedSecret` and `sslGlobalPassphrase` is generated and available at:

   DeployedComponent > **Server** > **NGAMServer** > **Profile** > **oamproxy**

   `SharedSecret` should have a value different from `1234567812345678` and `sslGlobalPassphrase` different from `changeit`.

3.3.4 Download IBM JDK to Fix Issue with Configuring Remote Administrators

If Oracle Access Manager remote registration of administrators is failing on AIX, download IBM JDK 1.6 SR7 with Interim Fixes (iFix) for Oracle.

> **Note:** These instructions are to be followed only for IBM JDK 1.6 SR7+ifixes. They are not applicable for SR7.

If you do not have a universal IBM user ID, you can register by following the instructions on the IBM Web site. If there are any registration related issues, contact IBM as instructed on their Web site.

1. Go to

   https://www14.software.ibm.com/webapp/iwm/web/reg/signup.do?source=swg-ibmjavaisv&S_TACT=IBMJavaISV%E2%8C%A9=en_US

2. Click **Downloads**.

   You are taken to the IBM software downloads page.

3. Enter the Access Key, `MJ3D7TQGMK`.

4. Select to use the **Download Director** (recommended for Windows) or **HTTP** (recommended for UNIX).

   The builds will appear under the product name: **IBM SDK's for Oracle Fusion Middleware 11g**.

   As noted earlier, the version that should be downloaded and used is:

   pap6460sr7ifix-20100512_01(JDK 6 SR7 +IZ70326+IZ68993+IZ74399)

3.3.5 Auditing Does Not Capture the Information Related to Authentication Failures if a Resource is Protected Using Basic Authentication Scheme

Although a resource can be protected using the BASIC scheme, the WebLogic server has a feature by which it first authenticates the user and then sends it to the server.

If you add the following flag under `<security-configuration>` in `config.xml` and restart the server, you will be able to bypass WebLogic server's authentication `<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>`. Once the credentials are submitted back to the OAM Server, it will be audited.

The WebLogic Server Administration Console does not display or log the `enforce-valid-basic-auth-credentials` setting. However, you can use WLST to check the value in a running server. You must modify this value by setting this in `config.xml`.

To do so, refer to "Developing Secure Web Applications" at:

http://download.oracle.com/docs/cd/E13222_01/wls/docs103/security/thin_client.html#wp1037337

3.3.6 Unable to Access Partner Information on the Production Environment

After test-to-production migration, the following steps must be performed:

1. Ensure that the production OAM Server(s) are down when the policy is imported from the test system.
2. Log in to the Oracle Access Manager Console and modify the primary /secondary server list for all agents in the production system (including the IAMSuiteAgent).
3. Copy the generated artifacts for Webgate generated for each of the Webgate agents (excluding IAMSuiteAgent).
4. Start the production OAM managed server(s).
5. Restart all the Webgate agents' OHS.

In migrating partner information from a test environment to a production one, you will not be able to access partner information if

- The `migratePartnersToProd` command was used. It is outdated. The following set of commands should be used instead:
  - `exportPartners`- This command is used to export the partners from the test environment. It needs to be run from the OAM Server, from where the partners needs to be exported. This command takes the path to the temporary `oam-partners` file as a parameter.

    ```
    exportPartners(pathTempOAMPartnerFile=', <pathTempOAMPartnerFile>')
    ```

  - `importPartners`- This command is used to import the partners to the production environment. It needs to be run from the OAM Server to which the partners needs to be imported. This command takes the path to the temporary `oam-partners` file as a parameter.

    ```
    importPartners(pathTempOAMPartnerFile=', <pathTempOAMPartnerFile>')
    ```

- The agent profiles were not edited after the migration to match the production system.

  A Webgate Agent might be configured with a list of primary/secondary server hosts and nap ports available in the test system. The production system may not contain server instances with the same hosts and ports as configured in the test system. Since the SysConfig Agent Profile user interface obtains the server name by picking up the servers matching the host and port details of the primary/secondary server list, the server names may not be displayed in the user interface after migration. Since the primary/secondary server lists could be a subset of the list of available server instances in the production system, the agent profiles need to be edited after migration to match the production system.

3.3.7 Incompatible Msvcirt.dll Files

When you install the Oracle Access Manager 10g Webgate, do not replace the current version of `msvcirt.dll` with a newer version when prompted. If you do so, there may be incompatibility issues. Later, when you try to install OSSO 10g (10.1.4.3), the `opmn.exe` command might fail to start and the `OracleCSService` might time out because the required `.dll` file is missing.

3.3.8 IPv6 Support

The supported topology for Oracle Access Manager 11g is shown below.

Supported Topology

- WebGate10g or Webgate 11g and protected applications on IPv4 (Internet Protocol Version 4) protocol host
- OHS (Oracle HTTP Server) reverse proxy on dual-stack host
- Client on IPv6 (Internet Protocol Version 6) protocol host

Dual-stack is the presence of two Internet Protocol software implementations in an operating system, one for IPv4 and another for IPv6.

The IPv6 client can access Webgate (10g or 11g) through the reverse proxy on IPv4/IPv6 dual-stack.

3.3.9 What to Avoid or Note in Oracle Access Manager Configuration

This section contains scenarios and items to note in Oracle Access Manager Configuration

3.3.9.1 Unsupported Operations for WLST Scripts

WLST scripts for Oracle Access Manager 10g and Oracle Access Manager 11g WebGates do not support changing Agent security modes.

3.3.9.2 Unsupported Operations for Oracle Access Manager Console and WLST

Unsupported operations for the Oracle Access Manager Console and WLST are described in the following subsections.

3.3.9.2.1 OAM Server

Use Case: Concurrent Deletion and Updating

Description

1. Open an OAM Server instance in edit mode in Browser 1.
2. Using the Oracle Access Manager Console in another browser (Browser 2) or using a WLST script, delete this server instance.
3. Return to Browser 1 where the server instance is opened in edit mode.
4. In Browser 1, click the **Apply** button.

Current Behavior

The Oracle Access Manager Console displays the message, "Server instance *server_name* might be in use, are you sure you want to edit it?" along with the confirmation that the update succeeded.

On clicking Yes, the following error message pops up, as expected, and the OAM Server instance page is closed (correct behavior):

`"Error while reading your_server-name OAM Server Instance Configuration."`
However, the navigation tree node might continue to display the OAM Server instance until you click the Refresh command button for the navigation tree.

Use Case: Two OAM Server Instances with Same Host Cannot have the Same Proxy Port.

Description

For this use case, there are two instances of the OAM Server: **oam_server1** and **oam_server2**.

1. Open **oam_server1** in edit mode and specify a host and OAM proxy port.
2. Now open **oam_server2** in edit mode and specify the same host and proxy port as **oam_server1**.

The changes are saved without any error message.

Current Behavior

The Oracle Access Manager Console does not display any error and allows the update.

The behavior is incorrect.

Use Case: Log Statements Detailing the Server Instance Creation, Update and Delete are not Present on the Oracle Access Manager Console

Description

If you create, edit, or delete an OAM Server instance from the Oracle Access Manager Console, the log statements corresponding to create, edit and delete are not displayed by the Console.

3.3.9.2.2 LDAP Authentication Module:

Use Case: Concurrent Deletion/Creation of User Identity Store does not Reflect in the List of Identity Stores in the LDAP Authentication Module Create and Edit

Description

1. Open create/ edit for the LDAP authentication module.

   A list displays the identity stores present in the system.
2. Now create a user identity store using another tab.
3. Return to the create/edit tab for the LDAP authentication module and check the list for user identity stores.

Current Behavior

The Oracle Access Manager Console displays the error message, as expected, and closes the Authentication Module page (correct behavior):

`"Error while reading` *`module-name`* `Authentication Module Configuration."`
However, the navigation tree node might continue to display the Authentication Module node until you click the Refresh command button for the navigation tree.

3.3.9.2.3 LDAP, Kerberos and X509 Authentication Module

Use Case: Concurrent deletion and updating

Description

1. Open an LDAP/Kerberos/X509 authentication module in edit mode in Oracle Access Manager Console in Browser 1.
2. Using Oracle Access Manager Console in another browser (Browser 2) or using a WLST script, delete this authentication module.
3. Now return to Browser 1 where the authentication module is opened in edit mode.
4. Click the **Apply** button.

Current Behavior

The Oracle Access Manager Console updates this authentication module configuration and writes it to back end.

The behavior is incorrect.

Use Case: Log Statements Detailing the Server Instance Creation, Update and Delete are Not present on Oracle Access Manager Console side.

Description

When you create, edit or delete an authentication module from Oracle Access Manager Console, the log statements corresponding to create, edit and delete are not written by the Console.

3.3.9.2.4 OAM 11G Webgate

Use Case: Concurrent Deletion and Update

Description

1. Open an OAM 11g Webgate instance in edit mode in Oracle Access Manager Console in Browser 1.
2. Using the Oracle Access Manager Console in another browser (Browser 2) or using a WLST script, delete this OAM 11g Webgate.
3. Now return to the Browser1 where the server instance is opened in edit mode.
4. Click on the **Apply** button.

Current Behavior

The Oracle Access Manager Console for edit OAM11g Webgate does not change and the tab does not close.

A OAM11g Webgate configuration not found error dialog is displayed by the Oracle Access Manager Console.

However, the navigation tree is blank and attempts to perform any operation results in a javax.faces.model.NoRowAvailableException".

The behavior is incorrect.

3.3.9.2.5 OSSO Agent

Use Case: Concurrent Deletion and Update

Description

1. Open an OSSO Agent instance in edit mode in the Oracle Access Manager Console in Browser 1.
2. Using the Oracle Access Manager Console in another browser (Browser 2) or using a WLST script, delete this OSSO Agent.
3. Now return to the Browser 1 where the OSSO Agent instance is opened in edit mode.
4. Click on **Apply** button.

Current Behavior

Editing the OSSO Agent in the Oracle Access Manager Console results in a null pointer exception.

The behavior is incorrect.

3.3.10 Install Guides Do Not Include Centralized Logout Configuration Steps

Single-Sign On is enabled after Oracle Access Manager is installed; to complete configuration of Single-Sign On out of the box, centralized log out must be configured post-install. Configure centralized log out by following direction from these sections:

- Configuring Centralized Logout for ADF-Coded Applications with Oracle Access Manager 11*g*

  In order for the ADF logout to work correctly, Single Sign-On Server Patch 9824531 is required. Install this patch, as described in the `readme` file that is included in the patch.

- Configuring Centralized Logout for the IDM Domain Agent (in the patch set this is now the IAMSuiteAgent)

3.3.11 NULL Pointer Exception Shown in Administration Server Console During Upgrade

A NULL pointer exception occurs because of the configuration events trigger when the identity store shuts down. The upgrade is successful, however, and error messages are seen in administration server console. There is no loss of service.

If the NULL pointer is seen during upgrade, there is no loss of service, you can ignore the error.

If the NULL pointer is seen during WLST command execution, you must restart the administration server.

3.3.12 Using Access SDK Version 10.1.4.3.0 with Oracle Access Manager 11g Servers

In general, the Sun Microsystems JDK 1.4.x compiler is the JDK version used with the Java interfaces of Access SDK Version 10.1.4.3.0.

As an exception, the Java interfaces of the 64-bit Access SDK Version 10.1.4.3.0, specifically for the Linux operating system platform, requires the use of Sun Microsystems JDK 1.5.x compiler.

The new Session Management Engine capability within Oracle Access Manager 11g will create a session for every Access SDK version 10.1.4.3.0 call for authentication.

This may cause issues for customers that use Access SDK to programmatically authenticate an automated process. The issue is the number of sessions in the system that is generated within Access SDK will increase dramatically and cause high memory consumption.

3.3.13 Finding and Deleting Sessions Using the Console

When session search criteria is generic (using just a wild card (*), for example), there is a limitation on deleting a session from a large list of sessions.

Oracle recommends that your session search criteria is fine-grained enough to obtain a relatively small set of results (ideally 20 or less).

3.3.14 Non-ASCII Users with Resource Protected by Kerberos Authentication Scheme

Non-ASCII users fail to access a resource protected by a Kerberos authentication scheme using WNA as a challenge method.

The exception occurs when trying to get user details to populate the subject with the user DN and GUID attributes.

3.4 Oracle Security Token Service Issues and Workarounds

This section provides the following topics:

3.4.1 No Warnings Given If Required Details are Omitted

On the Token Mapping page of a new Validation Template with the following characteristics:

- WS-Security
- Token Type SAML 1.1
- Default Partner Profile: requester profile

No warnings are given:

- If you check the box to Enable Attribute Based User Mapping if you leave empty the required User Attributes field

  A new row is not saved if the User Attribute field is empty. However, it is saved if both fields are filled. Removing the value of the User Attribute field in a user-added row causes the row to be deleted when you Apply changes

- If you attempt to delete built-in Name Identifier Mapping rows

  Built-in Name Identifier Mapping rows cannot be deleted.

3.4.2 New Requester Pages, Internet Explorer v7, and Japanese Locale

When using the Japanese Locale with Internet Explorer v7, the title "New Requester" is not displayed in one line on the page. The Partner, Name, Partner Type, and Partner Profile fields might wrap on the page.

This can occur whether you are creating or modifying the Partner (Requester, Relying Party, and Issuing Authority).

3.4.3 Delete Button Not Disabled When Tables Have No Rows

The Delete button is enabled even though there are no rows to be deleted in the following tables:

- The Attribute Name Mapping table (Token and Attributes page for Partner Profiles (Requester, Relying Party, Issuing Authority Profiles).
- The Value Mapping table in Issuing Authority Partner Profiles

When there are no rows in a table, the Delete button should be disabled by default.

3.4.4 Copying an Issuance Template Does Not Copy All Child Elements

Issuance Template Copy Like function does not copy nested tables (attribute mapping and filtering tables, and the custom token attribute table).

Workaround: Navigate to the desired Issuance Template, click the name in the navigation tree and click the Copy Like button. Manually enter missing information from the original: Attribute Mappings or custom attribute tables.

3.4.5 Apply and Revert Buttons are Enabled

The Apply and Revert buttons are enabled on Oracle Security Token Service pages even if there are no changes to apply or saved changes to revert to the previous version.

3.4.6 Only Generic Fault Errors Written to Oracle WSM Agent Logs

No content is written logs for the Oracle WSM agent errors. There is only a generic fault error.

Workaround: Enable message logging for the Oracle WSM agent on the host OAM Server.

1. Locate the logging.xml file in $DOMAIN/config/fmwconfig/server/oam_server1/logging.xml file.
2. Change the WSM block of the logging.xml file, to:

```
<logger name="oracle.wsm" level="TRACE:32" useParentHandlers="false">
<handler name="odl-handler"/>
</logger>

<logger name="oracle.wsm.msg.logging" level="TRACE:32"
useParentHandlers="false">
<handler name="owsm-message-handler"/>
<handler name="wls-domain"/>
</logger>
```

3. **OSTS Policies**: When Oracle Security Token Service policies are used (instead of Oracle-provided WSM policies) perform the following steps:
   a. Locate: Oracle_IDM1/oam/server/policy
   b. Unjar sts-policies.jar.
   c. Change all the polices to set Enforced to true: META-INF/polices/sts.

```
<oralgp:Logging orawsp:name="Log Message1" orawsp:Silent="true
orawsp:Enforced="true" orawsp:category="security/logging">
<oralgp:msg-log>
<oralgp:request>all</oralgp:request>
<oralgp:response>all</oralgp:response>
<oralgp:fault>all</oralgp:fault>
</oralgp:msg-log>
</oralgp:Logging>
```

4. Re-jar the updated sts-policies.jar.
5. Restart the AdminServer and managed servers.

3.4.7 Server and Client Key Tab Files Must be the Same Version

An exception to authenticate the Kerberos token occurs if WebLogic 10.3.5 is configured with Sun JDK6 greater than u18.

When using the Kerberos token as an authentication token requesting the security token from Oracle Security Token Service:

- The keytab file configured in the validation template should always be the latest version from the KDC server
- The KVNO should always be the latest that is available on the server:

3.4.8 Default Partner Profile Required for WS-Security

The *Oracle Access Manager Access Administration Guide* states "When you toggle the Token Protocol from WS-Trust to WS-Security, options in the Token Type list do not change. However, the required "Default Partner Profile" list appears from which you must choose one profile for WS-Security."

Correction: When you toggle the Token Protocol from WS-Trust to WS-Security a required field "Default Partner Profile" will appear. You must choose a value for this field. If you again toggle back to WS-Trust without choosing a value for this field The options in the Token Type list are not updated correctly to have the WS-Trust Token Type values.

3.4.9 SAML Token Issued When NameID is Not Found

Rather than returning an error response, an assertion issued with an empty NameIdentifier field can be issued even when the NameIdentifier user attribute has a null or empty value. For example:

```
<saml:NameIdentifier
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"/>
```

Workaround: The "Name Identifier User Attribute" Field in the Issuance Template requires a value for the Userstore.

3.5 Integration and Inter-operability Issues and Workarounds

This section provides the following topics:

- Section 3.5.1, "WNA Authentication Does Not Function on Windows 2008"
- Section 3.5.2, "JVM Plug-in Ignores Cookies Marked 'httponly'"

3.5.1 WNA Authentication Does Not Function on Windows 2008

The default Kerberos encryption supported by Windows 2008 Server and Windows 2007 machines are "AES256-CTS-HMAC-SHA1-96", "AES128-CTS-HMAC-SHA1-96" and "RC4-HMAC".

If the clients are configured to use DES only encryption, users will not be able to access protected resources with Kerberos authentication. The error message, `An incorrect username and password was specified` might be displayed.

Because the initial Kerberos tokens are not present, the browser sends NTLM tokens, which the OAM Server does not recognize; therefore, the user authentication fails.

The workaround is to enable the encryption mechanisms, and follow the procedure mentioned in:

`http://technet.microsoft.com/en-us/library/dd560670%28WS.10%29.aspx`

3.5.2 JVM Plug-in Ignores Cookies Marked 'httponly'

Cookies set with the `httponly` flag are not available to Browser Side Scripts and Java Applets. The JVM plugin ignores cookies marked 'httponly.'

To resolve the issue

1. In mod_sso.conf, disable the `OssoHTTPOnly off` parameter.

2. Add the required OSSO cookies to the list of possible applet parameters to pass for authentication.

3.6 Oracle Access Manager with Impersonation Workarounds

This section provides the following topics:

- Section 3.6.1, "Impersonation Can Fail on Internet Explorer v 7, 8, 9"
- Section 3.6.2, "With Oracle Access Manager 11g ORA_FUSION_PREFS Cookie Domain is Three Dots"

3.6.1 Impersonation Can Fail on Internet Explorer v 7, 8, 9

Due to a limitation with the Internet Explorer browser, Impersonation can fail to go to the Consent page when the Impersonatee's userid contains Non-ASCII characters.

Impersonation goes instead to the failure_url if you directly type or paste the starting impersonation URL in the browser.

3.6.2 With Oracle Access Manager 11g ORA_FUSION_PREFS Cookie Domain is Three Dots

With Oracle Access Manager 10g the ORA_FUSION_PREFS cookie domain used the following form (2 dots):

10g Form `.example.com`

However, Oracle Access Manager 11g localized login accepts only the following format for the ORA_FUSION_PREFS cookie domain (3 dots):

11g Form `.us.example.com`

For example, if the host name is `ruby.us.example.com`, Oracle Access Manager 11g creates a cookie with the domain name `.us.example.com`.

However, the application session creates a cookie with the domain name `.example.com`, which causes inter-operability failure between Fusion Middleware and the application session using this cookie.

Workaround: Update the `FACookieDomain` parameter to correspond to 11g requirements, and increment the `Version xsd:integer` in the oam-config.xml, as shown in this example:

1. Back up *DOMAIN_HOME*/config/fmwconfig/oam-config.xml.
2. Open the file for editing and pay close attention to your changes.
3. Set `FACookieDomain` to your domain (with 3 dot separators):

```
<Setting Name="FAAppsConfig" Type="htf:map">
     <Setting Name="FACookieDomain" Type="xsd:string">.us.example.com</Setting>
     <Setting Name="FAAuthnLevel" Type="xsd:integer">2</Setting>
     <Setting Name="consentPage" Type="xsd:string">/oam/pages/impconsent.jsp
     </Setting>
</Setting>
```

4. **Configuration Version:** Increment the `Version xsd:integer` as shown in the next to last line of this example (existing value (26, here) + 1):

   Example:

```
<Setting Name="Version" Type="xsd:integer">
```

```
  <Setting xmlns="http://www.w3.org/2001/XMLSchema"
    Name="NGAMConfiguration" Type="htf:map:>
  <Setting Name="ProductRelease" Type="xsd:string">11.1.1.3</Setting>
    <Setting Name="Version" Type="xsd:integer">26</Setting>
</Setting>
```

5. Save oam-config.xml.

3.7 Documentation Errata

This section provides documentation errata for the following guides:

- Section 3.7.1, "Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service"
- Section 3.7.2, "Oracle Fusion Middleware Developer's Guide for Oracle Access Manager and Oracle Security Token Service"
- Section 3.7.3, "Oracle Fusion Middleware Integration Guide for Oracle Access Manager"

3.7.1 Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service

There is no documentation errata for this guide.

3.7.2 Oracle Fusion Middleware Developer's Guide for Oracle Access Manager and Oracle Security Token Service

There is no documentation errata for this guide.

3.7.3 Oracle Fusion Middleware Integration Guide for Oracle Access Manager

This section contains documentation errata applicable to the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*, part number E15740-04 *only*.

The following documentation errata are included for this guide:

- Section 3.7.3.1, "Updates to Prerequisites for OAM-OIM Integration"
- Section 3.7.3.2, "Properties for configOIM Command"
- Section 3.7.3.3, "Updated Example for Integrating OIF/SP"

3.7.3.1 Updates to Prerequisites for OAM-OIM Integration

In the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*, part number E15740-04, Chapter 5 Integrating Oracle Access Manager and Oracle Identity Manager, Section 5.2 Prerequisites, Step 8a instructs you to prepare to configure LDAP synchronization (LDAP sync) in the domain where Oracle Identity Manager runs.

Step 8a directs you to Section 14.8.5 Completing the Prerequisites for Enabling LDAP Synchronization of the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*, Part Number E12002-09. This may be confusing as some steps of that section (such as creating the OIM user and group) are already complete.

Instead, Step 8a should direct you to Section 14.8.5.2 Creating Adapters in Oracle Virtual Directory of the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*, so that you can configure the Oracle Virtual Directory adapter for Oracle Internet Directory.

Also in Section 5.2 Prerequisites, Step 8c instructs you to run a configuration wizard to configure LDAP synchronization (LDAP sync) in the domain where Oracle Identity Manager runs. This step does not work if Oracle Identity Manager was installed without LDAP synchronization enabled.

Instead, Step 8c should direct you to Section 10.1 Enabling Postinstallation LDAP Synchronization of the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*, Part Number E14308-08, for the correct procedure to enable LDAP synchronization post-installation.

3.7.3.2 Properties for configOIM Command

Section 5.4, Perform Integration Tasks in Oracle Identity Manager, does not provide definitions of all the properties to be specified in the properties file when executing the `-configOIM` command in Step 3.

Use the following property definitions to assist you in configuring the properties file of the procedure:

Table 3–1 Properties for configOIM Command

Property	Definition
LOGINURI	URI required by OPSS. Default value is /${app.context}/adfAuthentication
LOGOUTURI	URI required by OPSS. Default value is /oamsso/logout.html
AUTOLOGINURI	URI required by OPSS. Default value is /obrar.cgi
ACCESS_SERVER_HOST	Oracle Access Manager hostname.
ACCESS_SERVER_PORT	Oracle Access Manager NAP port.
ACCESS_GATE_ID	The OAM access gate ID to which OIM needs to communicate.
OIM_MANAGED_ SERVER_NAME	The name of the Oracle Identity Manager managed server. If clustered, any of the managed servers can be specified.
COOKIE_DOMAIN	Web domain on which the OIM application resides. Specify the domain in the format .cc.example.com.
COOKIE_EXPIRY_ INTERVAL	Cookie expiration period. Set to -1.
OAM_TRANSFER_MODE	The security model in which the Access Servers function. Choices are OPEN or SIMPLE.
WEBGATE_TYPE	The type of WebGate agent you want to create. Set to `javaWebgate` if using a domain agent; set it to `ohsWebgate10g` if using a 10g WebGate.
SSO_ENABLED_FLAG	Flag to determine if SSO should be enabled. Set to `true` or `false`.
IDSTORE_PORT	The port number for the identity store (corresponding to the IDSTORE_DIRECTORYTYPE).
IDSTORE_HOST	The hostname of the identity store (corresponding to the IDSTORE_DIRECTORYTYPE).
IDSTORE_ DIRECTORYTYPE	The type of directory for which the authenticator must be created. `OID` for Oracle Internet Directory; `OVD` for all other directories.
IDSTORE_ADMIN_USER	User with admin privileges. Note that the entry must contain the complete LDAP DN of the user.
IDSTORE_ USERSEARCHBASE	The location in the directory where users are stored.

Table 3–1 (Cont.) Properties for configOIM Command

Property	Definition
IDSTORE_ GROUPSEARCHBASE	The location in the directory where groups are stored
MDS_DB_URL	The URL for the MDS database.
MDS_DB_SCHEMA_ USERNAME	The schema name for the MDS database.
WLSHOST	The WebLogic server hostname.
WLSPORT	The WebLogic server port number.
WLSADMIN	The WebLogic server administrator.
DOMAIN_NAME	The Oracle Identity Manager domain name.
DOMAIN_LOCATION	The Oracle Identity Manager domain location.

3.7.3.3 Updated Example for Integrating OIF/SP

In Section 4.3 Integrate Oracle Identity Federation in SP Mode, under sub-section 4.3.2 Delegate Authentication to Oracle Identity Federation, Step 7c contains an incorrect example of how to update the `OIFDAP` partner block in the `oam-config.xml` configuration file. The correct example should be:

```
registerOIFDAPPartner(keystoreLocation="/scratch/keystore",
logoutURL="http(s)://oifhost:oifport/fed/user/splooam11g?doneURL=
http(s)://oamhost:oamport/oam/server/pages/logout.jsp", rolloverTime="500")
```

Note that `oifhost` and `oifport` refer to the Oracle Identity Federation server host and port respectively; and `oamhost` and `oamport` refer to the Oracle Access Manager server host and port respectively.

4

Oracle Entitlements Server

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

4.1 General Issues and Workarounds

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

4.1.1 Using Backslash on Oracle Internet Directory Policy Store

When a backslash (`\`) is used in a policy object name and the backslash is followed by either a pound sign (`#`) or two hex characters (`[a-fA-f_0-9][a-fA-f_0-9]`), searches for the object may not work as expected. The issue has been observed when one of either a Resource Type name or a Resource name and action association has such a value causing the query of permission sets by Resource Type, Resource name or action to fail.

WORKAROUND:

Avoid using these values in policy object names.

4.1.2 Performance Tuning the Oracle Database Policy Store

The Oracle dbms_stats package can be used to improve data migration performance on an Oracle database policy store. The exact SQL command to be executed is:

```
*EXEC DBMS_STATS.gather_schema_stats
  ('DEV_OPSS',DBMS_STATS.AUTO_SAMPLE_SIZE,no_invalidate=>FALSE);*
```

where DEV_OPSS is the schema owner being used for the database policy store. You can use the other two parameters as illustrated.

WORKAROUND:

You can run this DBMS_STATS call periodically using either of the options below:

- Use DBMS_JOB.

  1. Copy and paste the following code to a SQL script.

     In this example, the job will be executed every 10 minutes.

     ```
     variable jobno number;
     BEGIN
     DBMS_JOB.submit
     (job => :jobno,
     what =>
     'DBMS_STATS.gather_schema_stats(''DEV_OPSS'',DBMS_STATS.AUTO_SAMPLE_SIZE,
     no_invalidate=>FALSE);',
     interval => 'SYSDATE+(10/24/60)');
     COMMIT;
     END;
     /
     #end of sql script
     ```

  2. Login to sqlplus as the schema owner; for example, 'DEV_OPSS' not sys_user.

  3. Run the SQL script.

     To find the job ID from the script you ran, execute the following:

     ```
     sqlplus '/as sysdba'
     SELECT job FROM dba_jobs WHERE schema_user = 'DEV_OPSS' AND what =
     'DBMS_STATS.gather_schema_stats(''DEV_OPSS'',DBMS_STATS.AUTO_SAMPLE_SIZE,
     no_invalidate=>FALSE);';
     ```

     To remove the job, login to sqlplus as the schema owner (for example, 'DEV_OPSS' not sys_user) and run the following SQL command:

     ```
     EXEC DBMS_JOB.remove(27);
     ```

- Use cron job or shell script to execute the SQL command.

  ```
  # run dbms_stats periodically
  ./runopssstats.sh
  # runopssstats.sh content is below:
  # In this example, we will execute the command in every 10 minutes
  #!/bin/sh

  i=1
  while [ $i -le 1000 ]
  do
  echo $i
  sqlplus dev_opss/welcome1@inst1 @opssstats.sql
  sleep 600
  ```

```
i=`expr $i + 1`
done
# end of sh

# opssstats.sql
EXEC DBMS_STATS.gather_schema_stats('DEV_OPSS',
  DBMS_STATS.AUTO_SAMPLE_SIZE,no_invalidate=>FALSE);
QUIT;
# end of sql
```

4.1.3 Action Bar Disappears When Using Internet Explorer 7

If you are using Internet Explorer 7 and select a role or user from an Administrator Role under System Configuration -> System Administrators, the action bar disappears thus, External Role Mappings and External User Mappings can not be deleted.

WORKAROUND:

This issue is specific to Internet Explorer 7. Use Firefox 3.

4.1.4 Re-created Application May Not Be Distributed in Controlled Mode

In some cases, when the PDP Service is running in controlled mode, if one Application object is deleted from the policy store and re-created using the same name, the change may not be distributed to the PDP Service. This is because the Application in the local cache has a higher version than the one in the policy store.

WORKAROUND:

Remove the local cache files for the PDP service and restart the PDP Service instance. The `oracle.security.jps.runtime.pd.client.localpolicy.work_folder` configuration parameter defines the path to the cache. The default value is `<SM_INSTANCE>/config/work/`.

4.1.5 Enterprise Manager Doesn't Pick Up Newly Added Audit Events

`component_events.xml` is the audit event definition file used by configuration tools (like Enterprise Manager and WebLogic Scripting Tool) and by the audit runtime and database loader. You need to modify the `component_events.xml` file to insure that Enterprise Manager picks up all newly added events in the Low/Medium list.

WORKAROUND:

1. Log out of Enterprise Manager.
2. Open the `component_events.xml` file.

   This file is located in the *$IDM_OPSS_ORACLE_HOME*`/modules/oracle.iau_11.1.1/components/JPS/` directory.
3. Search for `<FilterPresetDefinition name="Low">`.
4. In the event list, change *purgeDistributionStatus* to *PurgeDistributionStatus*.

   Note the capitalization.
5. Search for `<FilterPresetDefinition name="Medium">`.
6. In the event list, change *purgeDistributionStatus* to *PurgeDistributionStatus*.

   Note the capitalization.

7. Save the file and close it.
8. Start Enterprise Manager.

4.1.6 Attributes Passed to Authorization Request Are Treated as Case Sensitive

When using the PEP API names of passed attributes, they must be in the same case as those mentioned in the policies.

4.1.7 Audit Schema Definitions are Incomplete

The `IAUOES` audit schema is not synchronized with Oracle Entitlements Server event definitions, so it does not contain the necessary columns for this component. Consequently, data cannot be stored in the appropriate columns and audit reports cannot be run against Oracle Entitlements Server data.

WORKAROUND - Option 1

Use this option if RCU has not yet been run. The steps are:

1. Locate JPS.sql at this location:

   `$RCU_HOME/rcu/integration/iauoes/scripts/JPS.sql`

   Modify the file permission, making the file writable.

2. Copy over the file:

   `$IDM_OPSS_ORACLE_HOME/modules/oracle.iau_11.1.1/sql/scripts/JPS.sql`

   to:

   `$RCU_HOME/rcu/integration/iauoes/scripts/JPS.sql`

3. Run RCU to create the `IAUOES` schema.

WORKAROUND - Option 2

Use this option if RCU has already been run. The steps are:

1. Copy over the file:

   `$IDM_OPSS_ORACLE_HOME/modules/oracle.iau_11.1.1/sql/scripts/JPS.sql`

   to the directory from which you run `sqlplus`.

2. Connect to `sqlplus` as `sysdba`.
3. Run the following commands at the SQL prompt:
   a. alter session set current_schema=*audit_schema_user*
   b. drop table JPS;
   c. @@JPS.sql *audit_schema_user audit_schema_user*_Append *audit_schema_user_*Viewer;

4.1.8 Java Security Module on IPv6 Client Not Supported on Windows

Because of an issue with the JDK 1.6, the Java Security Module is not supported when using a Windows IPv6 client. We are working with the JDK development team for a resolution.

4.1.9 WebLogic Security Module Policy Distribution Configuration Issue on Windows IPv6 Hosts

The Policy Distribution URL may not be correctly generated on some Windows IPv6 hosts. Specifically, in `jps-config.xml` you might see the following line:

```
@ <property value="https://127.0.0.1:8002/pd-client"
name="oracle.security.jps.runtime.pd.client.DistributionServiceURL"/>
```

WORKAROUND:

Edit `jps-config.xml` (located in <*domain_home*>`/config/oeswlssmconfig/`) so it contains the correct policy distribution client URL. In the following example, <*WLS-SM-client-host*> is the hostname on which the WebLogic Server Security Module is running and <*Pd-client-port*> is the port on which the client is listening for policy distribution.

```
@ <property value="https://<WLS-SM-client-host>:<Pd-client-port>/pd-client"
name="oracle.security.jps.runtime.pd.client.DistributionServiceURL"/>
```

4.1.10 Validating Attribute Names in Custom Functions

When using custom function implementations, if the attribute name is invalid, the result of the authorization request could be wrong. Thus, attribute names must be validated before retrieving their values.

WORKAROUND:

Use the following code in custom function implementations to validate attribute names.

```
boolean isValidAttributeName(String name) {
    if (name == null) return false;
    return name.matches("[A-Za-z_][A-Za-z0-9_]*");
}
```

4.2 Configuration Issues and Workarounds

There are no configuration issues at this time.

4.3 Documentation Errata

There are no documentation errata at this time.

5 Oracle Identity Federation

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

- Section 5.1, "General Issues and Workarounds"
- Section 5.2, "Configuration Issues and Workarounds"
- Section 5.3, "Documentation Errata"

5.1 General Issues and Workarounds

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

- Section 5.1.1, "Database Table for Authentication Engine must be in Base64 Format"
- Section 5.1.2, "Considerations for Oracle Identity Federation HA in SSL mode"
- Section 5.1.3, "Database Column Too Short error for IDPPROVIDEDNAMEIDVALUE"

5.1.1 Database Table for Authentication Engine must be in Base64 Format

When using a database table as the authentication engine, and the password is stored hashed as either MD5 or SHA, it must be in base64 format.

The hashed password can be either in the base64-encoded format or with a prefix of {SHA} or {MD5}. For example:

```
{SHA}qUqP5cyxm6YcTAhz05Hph5gvu9M=
```

5.1.2 Considerations for Oracle Identity Federation HA in SSL mode

In a high availability environment with two (or more) Oracle Identity Federation servers mirroring one another and a load balancer at the front-end, there are two ways to set up SSL:

- Configure SSL on the load balancer, so that the SSL connection is between the user and the load balancer. In that case, the keystore/certificate used by the load balancer has a CN referencing the address of the load balancer.

  The communication between the load balancer and the WLS/Oracle Identity Federation can be clear or SSL (and in the latter case, Oracle WebLogic Server can use any keystore/certificates, as long as these are trusted by the load balancer).

- SSL is configured on the Oracle Identity Federation servers, so that the SSL connection is between the user and the Oracle Identity Federation server. In this case, the CN of the keystore/certificate from the Oracle WebLogic Server/Oracle Identity Federation installation needs to reference the address of the load balancer, as the user will connect using the hostname of the load balancer, and the Certificate CN needs to match the load balancer's address.

  In short, the keystore/certificate of the SSL endpoint connected to the user (load balancer or Oracle WebLogic Server/Oracle Identity Federation) needs to have its CN set to the hostname of the load balancer, since it is the address that the user will use to connect to Oracle Identity Federation.

5.1.3 Database Column Too Short error for IDPPROVIDEDNAMEIDVALUE

Problem

When Oracle Identity Federation is configured to use a database store for session and message data store, the following error is seen if data for `IDPPROVIDEDNAMEID` is over 200 characters long:

```
 ORA-12899: value too large for column
"WDO_OIF"."ORAFEDTMPPROVIDERFED"."IDPPROVIDEDNAMEIDVALUE" (actual: 240,
maximum: 200)\n]
```

Workaround

Alter table ORAFEDTMPPROVIDERFED to increase the column size for "idpProvidedNameIDValue" to 240.

5.2 Configuration Issues and Workarounds

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

5.2.1 WLST Environment Setup when SOA and OIF are in Same Domain

If your site contains Oracle SOA Suite and Oracle Identity Federation in the same domain, the `WLST` setup instructions in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation* are insufficient for `WLST` to correctly execute Oracle Identity Federation commands.

This can happen if you install an IdM domain, then extend it with an Oracle SOA install; the SOA installer changes the `ORACLE_HOME` environment variable. This breaks the Oracle Identity Federation `WLST` environment, as it relies on the IdM value for `ORACLE_HOME`.

Take these steps to enable the use of `WLST` commands:

1. Execute the instructions described in Section 9.1.1, Setting up the WLST Environment, in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.
2. Copy `OIF-ORACLE_HOME/fed/script/*.py` to `WL_HOME/common/wlst`.
3. Append the `CLASSPATH` environment variable with `OIF-ORACLE_HOME/fed/scripts`.

5.2.2 Oracle Virtual Directory Requires LSA Adapter

To use Oracle Virtual Directory as an Oracle Identity Federation user store or an authentication engine, you must configure a Local Storage Adapter, and the context root must be created as required at installation or post-install configuration time.

For details about this task, see the chapter Creating and Configuring Oracle Virtual Directory Adapters in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

5.2.3 Settings for Remote WS-Fed SP Must be Changed Dynamically

On the Edit Federations page, the Oracle Identity Federation (OIF) settings for remote WS-Fed service provider contain a property called **SSO Token Type**; you can choose to either inherit the value from the IdP Common Settings page or override it here. The number of properties shown in 'OIF Settings' depends on the value of **SSO Token Type**.

If you choose to override **SSO Token Type** with a different value (for example, by changing from SAML2.0 to SAML1.1), the number of properties shown in 'OIF Settings' does not change until you click the **Apply** button.

Also, if you have overridden the value for **Default NameID Format** to 'Persistent Identifier' or 'Transient/One-Time Identifier', then changed the **SSO Token Type** value from 'SAML2.0' to 'SAML1.1' or 'SAML1.0', you will notice that the value for **Default NameID Format** is now blank. To proceed, you must reset this property to a valid value from the list.

5.2.4 Required Property when Creating a WS-Fed Trusted Service Provider

When you create a WS-Fed Trusted Service Provider, you must set the value for the 'Use Microsoft Web Browser Federated Sign-On' property with these steps:

1. In Fusion Middleware Control, navigate to **Federations**, then **Edit Federations**.
2. Choose the newly create WS-Fed Trusted Service Provider and click **Edit**.
3. In the 'Trusted Provider Settings' section, set the value for Use Microsoft Web Browser Federated Sign-On by checking or unchecking the check-box.
4. Click **Apply**.

5.2.5 Federated Identities Table not Refreshed After Record Deletion

When the federation store is XML-based, a record continues to be displayed in the federated identities table after it is deleted.

The following scenario illustrates the issue:

1. The federation data store is XML.
2. Perform federated SSO, using "map user via federated identity".
3. In Fusion Middleware Control, locate the Oracle Identity Federation instance, and navigate to **Administration**, then **Identities**, then **Federated Identities**.
4. Click on the created federation record and delete it.

After deletion, the federated record is still in the table. Further attempts at deleting the record result in an error.

The workaround is to manually refresh the table by clicking **Search**.

5.2.6 Default Authentication Scheme is not Saved

Problem

This problem is seen when you configure Oracle Access Manager in Fusion Middleware Control as a Service Provider Integration Module. It is not possible to set a default authentication scheme since the default is set to a certain scheme (say `OIF-password-protected`) but the radio button is disabled.

Solution

Take these steps to set the preferred default authentication scheme:

1. Check the **Create** check-box for the scheme that is currently set as the default but disabled.
2. Check the **Create** check-box(es) for the authentication scheme(s) that you would like to create.
3. Click the radio button of the scheme that you wish to set as the default.
4. Uncheck the **Create** check-box of the scheme in Step 1 only if you do not want to create the scheme.
5. Provide all the required properties in the page.
6. Click the **Configure Oracle Access Manager** button to apply the changes.

The default authentication scheme is now set to the one that you selected.

Note: In addition, when trying to remove any authentication scheme, ensure that you do not remove the default scheme; if you must remove the scheme, change the default to another authentication scheme before you remove the scheme.

5.2.7 Configuring 10g to Work with 11g Oracle Identity Federation using Artifact Profile

In the SAML 1.x protocol, for a 10g Oracle Identity Federation server to work with an 11g Oracle Identity Federation server using the Artifact profile, you need to set up either basic authentication or client cert authentication between the two servers.

For instructions, see:

- Section 6.9 Protecting the SOAP Endpoint, in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*, 11g Release 1 (11.1.1)
- Section 6.5.13.2 When Oracle Identity Federation is an SP, in the *Oracle Identity Federation Administrator's Guide*, 10g (10.1.4.0.1)

5.2.8 Regenerating OAM 11g Key Requires Oracle Identity Federation Upgrade Script

In Oracle Enterprise Manager Fusion Middleware Control, when you configure the SP Integration Module for Oracle Access Manager 11*g*, you can regenerate the secret key by clicking the **Regenerate** button (Service Provider Integration Modules page, Oracle Access Manager 11g tab).

In an upgraded 11.1.1.7.0 environment, it is necessary to execute the Oracle Identity Federation upgrade script *before* you regenerate the OAM 11*g* secret key from this page. For details about how to run the script, see the *Oracle Fusion Middleware Patching Guide*.

5.3 Documentation Errata

This section contains documentation errata for the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*. There are no errata at this time.

Note: For documentation errata and other release notes relating to the integration of Oracle Identity Federation with Oracle Access Manager 11g , see the chapter for "Oracle Access Manager."

---

6 Oracle Identity Manager

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

6.1 Patch Requirements

This section describes patch requirements for Oracle Identity Manager 11*g* Release 1 (11.1.1). It includes the following sections:

6.1.1 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/`

6.1.2 Patch Requirements for Oracle Database 11g (11.1.0.7)

Table 6–1 lists patches required for Oracle Identity Manager 11*g* Release 1 (11.1.1) configurations that use Oracle Database 11*g* (11.1.0.7). Before you configure Oracle Identity Manager 11*g*, be sure to apply the patches to your Oracle Database 11*g* (11.1.0.7) database.

Table 6–1 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

Table 6–1 (Cont.) Required Patches for Oracle Database 11g (11.1.0.7)

Platform	Patch Number and Description on My Oracle Support
	7000281: DIFFERENCE IN FORALL STATEMENT BEHAVIOR IN 11G
	8327137: WRONG RESULTS WITH INLINE VIEW AND AGGREGATION FUNCTION
	8617824: MERGE LABEL REQUEST ON TOP OF 11.1.0.7 FOR BUGS 7628358 7598314
Windows 32 bit	8689191: ORACLE 11G 11.1.0.7 PATCH 16 BUG FOR WINDOWS 32 BIT
Windows 64 bit	8689199: ORACLE 11G 11.1.0.7 PATCH 16 BUG FOR WINDOWS (64-BIT AMD64 AND INTEL EM64T)

Note: The patches listed for UNIX/Linux in Table 6–1 are also available by the same names for Solaris SPARC 64 bit.

6.1.3 Patch Requirements for Oracle Database 11g (11.2.0.2.0)

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

Table 6–2 lists the patches required for Oracle Identity Manager 11*g* Release 1 (11.1.1) 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 6–2 Required Patches for Oracle Database 11g (11.2.0.2.0)

Platform	Patch Number and Description on My Oracle Support
Linux x86 (32-bit)	RDBMS Interim Patch#9776940.
Linux x86 (64-bit)	
Oracle Solaris on SPARC (64-bit)	
Oracle Solaris on x86-64 (64-bit)	
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].

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.

Note:

- Apply this patch in ONLINE mode. Refer to the readme.txt file bundled with the patch for the steps to be followed.
- In some environments, the RDBMS Interim Patch has been unable to resolve the issue, but the published workaround works. Refer to the metalink note "Wrong Results on 11.2.0.2 with Function-Based Index and OR Expansion due to fix for Bug:8352378 [Metalink Note ID 1264550.1]" for the workaround. This note can be followed to set the parameters accordingly with the only exception that they need to be altered at the Database Instance level by using ALTER SYSTEM SET <param>=<value> scope=<memory> or <both>.

6.1.4 Patch Requirements for Segregation of Duties (SoD)

Table 6–3 lists patches that resolve known issues with Segregation of Duties (SoD) functionality:

Table 6–3 SoD Patches

Patch Number / ID	Description and Purpose
Patch number 9819201 on My Oracle Support	Apply this patch on the SOA Server to resolve the known issue described in "SoD Check During Request Provisioning Fails While Using SAML Token Client Policy When Default SoD Composite is Used". The description of this patch on My Oracle Support is "ERROR WHILE USING SAML TOKEN CLIENT POLICY FOR CALLBACK."
Patch ID 3M68 using the Oracle Smart Update utility. Requires passcode: 6LUNDUC7.	Using the Oracle Smart Update utility, apply this patch on the Oracle WebLogic Server to resolve the known issue described in "SoD Check Fails While Using Client-Side Policy in Callback Invocation During Request Provisioning".

Note: The SoD patches are required to resolve the known issues in Oracle Identity Manager 11*g* Release 1 (11.1.1.3), but these patches are not required in 11*g* Release 1 (11.1.1.5).

6.1.5 Patch Upgrade Requirement

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

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

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

See "Obtaining Patches From My Oracle Support (Formerly OracleMetaLink)" on page 6-1 for information about downloading OPatch from My Oracle Support.

6.2 General Issues and Workarounds

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

6.2.1 Do Not Use Platform Archival Utility

Currently, the Platform Archival Utility is not supported and should not be used.

To work around this issue, use the predefined scheduled task named **Orchestration Process Cleanup Task** to delete all completed orchestration processes and related data.

6.2.2 SPML-DSML Service is Unsupported

Oracle Identity Manager's SPML-DSML Service is currently unsupported in 11*g* Release 1 (11.1.1). However, you can manually deploy the spml-dsml.ear archive file for Microsoft Active Directory password synchronization.

6.2.3 Resource Object Names Longer than 100 Characters Cause Import Failure

If a resource object name is more than 100 characters, an error occurs in the database and the resource object is not imported. To work around this issue, change the resource object's name in the XML file so the name is less than 100 characters.

6.2.4 Status of Users Created Through the Create and Modify User APIs

You cannot create users in Disabled State. Users are always created in Active State.

The Create and Modify User APIs do not honor the Users.Disable User attribute value. If you pass a value to the Users.Disable User attribute when calling the Create API, Oracle Identity Manager ignores this value and the USR table is always populated with a value of 0, which indicates the user's state is Active.

Use the Disable API to disable a user.

6.2.5 Status of Locked Users in Oracle Access Manager Integrations

When Oracle Access Manager locks a user account in an Oracle Identity Manager-Oracle Access Manager integration, it may take approximately five minutes, or the amount of time defined by the incremental reconciliation scheduled interval, for the status of the locked account to be reconciled and appear in Oracle Identity Manager. However, if a user account is locked or unlocked in Oracle Identity Manager, the status appears immediately.

6.2.6 Generating an Audit Snapshot after Bulk-Loading Users or Accounts

The GenerateSnapshot.[sh | bat] option does not work correctly when invoked from the Bulk Load utility. To work around this issue and generate a snapshot of the initial audit after bulk loading users or accounts, you must run GenerateSnapshot.[sh | bat] from the $*OIM_HOME*/bin/ directory.

6.2.7 Browser Timezone Not Displayed

Due to an ADF limitation, the browser timezone is currently not accessible to Oracle Identity Manager. Oracle Identity Manager bases the timezone information in all date values on the server's timezone. Consequently, end users will see timezone information in the date values, but the timezone value will display the server's timezone.

6.2.8 Date Format Change in the SoD Timestamp Field Not Supported

The date-time value that end users see in the Segregation of Duties (SoD) Check Timestamp field on the SoD Check page will always display as "YYYY-MM-DD hh:mm:ss" and this format cannot be localized.

To work around this localization issue, perform the following steps:

1. Open the "Oracle_eBusiness_User_Management_9.1.0.1.0/xml/Oracle-eBusinessSuite-TCA-Main-ConnectorConfig.xml" file.
2. In the EBS Connector import xml, locate the SoDCheckTimeStamp field for the Process Form. Change <SDC_FIELD_TYPE> to 'DateFieldDlg' and change <SDC_VARIANT_TYPE> to 'Date' as shown in the following example:

```
<FormField name = "UD_EBST_USR_SODCHECKTIMESTAMP">
             <SDC_UPDATE>!Do not change this field!</SDC_UPDATE>
             <SDC_LABEL>SoDCheckTimestamp</SDC_LABEL>
             <SDC_VERSION>1</SDC_VERSION>
             <SDC_ORDER>23</SDC_ORDER>
             <SDC_FIELD_TYPE>DateFieldDlg</SDC_FIELD_TYPE>
             <SDC_DEFAULT>0</SDC_DEFAULT>
             <SDC_ENCRYPTED>0</SDC_ENCRYPTED>
             <!--SDC_SQL_LENGTH>50</SDC_SQL_LENGTH-->
             <SDC_VARIANT_TYPE>Date</SDC_VARIANT_TYPE>
          </FormField>
```

3. Import the Connector.
4. Enable SoD Check.
5. Provision the EBS Resource with entitlements to trigger an SoD Check.
6. Check the SoDCheckTimeStamp field in Process Form to confirm it is localized like the other date fields in the form.

6.2.9 Bulk Loading CSV Files with UTF-8 BOM Encoding Not Supported

Bulk loading a CSV file for which UTF-8 BOM (byte order mark) encoding is specified causes an error. However, bulk-loading UTF-8 encoded CSV files works as expected if you specify "no BOM" encoding.

To work around this issue,

- If you want to load non-ASCII data, you must change your CSV file encoding to "UTF-8 no BOM" before loading the CSV file.
- If your data is stored in CSV files with "UTF-8 BOM" encoding, you must change them to "UTF-8 no BOM" encoding before running the bulkload script.

6.2.10 Date Type Attributes are Not Supported for the Default Scheduler Job, "Job History Archival"

The default Scheduler job, "Job History Archival," does not support date type attributes.

The "Archival Date" attribute parameter in "Job History Archival" only accepts string patterns such as "ddMMyyyy" and "MMM DD, yyyy."

When you run a Scheduler job, the code checks the date format. If you enter the wrong format, an error similar to the following example, displays in the execution status list and in the log console:

<IAM-1020063> <Incorrect format of Archival Date parameter. Archival Date is expected in DDMMYYYY or UI Date format.>

The job cannot run successfully until you input the correct Archival Date information.

6.2.11 Low File Limits Prevent Adapters from Compiling

On machines where the file limits are set too low, trying to create and compile an entity adapter causes a "Too many open files" error and the adapter will not compile.

To work around this issue, change the file limits on your machine to the following (located in /etc/security/limits.conf) and then restart the machine:

- `softnofile 4096`
- `hardnofile 4096`

6.2.12 Reconciliation Engine Requires Matching Rules

Currently, Oracle Identity Manager's Reconciliation Engine in 11*g* Release 1 (11.1.1) requires you to define a matching rule to identify the users for every connector in reconciliation. Errors will occur during reconciliation if you do not define a matching rule to identify users.

6.2.13 SPML Requests Do Not Report When Any Date is Specified in Wrong Format

When any date, such as activeStartDate, hireDate, and so on, is specified in an incorrect format, the Web server does not pass those values to the SPML layer. Only valid dates are parsed and made available to SPML. Consequently, when any SPML request that contains an invalid date format, the invalid date format from the request is ignored and is not available for that operation. For example, if you specify the HireDate month as "8" instead of "08," the HireDate will not be populated after the Create request is completed and no error message is displayed.

The supported date format is:

```
yyyy-MM-dd hh:mm:ss.fffffffff
```

No other date format is supported.

6.2.14 Logs Populated with SoD Exceptions When the SoD Message Fails and Gets Stuck in the Queue

SoD functionality uses JMS-based processing. Oracle Identity Manager submits a message to the oimSODQueue for each SoD request. If for some reason an SoD message always results in an error, Oracle Identity Manager never processes the next

message in the oimSODQueue. Oracle Identity Manager always picks the same error message for processing until you delete that message from the oimSODQueue.

To work around this issue, use the following steps to edit the queue properties and to delete the SoD message in oimSODQueue:

1. Log on to the WebLogic Admin Console at http://<hostname>:<port>/console
2. From the Console, select Services, Messaging, JMS Modules.
3. Click **OIMJMSModule**. All queues will be displayed.
4. Click oimSODQueue.
5. Select the Configurations, Delivery Failure tabs.
6. Change the retry count so that the message can only be submitted a specified number of times.
7. Change the default Redelivery Limit value from -1 (which means infinite) to a specific value. For example, if you specify 1, the message will be submitted only once.
8. To review and delete the SoD error message, go to the Monitoring tab, select the message, and delete it.

6.2.15 A Backslash (\) Cannot Be Used in a weblogic.properties File

If you are using the WeblogicImportMetadata.cmd utility to import data to MDS, then do not use a backslash (\) character in a path in the weblogic.properties file, or an exception will occur.

To work around this issue, you must use a double backslash (\\) or a forward slash (/) on Microsoft Windows. For example, change metadata_from_loc=C:\metadata\file to metadata_from_loc=C:\\metadata\\file in the weblogic.properties file.

6.2.16 Underscore Character Cannot Be Used When Searching for Resources

When you are searching for a resource object, do not use an underscore character (_) in the resource name. The search feature ignores the underscore and consequently does not return the expected results.

6.2.17 Assign to Administrator Action Rule is Not Supported by Reconciliation

Reconciliation does not support the Assign to Administrator Action rule.

To work around this issue, change the Assign to Administrator to `None` in the connector XML before importing the connector. However, after changing the value to None, you cannot revert to Assign to Administrator.

6.2.18 Some Buttons on Attestation Screens Do Not Work in Mozilla Firefox

If you are creating attestations in a Mozilla Firefox Web browser and you click certain buttons, nothing happens.

To work around this issue, click the **Refresh** button to refresh the page.

6.2.19 The maxloginattempts System Property Causes Autologin to Fail When User Tries to Unlock

WLS Security Realm has a default lock-out policy that locks out users for some time after several unsuccessful login attempts. This policy can interfere with the locking and unlocking functionality of Oracle Identity Manager.

To prevent the WLS Security Realm lock-out policy from affecting the lock/unlock functionality of Oracle Identity Manager, you must set the 'Lockout Threshold' value in the WLS 'User Lockout Policy' to at least 5 more than the value in Oracle Identity Manager. For example, if the value in Oracle Identity Manager is set to 10, you must set the WLS 'Lockout Threshold' value to 15.

To change the default values for the 'User lockout Policy,' perform the following steps:

1. Open the WebLogic Server Administrative Console.
2. Select **Security Realms**, *REALM_NAME*.
3. Select the **User Lockout** tab.
4. If configuration editing is not enabled, then click the **Lock and Edit** button to enable configuration editing.
5. Change the value of lockout threshold to the required value.
6. Click **Save** to save the changes.
7. Click **Activate** to activate your changes.
8. Restart all the servers in the domain.

6.2.20 "<User not found>" Error Message Appears in AdminServer Console While Setting-Up an Oracle Identity Manager-Oracle Access Manager Integration

When you set up Oracle Identity Manager-Oracle Access Manager Integration with a JAVA agent and log into the Admin Server Console, a "<User not found>" error message is displayed. This message displays even when the login is successful.

6.2.21 Do Not Use Single Quote Character in Reconciliation Matching Rule

If the single quote character (') is used in reconciliation data (for example, 'B'1USER1'), then target reconciliation will fail with an exception.

6.2.22 Do Not Use Special Characters When Reconciling Roles from LDAP

Due to a limitation in the Oracle SOA Infrastructure, do not use special characters such as commas (,) in role names, group names, or container descriptions when reconciling roles from LDAP. Oracle Identity Manager's internal code uses special characters as delimiters. For example, Oracle Identity Manager uses commas (,) as approver delimiters and the SOA HWF-level global configuration uses commas as assignee delimiters.

6.2.23 SoD Check During Request Provisioning Fails While Using SAML Token Client Policy When Default SoD Composite is Used

SoD check fails and the following error is displayed on the SOA console when SoD check is performed during request provisioning only when the Default SoD Check composite is used:

```
SEVERE: FabricProviderServlet.handleException Error during retrieval of test page
or composite resourcejavax.servlet.ServletException:
java.lang.NullPointerException
```

This happens when Callback is made from Oracle Identity Manager to SOA with the SoDCheck Results.

To resolve this issue, apply patch 9819201 on the SOA server. You can obtain patch 9819201 from My Oracle Support. The description of this patch on My Oracle Support is "ERROR WHILE USING SAML TOKEN CLIENT POLICY FOR CALLBACK."

For more information, refer to:

- Obtaining Patches From My Oracle Support (Formerly OracleMetaLink).
- Patch Requirements for Segregation of Duties (SoD)

6.2.24 SoD Check Fails While Using Client-Side Policy in Callback Invocation During Request Provisioning

SoD check fails and following error is displayed on the Oracle Identity Manager Administrative and User Console when SoD check is performed during request provisioning only when the Default SoD Check composite is used:

```
<Error> <oracle.wsm.resources.policymanager><WSM-02264> <"/base_domain/oim_
server1/oim/unknown/iam-ejb.jar/WEBSERVICECLIENTs/SoDCheckResultService/PORTs/Resu
ltPort" is not a recognized resource pattern.>
<Error> <oracle.iam.sod.impl> <IAM-4040002><Error getting Request Service :
java.lang.IllegalArgumentException: WSM-02264 "/base_domain/oim_
server1/oim/unknown/iam-ejb.jar/WEBSERVICECLIENTs/SoDCheckResultService/PORTs/Resu
ltPort" is not a recognized resource pattern.>
```

To resolve this issue, use the Oracle Smart Update utility to apply patch ID 3M68, which requires passcode of 6LUNDUC7, on Oracle WebLogic Server. For more information, refer to:

- The *Oracle Smart Update Installing Patches and Maintenance Packs* documentation.
- Patch Requirements for Segregation of Duties (SoD)

6.2.25 Error May Appear During Provisioning when Generic Technology Connector Framework Uses SPML

When using the generic technology connector framework uses SPML, during provisioning, the following error may appear:

```
<SPMLProvisioningFormatProvider.formatData :problem with Velocity Template Unable
to find resource 'com/thortech/xl/gc/impl/prov/SpmlRequest.vm'>
```

If the error occurs, it blocks provisioning by using the predefined SPML GTC provisioning format provider. Restarting the Oracle Identity Manager server prevents the error from appearing again.

6.2.26 Cannot Click Buttons in TransUI When Using Mozilla Firefox

When using the Mozilla Firefox browser, in certain situations, some buttons in the legacy user interface, also known as TransUI, cannot be clicked. This issue occurs intermittently and can be resolved by using Firefox's reload (refresh) function.

6.2.27 LDAP Handler May Cause Invalid Exception While Creating, Deleting, or Modifying a Role

If an LDAP handler causes an exception when you create, modify, or delete a role, an invalid error message, such as `System Error` or `Role does not exist`, may appear.

To work around this issue, look in the log files, which will display the correct error message.

6.2.28 Cannot Reset User Password Comprised of Non-ASCII Characters

If a user's password is comprised of non-ASCII characters, and that user tries to reset the password from either the My Profile or initial login screens in the Oracle Identity Manager Self Service interface, the reset will fail with the following error message:

```
Failed to change password during the validation of the old password
```

Note: This error does not occur with user passwords comprised of only ASCII characters.

To work around this issue, perform the following steps:

1. Set the JVM file encoding to UTF8, for example: `-Dfile.encoding=UTF-8`

   Note: On Windows systems, this may cause the console output to appear distorted, though output in the log files appear correctly.

2. Restart the Oracle WebLogic Server.

6.2.29 Benign Exception and Error Message May Appear While Patching Authorization Policies

When patches are applied to the Authorization Polices that are included with Oracle Identity manager and the JavaSE environment registers the Oracle JDBC driver, `java.security.AccessControlException` is reported and the following error message appears:

```
Error while registering Oracle JDBC Diagnosability MBean
```

You can ignore this benign exception, as the Authorization Policies are seeded successfully, despite the exception and error messages.

6.2.30 The DateTime Pick in the Trans UI Does Not Work Correctly in the Thai Locale

When locale is set to th_TH in Microsoft Windows Internet Explorer Web browser, the datetime in Oracle Identity Manager follows the Thai Buddhist calendar. In the Create Attestation page of the Administrative and User Console, when you select a date for start time, the year is displayed according to the Thai Buddhist calendar, for example,

2553. After you click **OK**, the equivalent year according to the Gregorian calendar, which is 2010, is displayed in the start time field. But when you click **Next** to continue creating the attestation, an error message is displayed stating that the start time of the process must not belong to the past.

To workaround this issue, perform any one of the following:

- Specify the datetime manually.
- Use Mozilla Firefox Web browser, which uses the Gregorian calendar.

6.2.31 User Without Access Policy Administrators Role Cannot View Data in Access Policy Reports

OIM user without the ACCESS POLICY ADMINISTRATORS role cannot view data in the following reports:

- Access Policy Details
- Access Policy List by Role

To workaround this issue:

1. Assign the ACCESS POLICY ADMINISTRATORS role to an OIM user.
2. Create a BI Publisher user with the same username in Step 1. Assign appropriated BI Publisher role to view reports.
3. Login as the BI Publisher user mentioned in step 2. View the Access Policy Details and Access Policy List by Role reports. All access policies are displayed.

6.2.32 Archival Utility Throws an Error for Empty Date

In case of empty date, archival utility throws an error message, but proceeds to archive data by mapping to the current date. Currently, no workaround exists for this issue.

6.2.33 TransUI Closes with Direct Provisioning of a Resource

TransUI closes while doing a direct provisioning if user defined field (UDF) is created with the default values. To work around this issue, you need to create a Lookup Code for the INTEGER/DOUBLE type UDF in the LKU/LKV table.

6.2.34 Scheduler Throws "ParameterValueTypeNotSupportedException" Instead of "RequiredParameterNotSetException"

On AIX platform, when a required parameter is missing during the creation of a scheduler job, instead of throwing "RequiredParameterNotSetException" with the error message "The value is not set for required parameters of a scheduled task.", it throws "ParameterValueTypeNotSupportedException" with the error message "Parameter value is not set properly". Currently, no workaround exists for this issue.

6.2.35 All New User Attributes Are Not Supported for Attestation in Oracle Identity Manager 11*g*

New user attributes are added in Oracle Identity Manager 11*g*. Not all of them are available for Attestation while defining user-scope. However, Attestation has been enhanced to include the following user attributes:

- USR_COUNTRY
- USR_LDAP_ORGANIZATION
- USR_LDAP_ORGANIZATION_UNIT
- USR_LDAP_GUID

Currently, no workaround exists for this issue.

6.2.36 LDAP GUID Mapping to Any Field of Trusted Resource Not Supported

Update fails in LDAP, if LDAP GUID is mapped to any field of trusted resource in LDAP-SYNC enabled installation. To work around this issue, Oracle does not recommend mapping for LDAP GUID field while creating reconciliation field mapping for a trusted resource.

6.2.37 User Details for Design Console Access Field Must Be Mapped to Correct Values When Reading Modify Request Results

When a Modify Request is raised, "End-User" and "End-User Administrator" values are displayed for the "Design Console Access" field. These values must be mapped to False/True while interpreting the user details.

6.2.38 Cannot Create a User Containing Asterisks if a Similar User Exists

If you try to create a user that contains an asterisk (*) after creating a user with a similar name, the attempt will fail. For example, if you create user test1test, followed by test*test, test*test will not be created.

It is recommended to not create users with asterisks in the User Login field.

6.2.39 Blank Status Column Displayed for Past Proxies

The Status field on the Post Proxies page is blank. However, active proxies are displayed correctly on Current Proxies page.

Currently, no workaround exists for this issue.

6.2.40 Mapping the Password Field in a Reconciliation Profile Prevents Users from Being Created

The Password field is available to be mapped with a reconciliation profile, but it should not be used. Attempting to map this field will generate a reconciliation event

that will not create users. (The event ends in "No Match Found State".) In addition, you will not be able to re-evaluate or manually link this event.

6.2.41 UID Displayed as User Login in User Search Results

Although you can select the UID attribute from the Search Results Table Configuration list on the Search Configuration page of the Advanced Administration, the search results table for advanced search for users displays the User Login field instead of the UID field.

6.2.42 Roles/Organizations Browse Trees Disappear

After you delete an organization, the Browse trees for organizations and roles might not be displayed.

To work around this issue, click the **Search Results** tab, then click the **Browse** tab. The roles and organizations browse trees display correctly.

6.2.43 Entitlement Selection Is Not Optional for Data Gathering

Entitlement (Child Table) selection during data gathering on the process form, for the "Depends On (Depended)" attribute is not optional. During data gathering, if dependent lookups are configured, then the user has to select the parent lookup value so that filtering happens on the child lookup and thus user gets a final list of entitlements to select . Currently, no workaround exists to directly filter the values based on the child lookup.

6.2.44 Oracle Identity Manager Server Throws Generic Exception While Deploying a Connector

Generic exceptions are shown in server logs every time deployment manager import happens or profile changes manually or profile changes via design console. This is because "WLSINTERNAL" is not an authorized user of Oracle Identity Manager. "WLSINTERNAL" is an internal user of WebLogic Server, and MDS uses it to invoke MDS listeners if there is a change in XMLs stored in MDS. Currently, no workaround exists for this issue.

6.2.45 Create User API Allows Any Value for the "Users.Password Never Expires", "Users.Password Cannot Change", and "Users.Password Must Change" Fields

Create User API allows the user to set any value between 0 and 9 instead of 0 or 1 for "Users.Password Never Expires", "Users.Password Cannot Change" and "Users.Password Must Change" fields. However, any value other than 0 is considered as TRUE and 0 is considered as FALSE, and the flag is set accordingly for the user being created. Currently, no workaround exists for this issue.

6.2.46 Incorrect Label in JGraph Screen for the GTC

The User Type label on the JGraph screen is displayed incorrectly as Design Console Access. To display User Type, add the line `Xellerate_Type=User Type` to the *OIM_HOME*/server/customResources/customResources.properties file.

6.2.47 Running the Workflow Registration Utility Generates an Error

When the workflow registration utility is run in a clustered deployment of Oracle Identity Manager, the following error is generated:

```
[java] oracle.iam.platform.utils.NoSuchServiceException:
java.lang.reflect.InvocationTargetException
```

Ignore the error message.

6.2.48 Native Performance Pack is Not Enabled On Solaris 64-bit JVM Install

For Oracle Identity Manager JVM install on a Solaris 64-bit computer, Oracle WebLogic log displays the following error:

```
Unable to load performance pack. Using Java I/O instead. Please ensure that a
native performance library is in:
```

To workaround this issue, perform the following to ensure that JDK picks up the 64-bit native performance:

1. In a text editor, open the *MIDDLEWARE_HOME*/wlserver_10.3/common/bin/commEnv.sh file.
2. Replace the following:

   ```
   SUN_ARCH_DATA_MODEL="32"
   ```

   With:

   ```
   SUN_ARCH_DATA_MODEL="64"
   ```

3. Save and close the commEnv.sh file.
4. Restart the application server.

6.2.49 Error in the Create Generic Technology Connector Wizard

If you enter incorrect credentials for the database on the Create Generic Technology Connector wizard, a system error window is displayed. You must close this window and run the wizard again.

6.2.50 DSML Profile for the SPML Web Service is Not Deployed With Oracle Identity Manager

The DSML profile for the SPML Web service is not deployed by default with Oracle Identity Manager 11*g* Release 1 (11.1.1). SPML-DSML binaries are bundled with the Oracle Identity Manager installer to support Microsoft Active Directory Password Synchronization. You must deploy the spml-dsml.ear file manually.

6.2.51 New Human Tasks Must Be Copied in SOA Composites

When you add a new human task to an existing SOA composite, you must ensure that all the copy operations for the attributes in the original human task are added to the

new human task. Otherwise, an error could be displayed on the View Task Details page.

6.2.52 Modify Provisioned Resource Request Does Not Support Service Account Flag

A regular account cannot be changed to a service account, and similarly, a service account cannot be changed to a regular account through a Modify Provisioned Resource request.

6.2.53 Erroneous "Query by Example" Icon in Identity Administration Console

In the Identity Administration console, when viewing role details from the Members tab, an erroneous icon with the "tooltip" (mouse-over text) of "Query By Example" appears. This "Query By Example" icon is non-functional and should be ignored.

6.2.54 The XL.ForcePasswordChangeAtFirstLogin System Property Is No Longer Used

The XL.ForcePasswordChangeAtFirstLogin system property is no longer used in Oracle Identity Manager 11*g* Release 1 (11.1.1.1). Therefore, forcing the user to change the password at first login cannot be configured. By default, the user must change the password:

- When the new user, other than self-registered users, is logging in to Oracle Identity Manager for the first time
- When the user is logging in to Oracle Identity Manager for the first time after the password has been reset

6.2.55 The tcExportOperationsIntf.findObjects(type,name) API Does Not Accept the Asterisk (*) Wilcard Character in Both Parameters

The tcExportOperationsIntf.findObjects(type,name) API accepts the asterisk (*) wildcard character only for the second parameter, which is name. For type, a category must be specified. For example, findObjects("Resource","*") is a valid call, but findObjects("*","*") is not valid.

6.2.56 Disabled Links on the Access Policy Summary Page Opened in Mozilla FireFox

In the Verify Information for this Access Policy page of the Create/Modify Access Policy wizards opened in Mozilla Firefox Web browser, you click **Change** for resource to be provisioned by the access policy, and then click **Edit** to edit the process form data for the resources to be provisioned. If you click the Close button on the Edit form, then the change links for any one of the access policy information sections, such as resources to be provisioned by the access policy, resources to be denied by the access policy, or roles for the access policy, do not work.

To workaround this issue, click **Refresh**. All the links in the Verify Information for this Access Policy page are enabled.

6.2.57 Benign Error is Generated on Editing the IT Resource Form in Advanced Administration

When you click the Edit link on the IT Resource form in the Advanced Administration, the following error message is logged:

```
<Error> <XELLERATE.APIS> <BEA-000000>
<Class/Method: tcFormDefinitionOperationsBean/getFormFieldPropertyValue encounter
```

```
some problems: Property 'Column Names' has not defined for the form field '-82'>
```

The error message is benign and can be ignored because there is no loss of functionality.

6.2.58 User Account is Not Locked in iPlanet Directory Server After it is Locked in Oracle Identity Manager

After reaching the maximum login attempts, a user is locked in Oracle Identity Manager. But in iPlanet DS/ODSEE, the user is not locked. The orclAccountLocked feature is not supported because the backend iPlanet DS/ODSEE does not support account unlock by setting the Operational attribute. Account is unlocked only with a password reset. The nsaccountlock attribute is available for administrative lockout. The password policies do not use this attribute, but you can use this attribute to independently lock an account. If the password policy locks the account, then nsaccountlock locks the user even after the password policy lockout is gone.

6.2.59 Oracle Identity Manager Does Not Support Autologin With JavaAgent

In an Oracle Access Manager (OAM) integrated deployment of Oracle Identity Manager with JavaAgent, when a user created in Oracle Identity Manager tries to login to the Oracle Identity Manager Administrative and User Console for the first time, the user is forced to reset password and set challenge questions. After this, the user is not logged in to Oracle Identity Manager automatically, but is redirected to the OAM login page. This is because Oracle Identity Manager does not support autologin when JavaAgent is used.

6.2.60 Benign Error Logged on Opening Access Policies, Resources, or Attestation Processes

As a delegated administrator, when you open the page to display the details of an access policy, resource, or attestation process, the following error is logged:

```
Error> <org.apache.struts.tiles.taglib.InsertTag> <BEA-000000>
<Can't insert page '/gc/EmptyTiles.jsp' : Write failed: Broken pipe
java.net.SocketException: Write failed: Broken pipe
```

The error is benign and can be ignored because there is no loss of functionality.

6.2.61 User Locked in Oracle Identity Manager But Not in LDAP

In a LDAP-enabled deployment of Oracle Identity Manager in which the directory servers are Microsoft Active Directory (AD) or Oracle Internet Directory (OID), when a user is manually locked in Oracle Identity Manager by the administrator, the user is not locked in LDAP if a password policy is not configured in LDAP. The configurable password policy in LDAP can either be the default password policy that is applicable to all the LDAP users, or it can be a user-specific Password Setting Object (PSO).

6.2.62 Reconciliation Profile Must Not Be Regenerated Via Design Console for Xellerate Organization Resource Object

By default, the Xellerate Organization resource object does not have reconciliation to Oracle Identity Manager field mappings and any matching/action rule information. As a result, when reconciliation profile for Xellerate Organization resource object is updated via Design Console, it corrupts the existing reconciliation configuration for that resource object, and reconciliation fails with empty status.

To workaround this issue, do not generate the reconciliation profile/configuration via the Design Console. Instead, export the Xellerate Organization profile from Meta Data Store (MDS) and edit it manually, and import it back into Oracle Identity Manager. If the profile changes include modification of the reconciliation fields, then the corresponding changes must be made in the horizontal table schema and its entity definition as well.

6.2.63 Benign Error Logged on Clicking Administration After Upgrade

After upgrading Oracle Identity Manager from Release 9.1.0.1 to 11g Release 1 (11.1.1), on clicking the Administration link on the Administrative and User Console, the following error is logged:

```
<Error> <oracle.adfinternal.view.page.editor.utils.ReflectionUtility>
<WCS-16178> <Error instantiating class -
oracle.adfdtinternal.view.faces.portlet.PortletDefinitionDTFactory>
```

This error is benign and can be ignored because there is no loss of functionality.

6.2.64 Provisioning Fails Through Access Policy for Provisioned User

When a user is already provisioned and you try to assign a role to the user that triggers provisioning to the target domain, the provisioning is not started. However, if the user is not provisioned already and you assign a role to the user, then the provisioning occurs successfully.

To workaround this issue:

1. Open the connector-specific user form in the Design Console.
2. Create a new version of the connector, and select **Edit**.
3. Click the **Properties** tab, and then click **server (ITResourceLookupField)**. Click **Add Property**.
4. Add Required for the property and specify true. Click **Make Version Active**, and then click **Save**.
5. Login to Oracle Identity Manager Administrative and User Console.
6. Navigate to System Property. Search for the 'Allows access policy based provisioning of multiple instances of a resource' system property. Change the value of this property to TRUE.
7. Restart Oracle Identity Manager.

Try provisioning a provisioned user to provision through access policy of the same IT Resource Type, and the provisioning is successful.

6.2.65 Benign Warning Messages Displayed During Oracle Identity Manager Managed Server Startup

Several messages resembling the following are logged during Oracle Identity Manager managed server startup:

```
<Mar 30, 2011 6:51:01 PM PDT> <Warning> <oracle.iam.platform.kernel.impl>
<IAM-0080071>
<Preview stage is not supported in kernel and found an event handler with name
ProvisionAccountPreviewHandler implemented by the class
oracle.iam.accesspolicy.impl.handlers.provisioning.ProvisionAccountPreviewHandlerf
or this stage. It will be ignored.>
```

These warning messages are benign and can be ignored because there is no loss of functionality.

6.2.66 Benign Message Displayed When Running the Deployment Manager

When running the Deployment Manager, a message with header ' XUL SYNTAX: ID Conflict' is displayed.

This message is benign and can be ignored because there is no loss of functionality. Close the message and continue.

6.2.67 Deployment Manager Export Fails When Started Using Microsoft Internet Explorer 7 With JRE Plugin 1.6_23

After upgrading Oracle Identity Manager from an earlier release to 11g Release 1 (11.1.1), when you use the Microsoft Internet Explorer 7 Web browser with JRE plugin 1.6_23 to open the Administrative and User Console and try to export files by using the Deployment Manager, an error is generated and you cannot proceed with the export.

To workaround this issue, use a combination of the following Web browsers and plugins:

- Mozilla Firefox 3.6 and JRE version 1.6_23 on 64-bit computer
- Microsoft Internet Explorer 7 and JRE version 1.5
- Microsoft Internet Explorer 8 and JRE version 1.6_18
- Microsoft Internet Explorer 7 and JRE version 1.6_24

6.2.68 User Creation Fails in Microsoft Active Directory When Value of Country Attribute Exceeds Two Characters

In a LDAP-enabled deployment of Oracle Identity Manager, user creation fails in the Microsoft Active Directory (AD) server if the value of the Country attribute exceeds two characters. AD mandates two characters for the Country attribute, for example US, based on the ISO 3166 standards.

6.2.69 Deployment Manager Import Fails if Scheduled Job Entries Are Present Prior To Scheduled Task Entries in the XML File

In Oracle Identity Manager 11g Release 1 (11.1.1), schedules job has a dependency on scheduled task. Therefore, scheduled task must be imported prior to scheduled job.

As a result, if a XML file has scheduled job entries prior to scheduled task entries, then importing the XML file using Deployment Manager fails with the following error message:

```
[exec] Caused By: oracle.iam.scheduler.exception.SchedulerException: Invalid
ScheduleTask definition
[exec] com.thortech.xl.ddm.exception.DDMException
```

To workaround this issue, open the XML file and move all scheduled task entries above the scheduled job entries.

6.2.70 Permission on Target User Required to Revoke Resource

When you login to the Administrative and User Console with Identity User Administrators and Resource Administrators roles, direct provision a resource to a user, and attempt to revoke the resource from the user, an error message is displayed.

To workaround this issue, you (logged-in user) must have the write permission on the target user (such as user1). To achieve this:

1. Create a role, such as role1, and assign self to this role.
2. Create an organization, such as org1, and assign role1 as administrative group.
3. Modify the user user1 and change its organization to org1. You can now revoke the resource from user1.

6.2.71 Reconciliation Event Fails for Trusted Source Reconciliation Because of Missing Reconciliation Rule in Upgraded Version of Oracle Identity Manager

When Oracle Identity Manager is upgraded from an earlier release to 11*g* Release 1 (11.1.1), for trusted source reconciliation, such as trusted source reconciliation using GTC, the reconciliation event fails with the following error message because of a missing reconciliation rule:

```
<Mar 31, 2011 6:27:41 PM CDT> <Info> <oracle.iam.reconciliation.impl>
<IAM-5010006> <The following exception occurred: {0}
oracle.iam.platform.utils.SuperRuntimeException:
Error occurred in XL_SP_RECONEVALUATEUSER while processing Event No 3
Error occurred in XL_SP_RECONUSERMATCH while processing Event No 3
One or more input parameter passed as null
```

To workaround this issue:

1. Create a reconciliation rule for the resource object.
2. In the Resource Object form of the Design Console, click **Create Reconciliation Profile**.

6.2.72 XML Validation Error on Oracle Identity Manager Managed Server Startup

The following error message is logged at the time of Oracle Identity Manager Managed Server startup:

```
<Mar 29, 2011 2:49:31 PM PDT> <Error> <oracle.iam.platform.kernel.impl>
<IAM-0080075> <XML schema validation failed for
XML/metadata/iam-features-callbacks/event_configuration/EventHandlers.xml and it
will not be loaded by kernel. >

<Mar 29, 2011 2:49:32 PM PDT> <Error> <oracle.iam.platform.kernel.impl>
<IAM-0080075> <XML schema validation failed for
XML/metadata/iam-features-OIMMigration/EventHandlers.xml and it will not be loaded
by kernel. >
```

This error message is benign and can be ignored because there is no loss of functionality.

6.2.73 Cannot View or Edit Adapter Mapping in the Data Object Manager Form of the Design Console

When you click **Map** on the Map Adapters tab in the Data Object Manager form of the Design Console, a dialog box is displayed that allows you to edit the individual entity

adapter mappings. But the list with fields on the user object to map is displayed as empty. As a result, you cannot view or edit the individual entity adapter mappings.

Use of entity adapters is deprecated in Oracle Identity Manager 11*g* Release 1 (11.1.1), although limited support is still provided for backward compatibility only. Event handlers must be used for all new or changed scenarios.

6.2.74 Role Memberships for Assign or Revoke Operations Not Updated on Enabling or Disabling Referential Integrity Plug-in

In a multi-directory deployment, the secondary server must be OID. The primary server can be OID or AD. For example, users can be stored in the OID or AD primary server, and roles can be stored in the OID secondary server. Enabling of disabling the referential integrity plug-in does not update the role memberships for assign or revoke operations.

6.2.75 Deployment Manager Import Fails if Data Level for Rules is Set to 1

An entry in the Oracle Identity Manager database cannot be updated if data level is set to 1. When you try to import a Deployment Manager XML, the following error is displayed:

```
Class/Method: tcTableDataObj/updateImplementation Error :The row cannot be
updated.
[2011-04-06T07:25:36.583-05:00] [oim_server1] [ERROR] []
[XELLERATE.DDM.IMPORT] [tid: [ACTIVE].ExecuteThread: '6' for queue:
'weblogic.kernel.Default (self-tuning)'] [userId: xelsysadm] [ecid:
cad00d8aeed4d8fc:-67a4db1a:12f2abbac4b:-8000-000000000000018e,0] [APP:
oim#11.1.1.3.0] The security level for this data item indicates that it cannot be
updated.
```

To workaround this issue, open the XML file and change the data level for rules from 1 to 0, as shown:

```
<RUL_DATA_LEVEL>0</RUL_DATA_LEVEL>
```

6.2.76 Reconciliation Data Displays Attributes That Are Not Modified

In an Oracle Identity Manager deployment with LDAP synchronization enabled and Microsoft Active Directory (AD) as the directory server, the Reconciliation Data tab of the Event Management page in the Administrative and User Console displays all the attributes of the reconciled user instead of displaying only the modified attributes. This is because of the way AD changelogs are processed, in which the entire entry is marked as updated when any attribute is changed. Therefore, Oracle Virtual Directory (OVD) returns the full entry. There is no way to figure out which attribute has been modified as a result of reconciliation.

6.2.77 Benign Errors Displayed on Starting the Scheduler Service When There are Scheduled Jobs to be Recovered

When the Scheduler service is started and there are some scheduled jobs that have not been recovered, the following error might be logged in the oim_diagnostic log:

```
Caused by: java.lang.NullPointerException
at
org.quartz.SimpleTrigger.computeNumTimesFiredBetween(SimpleTrigger.java:800)
at org.quartz.SimpleTrigger.updateAfterMisfire(SimpleTrigger.java:514)
```

```
at
org.quartz.impl.jdbcjobstore.JobStoreSupport.doUpdateOfMisfiredTrigger(JobStor
eSupport.java:944)
at
org.quartz.impl.jdbcjobstore.JobStoreSupport.recoverMisfiredJobs(JobStoreSuppo
rt.java:898)
at
org.quartz.impl.jdbcjobstore.JobStoreSupport.recoverJobs(JobStoreSupport.java:
780)
at
org.quartz.impl.jdbcjobstore.JobStoreSupport$2.execute(JobStoreSupport.java:75
2)
at
org.quartz.impl.jdbcjobstore.JobStoreSupport$40.execute(JobStoreSupport.java:3
628)
at
org.quartz.impl.jdbcjobstore.JobStoreSupport.executeInNonManagedTXLock(JobStor
eSupport.java:3662)
at
org.quartz.impl.jdbcjobstore.JobStoreSupport.executeInNonManagedTXLock(JobStor
eSupport.java:3624)
at
org.quartz.impl.jdbcjobstore.JobStoreSupport.recoverJobs(JobStoreSupport.java:
748)
at
org.quartz.impl.jdbcjobstore.JobStoreSupport.schedulerStarted(JobStoreSupport.
java:573)
```

This error is benign and can be ignored because there is no loss of functionality.

In an upgrade environment, the next time when some scheduled jobs will be triggered is not defined. This results in a null input for Quartz code, which is not handled gracefully in earlier versions of Quartz. This has been fixed in Quartz version 1.6.3, and therefore, this error is not generated when you upgrade to that version of Quartz.

6.2.78 Trusted Source GTC Reconciliation Mapping Cannot Display Complete Attribute Names

When creating a trusted GTC (for example, flat file), the right-hand column under OIM User is not wide enough to display the complete names for many attributes. For example, two entries are displayed as 'LDAP Organizati', whereas the attribute names are 'LDAP Organization' and 'LDAP Organization Unit'.

To workaround this issue, click the **Mapping** button for the attribute. The Provide Field Information dialog box is displayed with the complete attribute name.

6.2.79 Benign Error Logged for Database Connectivity Test

When running the database connectivity test in XIMDD, the following error is logged multiple times:

```
<Apr 10, 2011 7:45:20 PM PDT> <Error> <Default> <J2EE JMX-46335> <MBean attribute
access denied.
   MBean: oracle.logging:type=LogRegistration
   Getter for attribute Application
   Detail: Access denied. Required roles: Admin, Operator, Monitor, executing
subject: principals=[REQUEST TEMPLATE ADMINISTRATORS, SYSTEM ADMINISTRATORS,
APPROVAL POLICY ADMINISTRATORS, oimusers, xelsysadm, PLUGIN ADMINISTRATORS]
java.lang.SecurityException: Access denied. Required roles: Admin, Operator,
Monitor, executing subject: principals=[REQUEST TEMPLATE ADMINISTRATORS, SYSTEM
```

```
ADMINISTRATORS, APPROVAL POLICY ADMINISTRATORS, oim users, xelsysadm, PLUGIN
ADMINISTRATORS]
```

Each time the error occurs in the log, the name of the bean is different, but the error is same. In spite of these errors, the test passes. These errors are benign and can be ignored because there is no loss of functionality.

6.2.80 MDS Validation Error When Importing GTC Provider Through the Deployment Manager

An MDS validation error is generated when you import the GTC provider by using the Deployment Manager.

To workaround this issue, do not import the GTC provider through the Deployment Manager. If the Deployment Manager XML file contains tags for GTC provider, then remove it and import the rest of the XML by using the Deployment Manager. Import the XML file with the GTC provider tags separately by using the MDS import utility. To do so:

1. If the XML file being imported through the Deployment Manager contains <GTCProvider> tags, then remove these tags along with everything under them.

   The following is an example of the original XML file to be imported:

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<xl-ddm-data version="2.0.1.0" user="XELSYSADM"
database="jdbc:oracle:thin:@localhost:5521:myps12"
exported-date="1302888552341" description="sampleGTC"><GTCProvider
repo-type="MDS" name="InsertIntoTargetList"
mds-path="/db/GTC/ProviderDefinitions"
mds-file="InsertIntoTargetListProvTransport.xml"><completeXml><Provider><Provi
der>
   <Provisioning>
      <ProvTransportProvider
class="provisioningTransportProvider.InsertIntoTargetList"
name="InsertIntoTargetList">
         <Configuration>
            <Parameter datatype="String" name="targetServerName"
type="Runtime" encrypted="NO" required="YES"/>
            <Response code="FUNCTIONALITY_NOT_SUPPORTED"
description="Functionality not supported"/>
            <Response code="TARGET_SERVER_NAME_MISSING" description="Target
server name is missing"/>
            <Response code="TARGET_SERVER_NAME_STARTSWITH_A"
description="Target server name starts with A, from XML"/>
            <Response code="PROBLEM_WHILE_INITIALIZAING" description="Problem
occured while intializing Provider instance"/>
         </Configuration>
      </ProvTransportProvider>
   </Provisioning>
</Provider></Provider></completeXml></GTCProvider><GTCProvider
repo-type="MDS" name="PrepareDataHMap" mds-path="/db/GTC/ProviderDefinitions"
mds-file="PrepareDataHMapProvFormat.xml"><completeXml><Provider><Provider>
   <Provisioning>
      <ProvFormatProvider class="provisioningFormatProvider.PrepareDataHMap"
name="PrepareDataHMap">
         <Configuration>
            <DefaultAttribute datatype="String" name="testField" size="40"
encrypted="NO"/>
            <Response code="INCORRECT_PROCESS_DATA" description="Incorrect
```

```
process data received from GTC provisioning framework"/>
            <Response code="PROCESSING_ISSUE" description="Processing issue
in Preparing provisioning input, check logs"/>
         </Configuration>
      </ProvFormatProvider>
   </Provisioning>
</Provider></Provider></completeXml></GTCProvider><GTCProvider
repo-type="MDS" name="IsValidOrgInOIM" mds-path="/db/GTC/ProviderDefinitions"
mds-file="IsValidOrgInOIM.xml"><completeXml><Provider><Provider>
   <Validation>
      <ValidationProvider class="validationProvider.IsValidOrgInOIM"
name="IsValidOrgInOIM">
         <Configuration>
            <Parameter datatype="String" name="maxOrgSize"/>
         </Configuration>
      </ValidationProvider>
   </Validation>
</Provider></Provider></completeXml></GTCProvider><GTCProvider
repo-type="MDS" name="ConvertToUpperCase"
mds-path="/db/GTC/ProviderDefinitions"
mds-file="ConvertToUpperCase.xml"><completeXml><Provider><Provider>
   <Transformation>
      <TransformationProvider
class="transformationProvider.ConvertToUpperCase" name="ConvertToUpperCase">
         <Configuration>
            <Parameter type="Runtime" datatype="String" required="YES"
encrypted="NO" name="Input"/>
            <Response code="errorRespNullInput" description="Input String is
Missing"/>
         </Configuration>
      </TransformationProvider>
   </Transformation>
</Provider></Provider></completeXml></GTCProvider><Resource repo-type="RDBMS"
name="SAMPLEGTC_GTC">....</Resource><Process repo-type="RDBMS"
name="SAMPLEGTC_GTC">
...........
</Process><Form repo-type="RDBMS" name="UD_SAMPLEGT" subtype="Process
Form">.....
</Form>....</xl-ddm-data>
```

2. Import the rest of the XML file through the Deployment Manager.

   The following is the XML file after removing the <GTCProvider> tags from the original XML file. Import this XML file by using the Deployment Manager.

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<xl-ddm-data version="2.0.1.0" user="XELSYSADM"
database="jdbc:oracle:thin:@localhost:5521:myps12"
exported-date="1302888552341" description="sampleGTC"><Resource
repo-type="RDBMS" name="SAMPLEGTC_GTC">....</Resource><Process
repo-type="RDBMS" name="SAMPLEGTC_GTC">
...........
</Process><Form repo-type="RDBMS" name="UD_SAMPLEGT" subtype="Process
Form">.....
</Form>....</xl-ddm-data>
```

   The following is the removed XML content:

```
<GTCProvider
repo-type="MDS" name="InsertIntoTargetList"
mds-path="/db/GTC/ProviderDefinitions"
```

```
mds-file="InsertIntoTargetListProvTransport.xml"><completeXml><Provider><Provid
er>
   <Provisioning>
      <ProvTransportProvider
class="provisioningTransportProvider.InsertIntoTargetList"
name="InsertIntoTargetList">
         <Configuration>
            <Parameter datatype="String" name="targetServerName"
type="Runtime" encrypted="NO" required="YES"/>
            <Response code="FUNCTIONALITY_NOT_SUPPORTED"
description="Functionality not supported"/>
            <Response code="TARGET_SERVER_NAME_MISSING" description="Target
server name is missing"/>
            <Response code="TARGET_SERVER_NAME_STARTSWITH_A"
description="Target server name starts with A, from XML"/>
            <Response code="PROBLEM_WHILE_INITIALIZAING" description="Problem
occured while intializing Provider instance"/>
         </Configuration>
      </ProvTransportProvider>
   </Provisioning>
</Provider></Provider></completeXml></GTCProvider>

<GTCProvider
repo-type="MDS" name="PrepareDataHMap" mds-path="/db/GTC/ProviderDefinitions"
mds-file="PrepareDataHMapProvFormat.xml"><completeXml><Provider><Provider>
   <Provisioning>
      <ProvFormatProvider class="provisioningFormatProvider.PrepareDataHMap"
name="PrepareDataHMap">
         <Configuration>
            <DefaultAttribute datatype="String" name="testField" size="40"
encrypted="NO"/>
            <Response code="INCORRECT_PROCESS_DATA" description="Incorrect
process data received from GTC provisioning framework"/>
            <Response code="PROCESSING_ISSUE" description="Processing issue
in Preparing provisioning input, check logs"/>
         </Configuration>
      </ProvFormatProvider>
   </Provisioning>
</Provider></Provider></completeXml></GTCProvider>

<GTCProvider
repo-type="MDS" name="IsValidOrgInOIM" mds-path="/db/GTC/ProviderDefinitions"
mds-file="IsValidOrgInOIM.xml"><completeXml><Provider><Provider>
   <Validation>
      <ValidationProvider class="validationProvider.IsValidOrgInOIM"
name="IsValidOrgInOIM">
         <Configuration>
            <Parameter datatype="String" name="maxOrgSize"/>
         </Configuration>
      </ValidationProvider>
   </Validation>
</Provider></Provider></completeXml></GTCProvider>

<GTCProvider
repo-type="MDS" name="ConvertToUpperCase"
mds-path="/db/GTC/ProviderDefinitions"
mds-file="ConvertToUpperCase.xml"><completeXml><Provider><Provider>
   <Transformation>
      <TransformationProvider
class="transformationProvider.ConvertToUpperCase" name="ConvertToUpperCase">
```

```
         <Configuration>
            <Parameter type="Runtime" datatype="String" required="YES"
encrypted="NO" name="Input"/>
            <Response code="errorRespNullInput" description="Input String is
Missing"/>
         </Configuration>
      </TransformationProvider>
   </Transformation>
</Provider></Provider></completeXml></GTCProvider>
```

3. Separate the removed XML content based on the <GTCProvier> tags. The following is an example of the first <GTCProvider> tag:

```
<GTCProvider repo-type="MDS" name="InsertIntoTargetList"
mds-path="/db/GTC/ProviderDefinitions"
mds-file="InsertIntoTargetListProvTransport.xml"><completeXml><Provider><Provi
der>
   <Provisioning>
      <ProvTransportProvider
class="provisioningTransportProvider.InsertIntoTargetList"
name="InsertIntoTargetList">
         <Configuration>
            <Parameter datatype="String" name="targetServerName"
type="Runtime" encrypted="NO" required="YES"/>
            <Response code="FUNCTIONALITY_NOT_SUPPORTED"
description="Functionality not supported"/>
            <Response code="TARGET_SERVER_NAME_MISSING" description="Target
server name is missing"/>
            <Response code="TARGET_SERVER_NAME_STARTSWITH_A"
description="Target server name starts with A, from XML"/>
            <Response code="PROBLEM_WHILE_INITIALIZAING" description="Problem
occured while intializing Provider instance"/>
         </Configuration>
      </ProvTransportProvider>
   </Provisioning>
</Provider></Provider></completeXml></GTCProvider>
Resultant xml after removal of tags surronding inner <Provider> tag:
<Provider>
   <Provisioning>
      <ProvTransportProvider
class="provisioningTransportProvider.InsertIntoTargetList"
name="InsertIntoTargetList">
         <Configuration>
            <Parameter datatype="String" name="targetServerName"
type="Runtime" encrypted="NO" required="YES"/>
            <Response code="FUNCTIONALITY_NOT_SUPPORTED"
description="Functionality not supported"/>
            <Response code="TARGET_SERVER_NAME_MISSING" description="Target
server name is missing"/>
            <Response code="TARGET_SERVER_NAME_STARTSWITH_A"
description="Target server name starts with A, from XML"/>
            <Response code="PROBLEM_WHILE_INITIALIZAING" description="Problem
occured while intializing Provider instance"/>
         </Configuration>
      </ProvTransportProvider>
   </Provisioning>
</Provider>
```

4. From the removed <GTCProvider> tags, remove everything surrounding the inner <Provider> tag. In other words, keep the content inside the inner <Provider> tag.

For each <Provider> tag, create a separate XML file. This results in multiple XML files with each <Provider> tag as the root element.

The following is the resultant XML content after removal of tags surrounding the inner <Provider> tag:

```
<Provider>
   <Provisioning>
      <ProvTransportProvider
class="provisioningTransportProvider.InsertIntoTargetList"
name="InsertIntoTargetList">
         <Configuration>
           <Parameter datatype="String" name="targetServerName" type="Runtime"
encrypted="NO" required="YES"/>
            <Response code="FUNCTIONALITY_NOT_SUPPORTED"
description="Functionality not supported"/>
            <Response code="TARGET_SERVER_NAME_MISSING" description="Target
server name is missing"/>
            <Response code="TARGET_SERVER_NAME_STARTSWITH_A"
description="Target server name starts with A, from XML"/>
            <Response code="PROBLEM_WHILE_INITIALIZAING" description="Problem
occured while intializing Provider instance"/>
         </Configuration>
      </ProvTransportProvider>
   </Provisioning>
</Provider>
```

5. Name the resultant XML files, which have the <Provider> tag as the root element, with the mds-file attribute value from the <GTCProvider> tag. For example, name the first XML file with the first <GTCProvider> tag as InsertIntoTargetListProvTransport.xml. The file name must be the value of the mds-file attribute.
6. Similarly, create other GTC provider XML files. There must be one XML file for each <GTCProvider> tag.
7. Import the GTC Provider XML files by using the MDS utility.

6.2.81 Encrypted User-Defined Field (UDF) Cannot be Stored with Size of 4000 Characters or More

An encrypted UDF cannot be stored with size of 4000 characters or more. This is because encryption automatically increases the column width by 1.5 times approximately, and the size of the attribute exceeds the maximum allowable width of 4000. As a result, the UDF is automatically type-promoted to a CLOB data type. Oracle Identity Manager 11*g* Release 1 (11.1.1) does not intercept this as an exception and might subsequently show errors. This is likely to be addressed in the next patch release.

However, an encrypted attribute that does not exceed the final width of 4000 characters can be stored. The specified width must factor in the increment of 1.5 times, which means that it must not exceed approximately 2500 characters.

6.2.82 Request Approval Fails With Callback Service Failure

In an environment where SSL is enabled in the OAAM server but not in Oracle Identity Manager and SOA server, when you create a request, the request-level approval is successful on the SOA side, but the operational-level approval is not displayed anywhere in the UI. When the SOA composite that provides approval

workflow for the Oracle Identity Manager request tries to invoke the request callback Web service to indicate whether the workflow is approved or rejected, the Web service invocation fails with the following error:

```
Unable to dispatch request to
http://slc402354.mycompany.com:14000/workflowservice/CallbackService due to
exception[[
javax.xml.ws.WebServiceException:
oracle.fabric.common.PolicyEnforcementException: PolicySet Invalid: WSM-06162
PolicyReference The policy referenced by URI
"oracle/wss11_saml_token_with_message_protection_client_policy" could not be
retrieved as connection to Policy Manager cannot be established at
"t3s://slc402354:14301" due to invalid configuration or inactive state.
```

The error indicates that OWSM is not able to connect to the Policy Manager on the specified port. This port is for the OAAM server in SSL mode, which is shut down. The issue occurs because SSL is enabled in the OAAM server but not on Oracle Identity Manager and SOA server, and the Policy Manager is also targeted on that server. If there is an SSL-enabled Policy Manager, then OWSM does not use the non-SSL ports anymore. In this setup, SSL is enabled only for OAAM and not for others. Therefore, the only usable WSM Policy Manager is on OAAM. Because the OAAM server is down, the connection to the Policy Manager is not established, and as a result, the call fails.

To workaround this issue, start the OAAM server and then create the request.

Note: This issue does not occur if:

- OAAM server is not SSL-enabled.
- SSL is enabled on any other server that is up and running, such as Oracle Identity Manager or SOA server.

6.2.83 Localized Display Name is Not Reconciled Via User/Role Incremental Reconciliation with iPlanet Directory Server

In an Oracle Identity Manager deployment with LDAP synchronization enabled in which iPlanet is the directory server, the following issues occur:

- The localized Display Name is not reconciled into Oracle Identity Manager via user/role incremental reconciliation.
- The localized value of the Display Name attribute is returned to Oracle Identity Manager, but the original base value of Display Name is lost and is replaced by the localized value that is received from iPlanet.

6.2.84 LDAP Role Hierarchy and Role Membership Reconciliation With Non-ASCII Characters Does Not Reconcile Changes in Oracle Identity Manager

LDAP role hierarchy and role membership reconciliation jobs with non-ASCII characters do not bring in role hierarchy and role membership changes into Oracle Identity Manager. This issue is applicable to incremental reconciliation only.

6.2.85 Import of Objects Fails When All Objects Are Selected for Export

In an upgraded environment of Oracle Identity Manager 11g Release 1 (11.1.1), the import of objects can fail when you select the Select All option to export the objects. When you select all the objects to be exported, the corresponding XML file grows in

size. If it exceeds 2.5 million records, then it does not remain valid. As a result, the import fails. However, selecting all objects works if the data is small and the generated XML file does not exceed 2.5 million records.

To workaround this issue, select the objects to be exported in smaller logical units. For example, if there are 20 resource objects in the system, then select four or five resource objects with all dependencies and children objects in a XML file, and export. Then select another five resource objects into a new XML file. Similarly, for all other objects, such as GTC or adapters, export in small logical units in separate XML files. Examples of logical unit grouping are:

- Resource objects, process definition forms, adapters, IT resources, lookup definitions, and roles
- Organizations, attestation, and password policies
- Access policies and rules
- GTC and resource objects

6.2.86 Benign Audit Errors Logged After Upgrade

After upgrading from Oracle Identity Manager Release 9.1.0 to 11*g* Release 1 (11.1.1), audit errors are logged. An example of such an audit error is:

```
IAM-0050001
oracle.iam.platform.async.TaskExecutionException: java.lang.Exception: Audit
handler failed
at com.thortech.xl.audit.engine.jms.XLAuditMessage.execute(XLAuditMessage.java:59)
```

These errors are benign and can be ignored because there is no loss of functionality.

6.2.87 Connector Upgrade Fails if Existing Data is Bigger in Size Than New Column Length

In the current release of some connectors, the sizes of some process form fields have been reduced. For example, the length of the UD_ADUSER_MNAME field in the Microsoft Active Directory connector release 9.1.1.5 has been reduced to 6 characters from 80 characters in release 9.0.4.16 of the connector. The length of the existing data in these columns or fields are already bigger in size than the new column length. As a result, the connector upgrade fails, and the following error is logged:

```
<Apr 16, 2011 4:52:37 PM GMT+05:30> <Error> <XELLERATE.DATABASE> <BEA-000000>
<ALTER TABLE UD_ADUSER MODIFY UD_ADUSER_MNAME VARCHAR2(6) java.sql.SQLException:
ORA-01441: cannot decrease column length because some value is too big
```

To workaround this issue:

1. Make sure that you create a backup of the database.
2. Restore the backed up database.
3. Check the logs to locate the 'ORA-01441: cannot decrease column length because some value is too big' exception. Note the form field name, such as UD_ADUSER_MNAME.
4. Open the Deployment Manager XML file that you are using for upgrade. Search for the form field in the <SDC_SQL_LENGTH> tag, and change the length to the base version length. You can get the base version length in the Deployment Manager XML of the base connector.
5. Retry the upgrade.

6.2.88 Connector Artifacts Count Increases in the Deployment Manager When File is Not Imported

When you upgrade a connector, map the connector artifacts between the base and latest versions, select the connector objects to be upgraded, and exit the upgrade without importing the objects by using the Deployment Manager, the connector artifacts count in the left panel displays more than the actual count. When this process is repeated, the artifacts count continues increasing. This is a known issue, and there is no loss of functionality.

6.2.89 Uploading JAR Files By Using the Upload JAR Utility Fails

When SSL is enabled for Oracle Identity Manager, uploading the JAR files by using the Upload JAR utility fails with the following error:

```
Error occurred in performing the operation:
Exception in thread "main" java.lang.NullPointerException at
oracle.iam.platformservice.utils.JarUploadUtility.main(JarUploadUtility.java:229)
```

With SSL enabled in Oracle Identity Manager, the server URL must contain the exact host name or IP address. If localhost is used as the host name, then the error is generated.

To workaround this issue, use the exact server URL.

6.2.90 Oracle Identity Manager Data and MT Upgrade Fails Because Change of Database User Password

If you are NOT upgrading the original Oracle Identity Manager Release 9.x database, but choose to export/import to a new database, then you must make sure that the database connection setting, schema name, and password in the *OIM_HOME*/xellerate/config/xlconfig.xml file used for the upgrade is correct.

To workaround this issue, change the Oracle Identity Manager database information in the xlconfig.xml file. You must create a backup of this file before updating it. To update the file with the new database information, modify the information of the loaction where the database has been imported in the <URL>, <username>, and <Password ...> tags, as shown:

```
<DirectDB>
<driver>oracle.jdbc.driver.OracleDriver</driver>
<url>jdbc:oracle:thin:@localhost:1522:oimdb</url>
<username>oimadm</username>
<password encrypted="false"><NEW_PASSWORD_FOR_OIM_DB_USER></password>
<maxconnections>5</maxconnections>
<idletimeout>360</idletimeout>
<checkouttimeout>1200</checkouttimeout>
<maxcheckout>1000</maxcheckout>
</DirectDB>
```

6.2.91 Reverting Unsaved UDFs Are Not Supported in the Administration Details Page for Roles and Organizations

The Administration Details pages for roles and organizations in the Administrative and User Console do not support reverting unsaved UDF attribute values. Therefore, if you modify the UDF attribute values for a role or organization and then do not want to save the changes to these attributes, then perform one of the following:

- Close the tab with the modified role or organization. A warning message is displayed asking if you want to continue. Clicking **Yes** cancels all unsaved changes.
- You can manually edit the modified attributes to their original state. Saving the entity applies any other desired changes made.

6.2.92 Resources Provisioned to User Without Checking Changes in User Status After Request is Submitted

After submission of a request, if the user associated with the request, such as beneficiary, requester, or approver, is disabled or deleted, then the resources are provisioned to the user without checking for user status, such as Disabled or Deleted, after the request is approved.

6.2.93 Starting UCP Connection Pool Fails When Trying to Create User on 64-Bit Microsoft Windows With JDK 6

CRUD operations on Microsoft Windows 64-bit platform using JDK 6 fails in Non Input Output (NIO) mode. This is because of a limitation in JDK 6 to support IPv6 stack in Microsoft Windows Vista 2008. This support is added in JDK 7 since Build b36. With JDK 7, it works in OVD NIO mode.

To workaround this issue:

1. In the OVD server, turn off NIO mode. To do so:
   a. Open the OracleInstance/config/OVD/ovd1/listeners.os_xml file.
   b. Add <useNIO>false</useNIO> at the following location:

```
<ldap id="LDAP Endpoint" version="0">
    <port>6501</port>
    ...
    <socketOptions>
        ...
    </socketOptions>
    <useNIO>false</useNIO>
</ldap>
```

   c. Save the listeners.os_xml file.
2. Restart the OVD server.

6.2.94 Config.sh Command Fails When JRockit is Installed With Data Samples and Source

When you install jrockit-jdk1.6.0_24-R28.1.3-4.0.1-linux-x64.bin with demo samples and source, and install Oracle WebLogic Server using wls1035_generic.jar on a Linux 64-bit computer, and run Oracle Identity Manager configuration wizard by running the config.sh command from the $ORACLE_HOME/bin/ directory, the Oracle universal installer does not start and the following error message is displayed:

```
config.sh: line 162:  9855 Segmentation fault $INSTALLER_
DIR/runInstaller-weblogicConfig ORACLE_HOME="$ORACLE_HOME" -invPtrLoc$ORACLE_
HOME/oraInst.loc -oneclick $COMMANDLINE -Doracle.config.mode=true
```

6.2.95 Unexpected Memory Usage in Oracle Identity Manager 11*g* Release 1(11.1.1)

On running scheduled tasks that perform user orchestration in bulk, such as EndDateSchedulerTask and StartDateSchedulerTask, Oracle Identity Manager 11*g* Release 1 (11.1.1) might consume large memory space. This can cause Out of Memory issues.

This is a known issue, and a workaround is not available for this in the current release.

6.2.96 Reports Link No Longer Exists in the Administrative and User Console

Under the Administration tab of the Advanced Administration in the Administrative and User Console, the Reports link to generate BI Publisher Reports has been removed, even though BIP has been selected while installing Oracle Identity Manager.

6.2.97 Not Allowing to Delete a Role Whose Assigned User Members are Deleted

If the user members of a role have been deleted before revoking the role memberships, then the role cannot be deleted. Therefore, you must revoke the user role memberships that have been explicitly assigned before deleting the user.

6.2.98 Roles and Organizations Do Not Support String UDFs of Password Type

Creating a String UDF of password type for roles and organizations is not supported. If you try to create such a UDF, then the Administrative and User Console does not allow you create roles and organizations.

6.2.99 Error on Importing Connector By Using the Deployment Manager

If you export a connector from a Oracle Identity Manager deployment to another deployment by using the Deployment Manager, then an error similar to the following might be generated:

```
[ERROR] [] [XELLERATE.WEBAPP]
[tid: [ACTIVE].ExecuteThread: '0' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: xelsysadm] [ecid:
f9e72ab2a292a346:-421e2bf0:12f77f65b9a:-8000-0000000000000174,0] [APP:
oim#11.1.1.3.0] Class/Method: LoadDeploymentUtility/importSelected encounter
some problems: oracle.iam.reconciliation.exception.ConfigException: Profile
:AD User Trusted InvalidAttributes : [ObjectGUID][[
com.thortech.xl.ddm.exception.DDMException:
oracle.iam.reconciliation.exception.ConfigException: Profile :AD User Trusted
InvalidAttributes : [ObjectGUID]
at
com.thortech.xl.ejb.beansimpl.tcImportOperationsBean.performImport(tcImportOpe
.
rationsBean.java:1199)
```

This problem is because of the missing dependencies of UDFs created on the user entity. To avoid this problem, perform any one of the following:

- Manually create the UDFs in the system before importing the connector XMLs.
- Export the user meta data through the Deployment Manager and import it in the target environment. This bring in all the UDFs created on the user entity. However, if the requirement confines to some specific UDFs or if it is not desirable to have all the UDFs in the target system, then create the required UDFs manually.

6.2.100 Manage Localizations Dialog Box Does Not Open After Modifying Roles

After a role is modified, the Manage Localizations dialog box is not opening on clicking the **Manage Localizations** button in the role details page.

To open the Manage Localizations dialog box after modifying a role, close the role details page and open it again.

6.2.101 Not Allowing to Create User With Language-Specific Display Name Values

In an Oracle Identity Manager deployment with Microsoft Active Directory (AD) as the LDAP server, localized display name values are supported when you specify the oimLanguage parameter values in the UserManagement plugin adapter for AD via OVD. However, a user cannot be created when a language-specific value for the Display Name attribute is specified in Canadian French or Latin American Spanish, even if these languages have been specified in oimLanguage. In addition, when you create a user without language-specific Display Name, and then modify the user to add Canadian French or Latin American Spanish Display Name values, the same issue persists.

6.2.102 SoD Check Results Not Displayed for Requests Created by Users for the PeopleSoft Resource

SoD check results are not displayed for the requests created by users for the PeopleSoft (PSFT) resource.

To workaround this issue:

1. Open the PSFT connector XML file.
2. Under the <ITResource name = "PSFT Server"> tag, add the following:

```
<ITResourceAdministrator>
    <SUG_READ>1</SUG_READ>
    <SUG_UPDATE>1296129050000</SUG_UPDATE>
    <UGP_KEY UserGroup = "ALL USERS"/>
</ITResourceAdministrator>
```

3. Save the PSFT connector XML file.
4. Manually add or assign the ALL USERS role with Read permission to the PSFT Server IT resource.

6.2.103 The XL.UnlockAfter System Property and the Automatically Unlock User Scheduled Job Do Not Take Effect

The XL.UnlockAfter system property determines the unlock time for the locked user accounts after the specified time. If the user account is locked because of the maximum login attempt failure with invalid credentials, then the account is automatically unlocked after the time (in minutes) as configured in the XL.UnlockAfter system property. By default, the value of this system property is 0, which implies that the locked user is never unlocked automatically.

The Automatically Unlock User scheduled job is responsible for unlocking such users. This scheduled job is configured to run after every 24 hours (1 day).

Therefore, even after the maximum time of Oracle WebLogic lockout threshold and expiry of the time specified for the XL.UnlockAfter system property, the locked users might not be able to login unless the Automatically Unlock User scheduled job is run.

If you are changing the default value of the XL.UnlockAfter system property, then it is recommended to change the frequency of the Automatically Unlock User scheduled task so that both the values are in sync. This ensures that the scheduled task gets triggered at the appropriate interval, and the users are unlocked successfully and are able to login in to Oracle Identity Manager.

6.2.104 Resetting Password on Account Lockout Does Not Unlock User

In a Oracle Identity Manager deployment with LDAP synchronization enabled and integrated with Oracle Access Manager (OAM), a user is locked on entering incorrect password more than the maximum allowed limit. However, the user is not allowed to unlock by resetting the password until after reconciliation is run.

6.2.105 Starting Oracle Identity Manager and SOA Server on Some 64-bit Microsoft Windows Computers for the First Time Takes Time

On some Microsoft Windows 64-bit computers, it is observed that Oracle Identity Manager and SOA Server take more than an hour to start for the first time. However, do not stop the managed servers while this process is going on. After the first start, subsequent restarts do not take the extended time.

6.2.106 Incremental and Full Reconciliation Jobs Cannot Be Run Together

Both incremental and full reconciliation jobs cannot be run at the same time. Incremental reconciliation jobs are enabled and run in periodic intervals of 5 minutes. At the same time, when full reconciliation job is run, an error is generated.

To workaround this issue, if full reconciliation needs to be run, then disable the incremental reconciliation jobs before running the full reconciliation jobs. After full reconciliation completes successfully, re-enable the incremental reconciliation jobs.

6.2.107 Incorrect Content in the ScheduleTask Jars Loaded and Third Party Jars Tables in the MT Upgrade Report

When Oracle Identity Manager release 9.1.x is upgraded to Oracle Identity Manager 11*g* Release 1 (11.1.1), the contents of the ScheduleTask Jars Loaded and Third Party Jars tables in the CRBUpgradeReport.html page generated by MT upgrade are not correct. The original scheduled task JARs are not displayed in the ScheduleTask Jars Loaded table. Therefore, you must run the SQL query query to know the scheduled task JARs. In addition, the third-party JARs are incorrectly placed in the ScheduleTask Jars Loaded table.

However, this does not result in any loss of functionality.

6.2.108 Scroll Bar Not Available on the Select Connector Objects to Be Upgraded Page of the Connector Management - Upgrading Wizard

If the Connector Management - Upgrading wizard is opened by using Microsoft Internet Explorer, then all the fields and buttons on the Step 13: Select Connector Objects to Be Upgraded page might not be visible. There is no scroll bar available in this page. Therefore, maximize the window to display all the controls in the page.

6.2.109 Adapter Import Might Display Adapter Logic if Compilation Fails Because of Incorrect Data

If you import a process task adapter by using the Design Console and the adapter compilation fails because of incorrect data, then the error displays the entire code for the adapter.

This is a known issue, and a workaround is not available for this in the current release.

6.2.110 XIMDD Tests Fail in Oracle Identity Manager

After you deploy the Diagnostic Dashboard in Oracle Identity Manager, failures are encountered when you perform the following tests:

- Test OWSM setup by submitting a request with OWSM header information
- Test SPML to Oracle Identity Manager request invocation

The failures might occur because the Diagnostic Dashboard is not capable of performing tests when the wss1_saml_or_username_token_policy is attached to the SPML XSD Web services.

To workaround this issue, set the Web service to use the XIMDD supported policy. To configure the policies for the SPML XSD Web service:

1. Login to Fusion Middleware Control.
2. Navigate to **Application Deployments**, **spml-xsd**.
3. For a clustered deployment of Oracle Identity Manager, expand and select a node.
4. From the Application Deployment menu, select **Web Services**.
5. Click the **Web Service Endpoint** tab, and then click the **SPMLServiceProviderSOAP** link.
6. Click the **Policies** tab, and then click **Attach/Detach**.
7. Detach the default policy: oracle/wss11_saml_or_username_token_with_message_protection_service_policy.
8. Under Available Policies, select **oracle/wss_username_token_service_policy**. Otherwise, select the SSL version of the same policy if SSL is in use.
9. Click **Attach**, and then click **OK**.
10. For a clustered deployment of Oracle Identity Manager, repeat step 3 through step 9 for each managed node listed for SPML XSD.
11. Restart the application servers.

6.3 Configuration Issues and Workarounds

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

6.3.1 Configuring UDFs to be Searchable for Microsoft Active Directory Connectors

A Microsoft Active Directory connector installation automatically creates a UDF: USR_UDF_OBGUID. When you add a new user-defined field (UDF), the "searchable" property will be false by default unless you provide a value for that property. After installing an Active Directory connector, you must perform the following steps to make the user-defined field searchable:

1. Using the Advanced Administration console (user interface), change the "searchable" UDF property to true by performing the following steps:
   a. Click the Advanced tab.
   b. Select User Configuration and then User Attributes.
   c. Modify the USR_UDF_OBGUID attribute in the Custom Attributes section by changing the "searchable" property to true.
2. Using the Identity Administration console (user interface), create a new Oracle Entitlement Server policy that allows searching the UDF by performing the following steps:
   a. Click the Administration tab and open the Create Authorization policy.
   b. Enter a Policy Name, Description, and Entity Name as User Management.
   c. Select Permission, then View User Details, and then Search User.
   d. Edit the Attributes for View User Details and select all of the attributes.
   e. Select the SYSTEM ADMINSTRATOR role name.
   f. Click Finish.

6.3.2 Creating or Modifying Role Names When LDAP Synchronization is Enabled

When LDAP synchronization is enabled and you attempt to create or modify a role, entering a role name comprised of approximately 1,000 characters prevents the role from being created or modified and causes a `Decoding Error` to appear. To work around this issue, use role names comprised of fewer characters.

6.3.3 ADF Issue Causes Oracle Identity Manager to Fail on the Sun JDK

Due to an ADF issue, using the Oracle Identity Manager application with the Sun JDK causes a StringIndexOutOfBoundsException error. To work around this issue, add the following option to the DOMAIN_HOME/bin/setSOADomainEnv.sh or the setSOADomainEnv.cmd file:

1. Open the *DOMAIN_HOME*/bin/setSOADomainEnv.sh or setSOADomainEnv.cmd file.
2. Add the -XX:-UseSSE42Intrinsics line to the JVM options.

3. Save the setSOADomainEnv.sh or setSOADomainEnv.cmd file.

Note: This error does not occur when you use JRockit.

6.3.4 Nexaweb Applet Does Not Load In an Oracle Identity Manager and Oracle Access Manager Integrated Environment

In an Oracle Identity Manager and Oracle Access Manager (OAM) integrated environment, when you login to the Oracle Identity Manager Administrative and User Console and click a link that opens the Nexaweb applet, the applet does not load.

To workaround this issue, configure loading of the NexaWeb Applet in an Oracle Identity Manager and OAM integrated environment. To do so:

1. Login to the Oracle Access Manager Console.
2. Create a new Webgate ID. To do so:
   a. Click the **System Configuration** tab.
   b. Click **10Webgates**, and then click the Create icon.
   c. Specify values for the following attributes:

      Name: *NAME_OF_NEW_WEBGATE_ID*

      Access Client Password: *PASSWORD_FOR_ACCESSING_CLIENT*

      Host Identifier: IDMDomain
   d. Click **Apply**.
   e. Edit the Webgate ID, as shown:

      set 'Logout URL' = /oamsso/logout.html
   f. Deselect the **Deny On Not Protected** checkbox.
3. Install a second Oracle HTTP Server (OHS) and Webgate. During Webgate configurations, when prompted for Webgate ID and password, use the Webgate ID name and password for the second Webgate that you provided in step 2c.
4. Login to the Oracle Access Manager Console. In the Policy Configuration tab, expand Application Domains, and open IdMDomainAgent.
5. Expand Authentication Policies, and open Public Policy. Remove the following URLs in the Resources tab:

   /xlWebApp/.../*

   /xlWebApp

   /Nexaweb/.../*

   /Nexaweb
6. Expand Authorization Policies, and open Protected Resource Policy. Remove the following URLs in the Resources tab:

   /xlWebApp/.../*

   /xlWebApp

   /Nexaweb/.../*

   /Nexaweb

7. Restart all the servers.
8. Update the obAccessClient.xml file in the second Webgate. To do so:
   a. Create a backup of the *SECOND_WEBGATE_HOME*/access/oblix/lib/ObAccessClient.xml file.
   b. Open the *DOMAIN_HOME*/output/*WEBGATE_ID_FOR_SECOND_WEBGATE*/ObAccessClient.xml file.

      Note: Ensure that the DenyOnNotProtected parameter is set to 0.

   c. Copy the *DOMAIN_HOME*/output/*WEBGATE_ID_FOR_SECOND_WEBGATE*/ObAccessClient.xml file to the *SECOND_WEBGATE_HOME*/access/oblix/lib/ directory.
9. Copy the mod_wls_ohs.conf from the *FIRST_OHS_INSTANCE_HOME*/config/*OHS_NAME*/directory to the *SECOND_OHS_INSTANCE_HOME*/config/*OHS_NAME*/ directory. Then, open the mod_wls_host.conf of the second OHS to ensure the WebLogicHost and WeblogicPort are still pointing to Oracle Identity Manager managed server host and port.
10. Remove or comment out the following lines in the *SECOND_OHS_INSTANCE_HOME*/config/*OHS_NAME*/httpd.conf file:

```
<LocationMatch "/oamsso/*">
   Satisfy any
</LocationMatch>
```

11. Copy the logout.html file from the FIRST_WEBGATE_HOME/access/oamsso/ directory to the SECOND_WEBGATE_HOME/access/oamsso/ directory. Then, open the logout.html file of the second Webgate to ensure that the host and port setting of the SERVER_LOGOUTURL variable are pointing to the correct OAM host and port.
12. Login to Oracle Access Manager Console. In the Policy Configuration tab, expand **Host Identifiers**, and open the host identifier that has the same name as the second Webgate ID name. In the Operations section, verify that the host and port for the second OHS are listed. If not, then click the add icon (+ sign) to add them. Then, click **Apply**.
13. Use the second OHS host and port in the URL for the OAM login page for Oracle Identity Manager. The URL must be in the following format:

    http://*SECOND_OHS_HOST*:*SECOND_OHS_PORT*/admin/faces/pages/Admin.jspx

6.3.5 Packing a Domain With managed=false Option

When a domain is packed with the managed=false option and unpacked on the another computer, Oracle Identity Manager Authentication Provider is not recognized by WebLogic and basic administrator authentication fails when the Oracle Identity Manager managed server is started.

The following workaround can be applied for performing successful authentication via Oracle Identity Manager Authentication Provider:

1. Login in to the Oracle WebLogic Administrative Console by using the following URL:

http://*HOST_NAME*:*ADMIN_PORT*/console

2. Navigate to **Security Realms**, **Realm(myrealm)**, and then to **Providers**.
3. Delete OIMAuthenticationProvider.

> **Note:** Make sure that you note the provider-specific details, such as the database URL, password, and driver, before deleting the provider.

4. Restart the WebLogic Administrative Server.
5. Navigate to **Security Realms**, **Realm(myrealm)**, and then to **Providers**.
6. Create a new Authentication Provider of type OIMAuthenticationProvider.
7. Enter the provider specific details and mark the control flag as SUFFICIENT.
8. Restart the WebLogic Administrative Server.
9. Restart Oracle Identity Manager and other servers, if any.

6.3.6 Option Not Available to Specify if Design Console is SSL-Enabled

While configuring Oracle Identity Manager Design Console, you cannot specify if Design Console is SSL-enabled.

To workaround this issue after installing Oracle Identity Manager Design Console, edit the *OIM_HOME*/designconsole/config/xlconfig.xml file to change the protocol in the Oracle Identity Manager URL from t3 to t3s.

6.3.7 Nexaweb Applet Does Not Load in JDK 1.6.0_20

Deployment Manager and Workflow Visualizer might not work if the client browser has JDK/JRE installed on it whose version is 1.6.0_20. To workaround this issue, uninstall the JDK/JRE version 1.6.0_20 from the client browser and reinstall the JDK/JRE version 1.6.0_15.

6.3.8 Error is Generated on Starting Servers With Sun JDK 160_24 (32-bit) on Microsoft Windows 2008

When you install Oracle WebLogic Server (64-bit), Oracle Identity Manager, and SOA Server, and select Sun JDK 160_24 (32-bit) on Microsoft Windows 2008, an out-of-memory error is generated on starting the SOA Server and Oracle Identity Manager.

To workaround this issue, add -XX:-DoEscapeAnalysis. For example:

```
set USER_MEM_ARGS=-Xms512m -Xmx1024m -XX:CompileThreshold=8000 -XX:PermSize=128m
-XX:MaxPermSize=512m -XX:-DoEscapeAnalysis
```

6.3.9 Oracle Identity Manager and Design Console Must be Installed in Different Directory Paths

Oracle recommends to install Oracle Identity Manager and the Design Console in different directory paths.

6.3.10 Error on Adding Organization to User in Windows Explorer 8

In Microsoft Windows Internet Explorer 8 web browser, when you find and select an organization in the popup window from the Create User page, clicking the **Add** button displays the following error:

```
popup is null or not an object
```

To workaround this issue, make sure that the **Display a notification about every script error** option is not selected in the Advanced tab of the Internet Options dialog box.

6.4 Multi-Language Support Issues and Limitations

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

6.4.1 Multi-language Valued Attributes in SPML and Oracle Identity Manager Do Not Match

Oracle Identity Manager supports only the Display Name attribute for multi-language values. SPML specifies additional attributes, such as commonName and surname, as multi-language valued in the PSO schema. When multiple locale-values are specified in an SPML request for one of these attributes, only a single value is picked and passed to Oracle Identity Manager. The request will not fail and a warning message identifying the attributes and the value that was passed to Oracle Identity Manager is provided in the response.

6.4.2 Login Names with Some Special Characters May Fail to Register

In Oracle Identity Manager, the user login name is case-insensitive. When a user is created, the login name is converted to upper case and saved in the database. But the password is always case-sensitive. However, some special characters may encounter an error while registering to Oracle Identity Manager:

- Both the Greek characters σ (sigma) and ς (final sigma) maps to the Σ character.
- Both English character i and Turkish character ı maps to the I character.
- Both German character ß and English string SS maps to the SS string.

This means that two user login names containing these special characters when the other characters in the login names are same cannot be created. For example, the user login names Johnß and JohnSS maps to the same user login name. If Johnß already exists, then creation of JohnSS is not allowed because both the ß character and the SS string maps to the SS string.

6.4.3 The Create Role, Modify Role, and Delete Role Request Templates are Not Available for Selection in the Request Templates List

The Create Role, Modify Role, and Delete Role request templates are not available in the Request Templates list of the Create Request wizard. This is because request creation by using any request template that are based on the Create Role, Modify Role, and Delete Role request models are supported from the APIs, but not in the UI. However, you can search for these request templates in the Request Templates tab. In

addition, the Create Role, Modify Role, and Delete Role request models can be used to create approval policies and new request templates.

6.4.4 Parameter Names and Values for Scheduled Jobs are Not Translated

In the Create Job page of Oracle Identity Manager Advanced Administration, the fields in the Parameter section and their values are not translated. The parameter field names and values are available only in English.

6.4.5 Bidirectional Issues for Legacy User Interface

The following are known issues in the legacy user interface, also known as TransUI, contained in the xlWebApp war file:

- Hebrew bidirectional is not supported
- Workflow designer bidirectional is not supported for Arabic and Hebrew

6.4.6 Localization of Role Names, Role Categories, and Role Descriptions Not Supported

Localization of role names, categories, and descriptions is not supported in this release.

6.4.7 Localization of Task Names in Provisioning Task Table Not Supported

All Task Name values in the Provisioning Task table list are hard-coded and these pre-defined process task names are not localized.

6.4.8 Localization of Search Results of Scheduled Tasks Not Supported

When you search Scheduler Tasks using a Simple or Advanced search, the search results are not localized.

6.4.9 Searching for User Login Names Containing Certain Turkish Characters Causes an Error

On the Task Approval Search page, if you select "View Tasks Assigned To", then "Users You Manage", and then choose a user whose login name contains a Turkish Undotted "&#305" or a Turkish dotted "&#304" character, a User Not Found error will result.

6.4.10 Localization of Notification Template List Values for Available Data Not Supported

Localizing Notification Template Available Data list values is not supported in this release. Oracle Identity Manager depends upon the Velocity framework to merge

tokens with actual values, and Velocity framework does not allow a space in token names.

6.4.11 Searching for Entity Names Containing German "ß" (Beta) Character Fails in Some Features

When you search for entity names containing the special German "ß" (beta) character from the Admin Console, the search fails in the following features:

- System Configuration
- Request Template
- Approve Policy
- Notification

In these features, the "ß" character matches to "ss" instead of itself. Consequently, the Search function cannot find entity names that contain the German beta character.

6.4.12 Special Asterisk (*) Character Not Supported

Although special characters are supported in Oracle Identity Manager, using the asterisk character (*) can cause some issues. You are advised not to use the asterisk character when creating or modifying user roles and organizations.

6.4.13 Translated Error Messages Are Not Displayed in UI

Oracle Identity Manager does not support custom resource bundles for Error Message display in user interfaces. Currently, there is no workaround for this issue.

6.4.14 Reconciliation Table Data Strings are Hard-coded on Reconciliation Event Detail Page

Some of the table data strings on the Reconciliation Event Detail page are hard-coded, customized field names. These strings are not localized.

6.4.15 Translated Password Policy Strings May Exceed the Limit in the Background Pane

Included as per bug# 9539501

The password policy help description may run beyond the colored box in some languages and when the string is too long. Currently, there is no workaround for this issue.

6.4.16 Date Format Validation Error in Bi-Directional Languages

When Job Detail page is opened in bi-directional languages, you cannot navigate away from this page because of "Date Format Validation Error". To work around this issue,

select a value for the "Start Date" using the date-time control and then move to another page.

6.4.17 Mistranslation on the Create Job page

On the Japanese locale (LANG=ja_JP.UTF-8), "Fourth Wednesday" is mistranslated as "Fourth Friday" on the Create Job page when "Cron" is selected as the Schedule Type and "Monthly on given weekdays" is selected as the Recurring Interval.

6.4.18 E-mail Notification for Password Expiration Cannot Be Created With Arabic Language Setting

When the server locale is set to ar_AE.utf8 and values for user.language and user.region system properties are ar and AE respectively, if you create a password expiration warning e-mail notification in the Design Console, the value AE is not available for selection in the Region field. As a result, the email notification message cannot be created.

To workaround this issue:

1. Open the Lookup Definitions form in the Design Console.
2. Search for 'Global.Lookup.Region'.
3. Add an entry with Code key and Decode value as 'AE'. You can now create an e-mail definition with language ar and region AE.

6.4.19 Translated Justification is Not Displayed in Access Policy-Based Resource Provisioning Request Detail

When an access policy with approval is created, it generates a resource provisioning request that is subject to approval. In the request details page in Self Service or Advanced Administration, the translated request justification according to the locale setting by the user is not displayed. The justification is displayed in the default server locale.

6.4.20 Additional Single Quotes Displayed in GTC Reconciliation Mapping Page for French UI

When you set the Oracle Identity Manager Administrative and User Console locale to French, select the Provisioning and Reconciliation checkboxes while creating a Generic Technology Connector (GTC), and map the reconciliation fields in the page for modifying mapping fields, a message is displayed with two single quotes. You can ignore the single quotes because this is benign and has no effect on functionality.

6.4.21 Not Allowing to Enter Design Console Password When Server Locale is Set to Simple Chinese, Traditional Chinese, Japanese, or Korean

When you set the server locale to Simple Chinese, Traditional Chinese, Japanese, or Korean, and start the Design Console, you are not allowed to enter the password to login to the Design Console.

To workaround this issue:

1. Kill all scim processes. To do so, run the following command:

```
kill `pgrep scim`
```

2. Edit the scim config file. To do so:
   a. Search for the following line:

      /FrontEnd/X11/Dynamic = ...

   b. Enter true as the value, as shown:

      /FrontEnd/X11/Dynamic = true

      Note: If this line does not exist, then enter:

      /Frontend/X11/Dynamic = true

   c. Save the file.
3. Log out of the VNC viewer.
4. Restart the VNC server and log in again. You can now enter the password for the Design Console.

6.4.22 Bidirectional Text Not Supported in Nexaweb Pages

The Nexaweb pages that open from the Oracle Identity Manager Administrative and User Console do not support bidirectional text. For example, when you select any of the languages that are written from right to left, such as Arabic or Hebrew, and click **Install Connector** on the Welcome page, search for a connector, click **Upgrade**, and then proceed to step 13 of the Connector Upgrade wizard, the text in the page is not displayed from right to left.

6.4.23 Do Not Modify Oracle Identity Manager Predefined System Properties in Non-English Locale

When the user preference language for the Administrative and User Console is not English, and you update the value of a predefined system property in Oracle Identity Manager, translated property name and keyword are written in the PTY table. Therefore, on searching for system properties in the Administrative and User Console, this system property is not found.

6.4.24 Error Generated When Translated String for System Property Name Exceeds Maximum Allowed Length in PTY_NAME Column

When you try to set the value of a system property in a Western language UI, such as French, and if the translation string length exceeds the maximum allowed length, which is 80 characters, in the PTY_NAME column of the PTY table, then an error is generated.

6.4.25 Password Notification is Not Sent if User Login Contains Special Characters

For a user entity created with valid e-mail address in LDAP, if the User Login contains the German beta character, then the notification message is not sent on running LDAP user create/update full reconciliation.

6.4.26 Reset Password Fails if User Login Contains Lowercase Special Characters

In a Oracle Identity Manage deployment with LDAP synchronization enabled, if the User Login contains special characters such as Turkis dotted I, dotless i, German beta, and Greek sigma in lowercase format, then the reset password does not work.

To workaround this issue, use uppercase User Login to reset password because User Login is not case-sensitive in Oracle Identity Manager.

6.4.27 Email Notification Not Send Per Preferred Locale

When provisioning a resource to a user, the provisioned user and the user's manager receive the email notification in the locale as specified for user.language and user.country instead of their preferred locale.

6.4.28 Help Contents Displayed in English on Non-English Browsers

On non-English Web browsers, clicking the **Help** link on the top-right corner of the Oracle Identity Manager Self Service, Identity Administration, or Advanced Administration opens the help window, but always displays the on-line help contents in English.

6.5 Documentation Errata

Documentation Errata: Currently, there are no documentation issues to note.

7

Oracle Internet Directory

This chapter describes the following issues associated with Oracle Internet Directory:

7.1 General Issues and Workarounds

This section describes the following general issues and workarounds associated with Oracle Internet Directory:

7.1.1 Cloned Oracle Internet Directory Instance Fails or Runs Slowly

In a cloned Oracle Internet Directory environment, undesired host names can cause errors, failures, or performance degradation.

This problem can occur when you clone an Oracle Internet Directory instance and the cloned target instance gets undesired host names from the source instance. Some of these hosts might be outside of a firewall or otherwise inaccessible to the target instance.

The cloned Oracle Internet Directory instance assumes it is in a clustered environment and tries to access the undesired hosts for notifications and other changes. However, the cloned instance cannot access some of the hosts and subsequently fails, returns errors, or runs slowly.

For example, this problem can occur during the following operations for a cloned Oracle Internet Directory target instance:

- Running the `faovmdeploy.sh createTopology` command to create an Oracle Virtual Machine (VM)
- Deploying Enterprise Manager agents in different Oracle Virtual Machines

To fix this problem, remove the undesired host names from the cloned Oracle Internet Directory instance, as follows:

1. Set the required environment variables. For example:

```
export ORACLE_INSTANCE=/u01/oid/oid_inst
export ORACLE_HOME=/u01/oid/oid_home
export PATH=$ORACLE_HOME/bin:$ORACLE_INSTANCE/bin:$PATH
export TNS_ADMIN=$ORACLE_INSTANCE/config
```

2. Connect to the Oracle Database and delete the entries with the undesired Oracle Internet Directory host names. For example, in the following queries, substitute the undesired host name for *sourceHostname*:

```
sqlplus ods@oiddb
delete from ods_shm where nodename like '%sourceHostname%';
delete from ods_shm_key where nodename like '%sourceHostname%';
delete from ods_guardian where nodename like '%sourceHostname%';
delete from ods_process_status where hostname like '%sourceHostname%';
commit;
```

3. Stop and then restart the cloned Oracle Internet Directory component. For example:

```
opmnctl stopproc ias-component=oid1
opmnctl startproc ias-component=oid1
```

4. Find the `cn` entries with the undesired Oracle Internet Directory host names. For example:

```
ldapsearch -h oid_host -p oid_port -D cn=orcladmin -w admin_password -b
"cn=subregistrysubentry" -s sub "objectclass=*" dn
cn=oid1_1_hostName1,cn=osdldapd,cn=subregistrysubentry
cn=oid1_1_hostName2,cn=osdldapd,cn=subregistrysubentry
cn=oid1_1_myhost.example.com,cn=osdldapd,cn=subregistrysubentry
```

5. From the results in the previous step, remove the entries with the undesired host names. For example:

```
ldapdelete h oid_host -p oid_port -D cn=orcladmin -w admin_password
"cn=oid1_1_hostName1,cn=osdldapd,cn=subregistrysubentry"
```

```
ldapdelete h oid_host -p oid_port -D cn=orcladmin -w admin_password
"cn=oid1_1_hostName2,cn=osdldapd,cn=subregistrysubentry"
```

6. Verify that the undesired host names are removed. For example:

```
ldapsearch h oid_host -p oid_port -D cn=orcladmin -w admin_password -b
"cn=subregistrysubentry" -s sub "objectclass=*" dn
cn=oid1_1_myhost.example.com,cn=osdldapd,cn=subregistrysubentry
```

See Also: "Cloning Oracle Fusion Middleware" in the *Oracle Fusion Middleware Administrator's Guide*.

7.1.2 Oracle Internet Directory Fails to Start on Solaris SPARC System Using ISM

Oracle Internet Directory fails to start on the following Oracle Solaris SPARC system using Intimate Shared Memory (ISM): `5.11 11.1 sun4v sparc sun4v`

As a workaround for this problem, set the following values, as shown in the next procedure:

- Set the total amount of operating system physical locked memory allowed (`project.max-locked-memory`) for Oracle Internet Directory to 2 GB or higher so that the value aligns with the supported page sizes. The `pagesize -a` command lists all the supported page sizes on Solaris systems.
- Set the `orclecachemaxsize` attribute to less than the `project.max-locked-memory` and ensure that the value aligns with the OS supported page sizes. For example, set the value to 256 MB.

In the following procedure, it is assumed that the Oracle Internet Directory services are managed by an operating system user named "oracle":

1. Log in to the Solaris SPARC system as the root user.
2. Check the project membership of the OID user.

   If the OID user belongs to the default project:

   a. Create a new project with the value of maximum locked memory set to 2 GB or higher, and associate the OID user with the newly created project. On Solaris 10 and 11, project id 3 represents the default project. For example:

```
# id -p oracle
uid=2345(oracle) gid=529(dba) projid=3(default)
# projadd -p 150 -K "project.max-locked-memory=(priv,2G,deny)" oidmaxlkmem
# usermod -K project=oidmaxlkmem oracle
```

   b. Verify that the value for the resource control `project.max-locked-memory` was set to 2 GB, as expected. For example:

```
# su - oracle

$ id -p oracle
uid=2345(oracle) gid=529(dba) projid=150(oidmaxlkmem)

$ prctl -n project.max-locked-memory -i project 150
project: 150: oidmaxlkmem
NAME    PRIVILEGE       VALUE    FLAG   ACTION                       RECIPIENT
project.max-locked-memory
        privileged      2.00GB      -   deny                                 -
        system          16.0EB    max   deny                                 -
```

If the OID user belongs to a non-default project:

a. Modify the corresponding project to include the `project.max-locked-memory` resource control and set the value to 2 GB or higher. For example:

```
# id -p oracle
uid=2345(oracle) gid=529(dba) projid=125(oraproj)

# projmod -a -K "project.max-locked-memory=(priv,2G,deny)" oraproj
```

b. Verify that the value for the resource control `project.max-locked-memory` was set to 2 GB, as expected. For example:

```
# projects -l oraproj
oraproj
        projid : 125
        comment: ""
        users  : (none)
        groups : (none)
        attribs: project.max-locked-memory=(priv,2147483648,deny)
                 project.max-shm-memory=(priv,34359738368,deny)

# su - oracle
$ id -p
uid=2345(oracle) gid=529(dba) projid=125(oraproj)

$ prctl -n project.max-locked-memory -i project 125
project: 125: oraproj
NAME    PRIVILEGE       VALUE    FLAG   ACTION                       RECIPIENT
project.max-locked-memory
        privileged      2.00GB      -   deny                                 -
        system          16.0EB    max   deny                                 -
```

3. Set the entry cache maximum size (`orclecachemaxsize` attribute) to a value that is less than the maximum locked memory size allowed by the OS and that aligns with the OS supported page sizes.

For example, using SQL*Plus, set the value to 256 MB:

```
sqlplus ods@oiddb
update ds_attrstore set attrval='256m'
  where entryid=940 and attrname='orclecachemaxsize';
commit;
```

4. Run the `config.sh` script to configure Oracle Internet Directory.

7.1.3 Custom Audit Policy Settings Fail When Set Through Enterprise Manager

If you set custom Audit Policy Settings for Oracle Internet Directory through 11g Oracle Enterprise Manager Fusion Middleware Control and select audit Custom events with Failures Only, no audit logs are generated and the audit process for failure events fails. Subsequently, other audit events are not logged later, even if the Audit Policy Settings are changed to a different value such as Low, Medium, or High.

To make auditing function again through Enterprise Manager, select a default policy or a policy with custom events other than All Failures and then recycle the Oracle Internet Directory server processes.

Alternatively, you can set custom audit policies using LDAP command-line tools such as `ldapmodify`. For more information, see Section 23.4, "Managing Auditing from the

Command Line" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

7.1.4 Deleting Mandatory `attributeTypes` Referenced by `objectClass` is Successful

If you delete a mandatory `attributeTypes` under the Oracle Internet Directory schema that is referenced by an `objectClass` in the schema, no error is returned and the `attributeTypes` is deleted successfully.

This problem also occurs for a DN entry created using the `objectClass` that uses the mandatory `attributeTypes`. The mandatory attribute is missing from the DN entry without any notice when it is deleted from the schema.

7.1.5 Oracle Unified Directory 11.1.2.0 `orclguid` Attribute is Not Mapped for Server Chaining

If you configure Oracle Internet Directory server chaining for Oracle Unified Directory 11.1.2.0 and then search for users, the `orclguid` attribute is missing from the search results.

The `orclguid` attribute is missing because Oracle Unified Directory uses the iplanet default mapping (`cn=oidsciplanet,cn=oid server chaining,cn=subconfigsubentry`), and the default iplanet mapping does not have `orclguid` mapped.

7.1.6 ODSM is Not Displaying Online Help Correctly in Internet Explorer 11

In Internet Explorer 11, the Oracle Directory Services Manager (ODSM) online Help does not display properly. Instead of showing the left pane with the navigation tree and the right pane with the Help contents, ODSM displays only links.

7.1.7 ODSM Browser Window Becomes Unusable

Under certain circumstances, after you launch ODSM from Fusion Middleware Control, then select a new ODSM task, the browser window might become unusable. For example, the window might refresh repeatedly, appear as a blank page, fail to accept user input, or display a null pointer error.

As a workaround, go to the URL: `http://`*`host`*`:`*`port`*`/odsm`, where *host* and *port* specify the location where ODSM is running, for example, `http://myserver.example.com:7005/odsm`. You can then use the ODSM window to log in to a server.

7.1.8 Bulkmodify Might Generate Errors

If Oracle Internet Directory is using Oracle Database 11*g* Release 1 (11.1.0.7.0), you might see `ORA-600` errors while performing `bulkmodify` operations. To correct this problem, apply the fixes for Bug 7019313 and Bug 7614692 to the Oracle Database.

7.1.9 Turkish Dotted I Character is Not Handled Correctly

Due to a bug, Oracle Internet Directory cannot handle the upper-case dotted I character in the Turkish character set correctly. This can cause problems in Oracle Directory Services Manager and in command-line utilities.

7.1.10 OIDCMPREC Might Modify Operational Attributes

By default, the `oidcmprec` tool excludes operational attributes during comparison. That is, `oidcmprec` does not compare the operational attributes values in source and destination directory entries. During reconciliation of user defined attributes however, operational attributes might be changed.

7.1.11 OIDREALM Does Not Support Realm Removal

The `oidrealm` tool supports creation, but not deletion, of a realm. A procedure for deleting a realm is provided in Note 604884.1, which is available on My Oracle Support at `https://support.oracle.com/`.

7.1.12 Apply Patch to Oracle Database 11.2.0.1.0 to Fix Purge Job Problem

If you use Oracle Database 11.2.0.1.0 with Oracle Internet Directory, apply Patch 9952216 (11.2.0.1.3 PSU) to the Oracle Database after you install Oracle Internet Directory:

Without the patch, a purge jobs operation does not function properly, and these symptoms can occur:

- Oracle Internet Directory change logs do not get purged, and the purge log shows ORA-23421 errors.
- Executing change log purge jobs with `orclpurgenow` set to 1 hangs.

7.1.13 SQL of OPSS ldapsearch Might Take High %CPU

The SQL of an OPSS one level `ldapsearch` operation, with filter "`orcljaznprincipal=`*`value`*" and required attributes, might take unreasonably high %DB CPU. If this search performance impacts the overall performance of the machine and other processes, you can alleviate the issue by performing the following steps in the Oracle Database:

1. Log in to the Oracle Database as user `ODS` and execute the following SQL:

```
BEGIN
DBMS_STATS.GATHER_TABLE_STATS(OWNNAME=>'ODS',
                              TABNAME=>'CT_ORCLJAZNPRINCIPAL',
                              ESTIMATE_PERCENT=>DBMS_STATS.AUTO_SAMPLE_SIZE,
                              CASCADE=>TRUE);
END;
/
```

2. Flush the shared pool by using the ALTER SYSTEM statement, as described in the *Oracle Database SQL Language Reference*.

7.1.14 If you Start the Replication Server by Using the Command Line, Stop it Using the Command Line

If you start the replication server by using the command line, stop it by using the command line. If you attempt to stop it by using Oracle Enterprise Manager Fusion Middleware Control, the attempt fails.

> **See Also:** Note 1313395.1 on My Oracle Support (formerly MetaLink): `https://support.oracle.com`

7.1.15 ODSM Problems in Internet Explorer 7

The ODSM interface might not appear as described in Internet Explorer 7.

For example, the **Logout** link might not be displayed.

If this causes problems, upgrade to Internet Explorer 8 or 9 or use a different browser.

7.2 Configuration Issues and Workarounds

This section describes the following configuration issues and workarounds associated with Oracle Internet Directory:

- Section 7.2.1, "Re-Create Wallet After Moving Oracle Internet Directory from Test to Production"

7.2.1 Re-Create Wallet After Moving Oracle Internet Directory from Test to Production

If you configure Oracle Internet Directory to use SSL in server authentication mode or mutual authentication mode on your test machine, and then move Oracle Internet Directory to a production machine, re-create the Oracle Internet Directory wallet on the production machine.

The old wallet contains the host name of the original machine as the DN in the certificate. This host name in the DN is not changed during the test to production move. Re-create the wallet on the production machine to avoid SSL communication issues.

7.3 Documentation Errata

This section describes the following documentation errata topics:

- Section 7.3.1, "Oracle Internet Directory VM Template is Not Available"
- Section 7.3.2, "Description of the `orclrevpwd` Attribute Needs Clarification"
- Section 7.3.3, "LDAP Commands Do Not Support the `-k|-K` Option"
- Section 7.3.4, "Description of the `orclOIDSCExtGroupContainer` Attribute Needs Clarification"
- Section 7.3.5, "Setting Up LDAP Replication Needs Clarification"
- Section 7.3.6, "Password Expired Response Control is Not Documented"
- Section 7.3.7, "Configuring the SSO Server for ODSM Integration Needs Clarification"
- Section 7.3.8, "Determining Expired Users in Oracle Internet Directory"
- Section 7.3.9, "New Superuser Account Must be Direct Member of `DirectoryAdminGroup` Group"
- Section 7.3.10, "SSL Authentication Mode 1 and Anonymous SSL Ciphers Need Clarification"
- Section 7.3.11, "Documentation of Replication Server Control and Failover is Incomplete"
- Section 7.3.12, "Server Restart After Adding an Encrypted Attribute is Not Documented"
- Section 7.3.13, "PASSWORD_VERIFY_FUNCTION Must be Set to NULL to Work with RCU is Not Documented"

7.3.1 Oracle Internet Directory VM Template is Not Available

In the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*, Appendix R describes how to use the Oracle Internet Directory VM template. However, this template is not available for Oracle Internet Directory 11g Release 1 (11.1.1.7.0).

As a workaround, install Oracle Internet Directory, as described in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

7.3.2 Description of the `orclrevpwd` Attribute Needs Clarification

In the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*, the description of the `orclrevpwd` attribute in the "Managing Password Verifiers " chapter needs clarification. The "Introduction to Password Verifiers for Authenticating to the Directory" section should include the following information.

Oracle Internet Directory stores the user password in a reversible encrypted format in the `orclrevpwd` configuration attribute. The `orclrevpwd` attribute is generated only if the `orclpwdencryptionenable` attribute in the password policy entry is set to 1.

The `orclrevpwd` attribute is maintained securely within Oracle Internet Directory server and cannot be queried, even if you modify the attribute's access control policies (ACIs). Oracle Directory Integration Platform, however, is allowed to query the `orclrevpwd` attribute so that password synchronization can function.

7.3.3 LDAP Commands Do Not Support the `-k|-K` Option

In the *Oracle Fusion Middleware Reference for Oracle Identity Management*, Chapter 3, "Oracle Internet Directory Data Management Tools," documents the `-k|-K` option for LDAP commands. However, this option is not valid for the LDAP commands and should not be used.

7.3.4 Description of the `orclOIDSCExtGroupContainer` Attribute Needs Clarification

In the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*, the description of the `orclOIDSCExtGroupContainer` attribute in the "Configuring Server Chaining" chapter needs clarification.

The description states that this attribute "is optional if the external user container and the external group container are the same." However, the attribute is required, and the description should include the following information:

If the external user container and the external group container are the same (that is, groups in the external directory server are stored in the same container as the users), the value for the `orclOIDSCExtGroupContainer` attribute must be the same as the value used for the user container (`orclOIDSCExtUserContainer` attribute).

7.3.5 Setting Up LDAP Replication Needs Clarification

The *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*, Chapter 40, "Setting Up Replication," does not document the following requirements.

To setup replication for a directory that has more than 100,000 entries, you must use the command-line tools (`ldifwrite` and `bulkload`). Use the Replication Wizard in Oracle Enterprise Manager Fusion Middleware Control (automatic bootstrapping method) only for a directory that has fewer than 100,000 entries.

If you have a deployment with a combination of Oracle Internet Directory 10g nodes and 11gR1 nodes, replication from the 10g node to an 11gR1 node must be setup before replication between the 11gR1 nodes is setup. For example, consider a deployment as follows:

- Two Oracle Internet Directory 10g nodes with a supplier node and consumer node
- Two new Oracle Internet Directory 11gR1 nodes (nodes 1 and 2) with LDAP multimaster replication

To setup replication for this deployment:

1. Setup LDAP one-way replication from one of the 10g nodes to 11gR1 node 1.
2. Setup replication bootstrap (if fewer than 100,000 entries) and then start the replication server on the 11gR1 node 1. (If the diretory has more than 100,000 entries, use the command-line tools.)
3. When the replication is complete, setup LDAP multimaster replication between 11gR1 node 1 and node 2.
4. Setup the replication bootstrap (if fewer than 100,000 entries) on 11gR1 node 2 and then start the replication server.

7.3.6 Password Expired Response Control is Not Documented

Both the *Oracle Fusion Middleware Reference for Oracle Identity Management* and the *Oracle Fusion Middleware Application Developer's Guide for Oracle Identity Management* do not document the Oracle Internet Directory password expired response control:

- **Object Identifier**: 2.16.840.1.113894.1.8.20
- **Name**: OID_PWDEXPIRED_CONTROL
- **Description**: Password policy control. The response control that the server sends when the password has expired, there are no grace logins remaining, and the client sends a request control.

7.3.7 Configuring the SSO Server for ODSM Integration Needs Clarification

In the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*, Section 7.4.3, "Configuring the SSO Server for ODSM Integration," does not document that to improve performance for SSO-ODSM integration, you should configure the ODSM URLs as follows:

- Protected: `/odsm/odsm-sso.jsp`
- Unprotected: `/odsm/faces/odsm.jspx`
- Excluded: `/odsm/.../`

Setting the CSS, JavaScript, and graphics (`/odsm/.../`) files to excluded prevents these files from being validated by Oracle Access Manager, which can improve the performance of your deployment.

7.3.8 Determining Expired Users in Oracle Internet Directory

The *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* does not fully explain the concept of expired users and how to determine if a user is in the expired state.

In some situations, you might want to determine expired users and then take a specific action, such as deleting those users from the directory.

> **Note:** Oracle Internet Directory expired users are not indicated by a specific attribute. An expired user is in a transient state that depends on the system time, the maximum inactive time allowed, and the user's last successful login time. The expired state is determined during a bind or password compare operation for the user.

To determine the expired users, your Oracle Internet Directory deployment must be configured as follows:

- The tracking of each user's last successful login time must be enabled by setting the `orclPwdTrackLogin` attribute to 1.
- The `orclpwdmaxinactivitytime` attribute must be set to a value other than 0 (the default). This attribute specifies the inactive time in seconds before a user's account is automatically considered to be expired.

To determine if a user's account is considered to be expired:

1. Determine the time stamp of the user's last successful login from the `orcllastlogintime` attribute.
2. Subtract the user's `orcllastlogintime` value from the current system time. If the result is greater than the `orclpwdmaxinactivitytime` value, then the user is considered to be in the expired state.
3. If you wish, delete the expired user from the directory.

For more information, see the "Managing Password Policies" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

7.3.9 New Superuser Account Must be Direct Member of `DirectoryAdminGroup` Group

In the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*, Section 12.6, "Creating Another Account With Superuser Privileges," does not mention that a new superuser account must be a direct member of the `DirectoryAdminGroup` group to use all Oracle Directory Services Manager (ODSM) features.

To use all ODSM features including the Security and Advanced tabs, a new superuser account must be a direct member of the `DirectoryAdminGroup` group. The new superuser account cannot be a member of a group that is in turn a member of the `DirectoryAdminGroup` group. In this configuration, the superuser would be able to access only the ODSM Home, Schema, and Data Browser tabs.

7.3.10 SSL Authentication Mode 1 and Anonymous SSL Ciphers Need Clarification

In the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*, the first bullet of the note in Section 27.1.3, "SSL Authentication Modes," mentions that you must have at least one Oracle Internet Directory server instance configured for the

default authentication mode and anonymous SSL ciphers. This statement is true only for specific deployments.

The first bullet of the note should be revised as follows:

- By default, the SSL authentication mode is set to 1 (encryption only, no authentication).

  If you are using Oracle Delegated Administration Services 10*g* or other client applications such as legacy versions of Oracle Forms and Oracle Reports that expect to communicate with Oracle Internet Directory on an encrypted SSL port configured for anonymous SSL ciphers, then at least one Oracle Internet Directory server instance must be configured for this default authentication mode.

  Otherwise, authentication mode 1 and anonymous SSL ciphers are not required for Oracle Internet Directory to function. The type of SSL ports that are made available and the ciphers that the SSL port will accept depend on your specific deployment requirements.

7.3.11 Documentation of Replication Server Control and Failover is Incomplete

The *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* does not fully describe the replication server (oidrepld) process control and failover in an Oracle Maximum Availability Architecture (MAA), including how to enable failover by setting the `orclfailoverenabled` attribute.

The `orclfailoverenabled` attribute is an OID Monitor configuration entry (`"cn=configset,cn=oidmon,cn=subconfigsubentry"`) that configures failover.

This attribute specifies the failover time in minutes before the OID Monitor will start failed processes on a surviving node. The default failover time is 5 minutes. A value of zero (0) disables failover for Oracle Internet Directory processes.

Additional information is provided in Note 1538250.1, which is available on My Oracle Support at:

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

> **See Also:** The "Understanding Process Control of Oracle Internet Directory Components" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

7.3.12 Server Restart After Adding an Encrypted Attribute is Not Documented

The *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* does not document that if you add an encrypted attribute to the list of sensitive attributes, you must restart the Oracle Internet Directory server instance for the new attribute to be added to the new list of sensitive attributes and recognized by the server.

> **Note:** The attributes in Table 28-1 "Sensitive Attributes Stored in orclencryptedattributes" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* are intended for use only by Oracle. Do not add to or modify the attributes shown in this table unless you are requested to do so by Oracle Support.

For more information, see the "Configuring Data Privacy" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

7.3.13 PASSWORD_VERIFY_FUNCTION Must be Set to NULL to Work with RCU is Not Documented

The *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* does not document that for Oracle Internet Directory to work with the Repository Creation Utility (RCU) for Oracle database version 11.2.x, the default PASSWORD_VERIFY_FUNCTION clause in the database must be set to NULL (which is the default value).

7.3.14 Setting Up Oracle Internet Directory SSL Mutual Authentication

Neither the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* nor the *Oracle Fusion Middleware Administrator's Guide* describes how to set up Oracle Internet Directory SSL Client and Server Authentication. This information is provided in Note 1311791.1, which is available on My Oracle Support at:

https://support.oracle.com/

7.3.15 Replication Instructions in Tutorial for Identity Management are Incomplete

In the *Tutorial for Identity Management*, which is linked from *Getting Started with Oracle Identity Management*, Chapter 3, "Setting up Oracle Internet Directory Replication," is missing important information.

Specifically, the instructions do not work unless the new consumer node is empty.

For more information, see Section 40.1.7, "Rules for Configuring LDAP-Based Replication," in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

8

Oracle Platform Security Services

This chapter describes notes on topics associated with Oracle Platform Security Services (OPSS), in the following sections:

- Section 8.1, "Configuration Issues and Workarounds"
- Section 8.2, "Documentation Errata"

The following documents are relevant to topics included in this chapter:

- *Oracle Fusion Middleware Security Guide*
- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware Administrator's Guide for Authorization Policy Manager*

8.1 Configuration Issues and Workarounds

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

- Section 8.1.1, "Oracle Fusion Middleware Audit Framework"
- Section 8.1.2, "Trailing '\n' Character in Bootstrap Key"
- Section 8.1.3, "Users with Same Name in Multiple Identity Stores"
- Section 8.1.4, "Script listAppRoles Outputs Wrong Characters"
- Section 8.1.5, "Propagating Identities over the HTTP Protocol"
- Section 8.1.6, "Pool Configuration Missing in Identity Store"

8.1.1 Oracle Fusion Middleware Audit Framework

This section describes configuration issues for the Oracle Fusion Middleware Audit Framework. It contains these topics:

- Section 8.1.1.1, "Configuring Auditing for Oracle Access Manager"
- Section 8.1.1.2, "Audit Reports do not Display Translated Text in Certain Locales"
- Section 8.1.1.3, "Audit Reports Always Display in English"
- Section 8.1.1.4, "Audit Store Does not Support Reassociation through EM"
- Section 8.1.1.5, "OWSM Audit Events not Audited"

8.1.1.1 Configuring Auditing for Oracle Access Manager

Although Oracle Access Manager appears as a component in Oracle Enterprise Manager Fusion Middleware Control, you cannot configure auditing for Oracle Access Manager using Fusion Middleware Control.

8.1.1.2 Audit Reports do not Display Translated Text in Certain Locales

The standard audit reports packaged with Oracle Business Intelligence Publisher support a number of languages for administrators. Oracle Business Intelligence Publisher can start in different locales; at start-up, the administrator can specify the language of choice by setting the preferred locale in Preferences.

Due to this bug, if Oracle Business Intelligence Publisher is started on any of these 3 locales:

- zh_CN (simplified chinese)
- zh_TW (traditional chinese)
- pt_BR (portuguese brazilian)

then users cannot see the report in that locale (the entire report including labels, headers, titles and so on appears in English), while the other locales display the translated text as expected. For example, when Oracle Business Intelligence Publisher is started in zh_CN, the text cannot be seen in zh_CN even though the preferred locale is set to zh_CN; information is displayed in English.

This issue will be fixed in a future release of Oracle Business Intelligence Publisher.

8.1.1.3 Audit Reports Always Display in English

The standard audit reports packaged with Oracle Business Intelligence Publisher support a number of languages.

Due to this bug, report titles and descriptions are displayed in English even when they have been translated.

This issue will be fixed in a future release of Oracle Business Intelligence Publisher.

8.1.1.4 Audit Store Does not Support Reassociation through EM

In Release 11gR1 (11.1.1.6.0), if you reassociated security stores through the Fusion Middleware Control Enterprise Manager (EM) console, most stores (policy store, credential store and so on) moved except for the audit store. This is because the audit store did not support reassociation through the console, only through the WLST command `reassociateSecurityStore`.

In a situation where the original migration from Release 11gR1 (11.1.1.6.0) to Release 11gR1 (11.1.1.7.0) was done through EM, this leaves the audit repository as file-based. You can use the following workaround to move all security store data to LDAP/DB in order to enable audit:

In the PS5 environment, run WLST command `reassociateSecurityStore` with a different `jpsroot` node. This effects an OID-to-OID directory reassociation and any existing data also gets migrated to the new node. After you take this action, audit data will no longer be file based and jps-config will have the new node.

8.1.1.5 OWSM Audit Events not Audited

In Release 11.1.1.7, due to a bug, audit events are not logged for Web Services Manager (OWSM) after auditing is configured for the component.

To resolve this issue, proceed as follows:

1. Register the OWSM components AGENT, PM-EJB with the audit service using the `registerAudit` WLST command:

   a. `registerAudit(xmlFile="$ORACLE_COMMON/modules/oracle.iau_11.1.1/components/OWSM-AGENT/component_events.xml", componentType="AGENT")`

   b. `registerAudit(xmlFile="$ORACLE_COMMON/modules/oracle.iau_11.1.1/components/OWSM-PM-EJB/component_events.xml", componentType="PM-EJB")`

2. Get the list of components using the `listAuditComponents` WLST command; for example, this command writes the list of components to a file named `complist.txt`:

   ```
   listAuditComponents(fileName = "/tmp/complist.txt")
   ```

3. For each component in the list, execute the WLST command `setAuditPolicy` as follows:

   ```
   setAuditPolicy(componentType="<component name from complist.txt>",
   filterPreset="None")
   ```

For details about syntax and usage of these commands, see *Oracle Fusion Middleware Application Security Guide*, part number E10043-11, Appendix C Oracle Fusion Middleware Audit Framework Reference.

8.1.2 Trailing '\n' Character in Bootstrap Key

In 11gR1, the process that reassociates XML to LDAP stores creates a bootstrap key with the trailing new line character '\n', or its equivalent code '&#xA'. This key value is written in the file `jps-config.xml` and stored in the wallet. In both places, the key value contains the trailing character '\n'.

When reusing that same wallet in 11gR1 PS1, upon retrieving the bootstrap key, the system trims out the trailing '\n' character; but the key value in the wallet, however, still contains the trailing character, a situation that leads to errors since the requested and stored key values no longer match.

To resolve this issue, proceed as follows:

1. Use the WLST command `modifyBootStrapCredential` to reprovision wallet credentials without trailing '\n'. For details on the command usage, see section 9.5.2.5 in the *Oracle Fusion Middleware Security Guide*.

2. Manually edit the file `jps-config.xml` and remove the trailing characters '&#xA' from any bootstrap key.

This problem arises only in the scenario above, namely, when an 11gR1 wallet is reused in 11gR1 PS1; in particular, when reassociating in an 11gR1 PS1 environment, the above trailing character is not an issue.

8.1.3 Users with Same Name in Multiple Identity Stores

If a user name is present in more than one LDAP repositories and the property virtualize is set to use LibOVD, then the data in only one of those repositories is returned by the User and Role API when that name is queried.

8.1.4 Script listAppRoles Outputs Wrong Characters

On Linux and Windows platforms, when the locale is set to non-UTF8 locales, such as `fr_FR_iso88591`, the OPSS script `listAppRoles` may wrongly output the character '?' instead of the expected character.

8.1.5 Propagating Identities over the HTTP Protocol

This section includes the following additions, corrections, and new information in the following sections:

- Addition to Section Propagating Identities over the HTTP Protocol
- Correction to Section Client Application Code Sample
- Correction to Section Keystore Service Configuration
- Updating the Trust Service Configuration Parameters

8.1.5.1 Addition to Section Propagating Identities over the HTTP Protocol

The following new information belongs in section 19.3.1.2:

The out of box configuration assumes that the token issuer name and the key alias is based on the WebLogic server name. Note that the key alias server name on WebSphere is set based on the WebSphere server root. For example, if the server root is `$T_WORK/middleware/was_profiles/DefaultTopology/was_as/JrfServer` then the server name is set to `JrfServer`. To change the default value, use the procedures explained in section 19.3.12.

8.1.5.2 Correction to Section Client Application Code Sample

The following sample illustrates a client application; note that the file `jps-api.jar` and OSDT jars `osdt_ws_sx.jar, osdt_core.jar, osdt_xmlsec.jar, osdt_saml2.jar` must be included the class path for the code sample to compile.

8.1.5.3 Correction to Section Keystore Service Configuration

Assuming that the WebLogic server name is `jrfServer_admin`, the following command illustrates the creation of the keystore, represented by the generated file `default-keystore.jks`.

8.1.5.4 Updating the Trust Service Configuration Parameters

The information in this section is new and it explains how to modify the trust service configuration parameters in the file `jps-config.xml` with a script.

Out-of-the-box the values of the parameters `trust.aliasName` and `trust.issuerName` are set to the WebLogic server name. To modify their values to deployment-specific values, use a script like the following:

```
import sys

wlsAdmin = 'weblogic'
wlsPwd ='password_value'
wlUrl='t3://localhost:7001'
issuer= 'issuer'
alias = 'alias'

print "OPSS Trust Service provider configuration management script.\n"

instance = 'trust.provider'
```

```
name = 'trust.provider.embedded'
cfgProps = HashMap()
cfgProps.put("trust.issuerName", issuer)
cfgProps.put("trust.aliasName", alias)
pm = PortableMap(cfgProps);

connect(wlsAdmin, wlsPwd, wlUrl)
domainRuntime()

params = [instance, name, pm.toCompositeData(None)]
sign = ["java.lang.String", "java.lang.String",
"javax.management.openmbean.CompositeData"]
on = ObjectName("com.oracle.jps:type=JpsConfig")
mbs.invoke(on, "updateTrustServiceConfig", params, sign)
mbs.invoke(on, "persist", None, None)

print "Done.\n"
```

8.1.6 Pool Configuration Missing in Identity Store

On the WebSphere Application Server, the out-of-the-box configuration file `jps-config.xml` is missing an entry for a property of the identity store. When the identity store, added at post-installation, is an LDAP-based identity store, the following property must be manually inserted in the `jps-config.xml` file within the identity store service instance element:

```
<property name="CONNECTION_POOL_CLASS"
          value="oracle.security.idm.providers.stdldap.JNDIPool"/>
```

To work around this issue, proceed as follows:

1. Shut down the server.
2. Open the file `was_profile_dir/config/cells/cell_name/fmwconfig/jps-config.xml` for edit, where *was_profile_dir* and *cell_name* stand for the profile directory name and cell name on your system.
3. Insert the missing property `CONNECTION_POOL_CLASS` into the configuration of the identity store service instance.
4. Save the file and restart the server.

8.2 Documentation Errata

This section contains corrections to documentation errors. It includes the topic:

8.2.1 Updated Configuration for Role Category

This note contains the correct configuration of a role category as described in Section 2.8 "The Role Category" in the *Oracle Fusion Middleware Application Security Guide*, part number E10043-10.

The configuration of the element `<role-category>` in the `jazn-data.xml` illustrated in section 2.8 should be replaced with the following:

```
<app-roles>
  <app-role>
    <name>AppRole_READONLY</name>
    <display-name>display name</display-name>
    <description>description</description>
    <class>oracle.security.jps.service.policystore.ApplicationRole</class>
    <extended-attributes>
      <attribute>
        <name>ROLE_CATEGORY</name>
        <values>
          <value>RC_READONLY</value>
        </values>
      </attribute>
    </extended-attributes>
  </app-role>
</app-roles>
<role-categories>
  <role-category>
    <name>RC_READONLY</name>
    <display-name>RC_READONLY display name</display-name>
    <description>RC_READONLY description</description>
  </role-category>
</role-categories>
```

The important point about this correction is the following:

- The members of a role category are *not* configured within the `<role-category>` element but within the element `<extended-attributes>` of the corresponding application role.

8.2.2 Correct setAuditRepository Command Reference Example

This note corrects a typo in Section C.4.5 "setAuditRepository" in the *Oracle Fusion Middleware Application Security Guide*, part number E10043-11.

In the example line:

```
setAuditRepository(switchToDB='true',dataSourceName='jdbcAuditDB',interval='14')
```

change '`jdbcAuditDB`' to read '`jdbc/AuditDB`'.

8.2.3 Demo CA Certificate not for Production Use

In the *Oracle Fusion Middleware Application Security Guide*, Part Number E10043-11, 11.1.3 Domain Trust Store, insert the following caution note at the top of the section:

Caution: The Demo CA has a well known hard-coded private key, Care should be taken not to trust the certificates signed by the Demo CA. As such, the Demo CA certificate in the trust store should not be used in production. It should be removed from the domain trust store in production.

8.2.4 Incorrect Link to ILM Content

In the *Oracle Fusion Middleware Application Security Guide*, part number E10043-12, in the chapter Configuring and Managing Auditing, section titled "Tiered Archival" contains an incorrect link for Oracle Information Lifecycle Management (ILM).

Change the link to read:

http://www.oracle.com/technetwork/database/enterprise-edition/index-090321.html

8.2.5 Incorrect Table Title in Appendix C

In the *Oracle Fusion Middleware Application Security Guide*, part number E10043-11, in Appendix C Oracle Fusion Middleware Audit Framework Reference, Table C-4 is incorrectly titled. The correct title should be "Oracle Internet Directory Events."

8.2.6 Clarification of Note in Appendix C

In the *Oracle Fusion Middleware Application Security Guide*, part number E10043-11, in Appendix C Oracle Fusion Middleware Audit Framework Reference, the note at the beginning of section 12.3.3 is incomplete. The note should read:

Note: The metadata store is separate from the audit data store which contains the actual audit data.

8.2.7 Notes Regarding Need for Server Restarts

In the *Oracle Fusion Middleware Application Security Guide*, part number E10043-11, Chapter 13 Configuring and Managing Auditing refers to the need to restart the server after audit policy changes. These references are in the following sections:

- Section 13.3 Managing Audit Policies, under the heading 'How Policies are Configured,', second sentence.
- Section 13.3.1 Manage Audit Policies for Java Components with Fusion Middleware Control, second bulleted note under Notes.
- Section 13.3.2 Manage Audit Policies for System Components with Fusion Middleware Control, second bulleted note under Notes.

However, a restart is not necessary; the changes take effect on the managed server after a few minutes.

9

SSL Configuration in Oracle Fusion Middleware

This chapter describes issues associated with SSL configuration in Oracle Fusion Middleware. It includes the following topic:

- Section 9.1, "General Issues and Workarounds"

9.1 General Issues and Workarounds

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

- Section 9.1.1, "Incorrect Message or Error when Importing a Wallet"

9.1.1 Incorrect Message or Error when Importing a Wallet

Problem 1

Fusion Middleware Control displays an incorrect message when you specify an invalid wallet password while attempting to import a wallet. The issued message "Cannot create p12 without password." is incorrect. Instead, it should notify the user that the password is incorrect and request a valid password.

Problem 2

Fusion Middleware Control displays an incorrect message when you attempt to import a password-protected wallet as an autologin wallet. The issued message "Cannot create p12 without password." does not provide complete information. Instead, it should notify the user that importing a password-protected wallet requires a password.

Problem 3

If you attempt to import an autologin wallet as a password-protected wallet using either Fusion Middleware Control or WLST, a NullPointerException error is displayed.

10

Oracle Directory Integration Platform

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

10.1 General Issues and Workarounds

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

10.1.1 Enabling the Domain-Wide Administration Port on Oracle WebLogic Server Prevents use of the DIP Command Line Interface

Be aware that enabling the domain-wide administration port on any WebLogic server running Directory Integration Platform will prevent you from using the DIP command line interface using a standard administrator account. Entering DIP commands will result in an error similar to the following:

```
User: "weblogic", failed to be authenticated
```

Administrators can still use the Enterprise Manager (EM) GUI to configure and manage Oracle Directory Integration Platform.

10.1.2 The AttrMapping Rule dnconvert() function is not Working During Directory Synchronization

During directory synchronization, the `AttrMapping` Rule `dnconvert()` function does not properly apply the attribute mapping rule. The `dnconvert()` function is supposed to take a `dnvalue` as its only argument and transform the value based on the domain mapping rule. Instead, no transformation is taking place.

For example:

```
DomainRules
cn=users,dc=ADdomain,dc=com:cn=users,dc=OIDdomain,dc=com:cn=%,dc=OIDdomain,c=com

###
AttributeRules
# attribute rule common to all objects
objectguid:
:binary:top:orclobjectguid:string:orclADObject:bin2b64(objectguid)
ObjectSID: :binary:user:orclObjectSID:string:orclADObject:bin2b64(ObjectSID)
distinguishedName: : :top:orclSourceObjectDN: :orclADObject:
samaccountname:::user:cn::person:
manager:::organizationalperson:manager::inetorgperson:dnconvert(manager)
```

In this example, the new entry from Active Directory to Oracle Internet Directory does not pull the `samAccountName` value but rather the DN value for the `manager`.

10.1.3 The Oracle Password Filter for Microsoft Active Directory is not Certified for use With Oracle Unified Directory or Oracle Directory Server Enterprise Edition

To use the Oracle Password Filter for Microsoft Active Directory, your Oracle back-end directory must be Oracle Internet Directory. The Oracle Unified Directory back-end directory and the Oracle Directory Server Enterprise Edition back-end directory do not support integration with the Oracle Password Filter for Microsoft Active Directory.

10.1.4 LDIF Files That Contain Non-ASCII Characters Will Cause the `testProfile` Command Option to Fail if the LDIF File has Native Encoding

When running DIP Tester from a command-line, the `manageSyncProfiles testProfile` command will fail if the `-ldiffile` option is specified and the LDIF file contains non-ASCII characters.

Note that LDIF files with UTF-8 encoding are not impacted by this limitation. If an LDIF file containing multibyte characters cannot be saved with UTF-8 encoding, then use the following workaround:

1. From a command-line, add the entry using the `ldapadd` command and include the `-E` option to specify the locale. See the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for the required command syntax.
2. Get the specific `changeNumber` for the last add operation.
3. Execute the `testProfile` command using the `changeNumber` from the previous step.

For more information, see "Section 7.1.5.2, Running DIP Tester From the WLST Command-Line Interface" in the *Administrator's Guide for Oracle Directory Integration Platform*.

10.1.5 Some Changes May Not Get Synchronized Due to Race Condition in Heavily-Loaded Source Directory

If the source directory is heavily-loaded, a race condition may occur where database commits cannot keep pace with updates to the lastchangenumber. If this race condition occurs, Oracle Directory Integration Platform may not be able to synchronize some of the changes.

To work around this issue, perform the following steps to enable database commits to keep pace with the lastchangenumber:

1. Increase the value of the synchronization profile's Scheduling Interval.
2. Control the number of times the search is performed on the source directory during a synchronization cycle by setting the `searchDeltaSize` parameter in the profile. Oracle suggests starting with a value of 10, then adjusting the value as needed.

10.1.6 Synchronization Continues After Stopping Oracle Directory Integration Platform

If you stop the Oracle Directory Integration Platform application during synchronization, the synchronization process that the Quartz scheduler started will continue to run.

To work around this issue, restart the Oracle WebLogic Managed Server hosting Oracle Directory Integration Platform or redeploy the Oracle Directory Integration Platform application.

10.1.7 File Path Separator Must Be Escaped on Windows

On Windows, you must escape the file path separator using a back-slash (\ ) in profile properties files and when executing Oracle Directory Integration Platform commands. For example:

- In profile properties files:

```
odip.profile.configfile = C:\\test\\Oracle_
IDM1\\ldap\\odi\\conf\\activeimp.cfg.master
```

- When executing an Oracle Directory Integration Platform command, such as `manageDIPServerConfig`:

```
C:\test\Oracle_IDM1\BIN>manageDIPServerConfig.bat set -attribute \
keystorelocation -h myhost.mycompany.com -p 7005 -D LOGIN_ID \
-value C:\\test\\Oracle_IDM1\\bin\\server_keystore.jks
```

10.1.8 Certain Queries and Provisioning Profile Functionality may Fail on JDK 1.6 u 21

LDAP JNDI filter processing has been updated to be stricter in JDK 1.6 u21. Consequently, certain queries performed by Oracle Directory Integration Platform may fail on JDK 1.6 u21 and provisioning profile functionality may also be affected. To fix this issue, download and apply patch 10631569, which is available for download on My Oracle Support (formerly MetaLink). Access My Oracle Support at https://support.oracle.com.

Oracle strongly recommends that you download and apply patch 10631569 for Identity Management 11.1.1.4.0.

10.2 Configuration Issues and Workarounds

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

10.2.1 Update the Mapping Rule for Novell eDirectory

If Directory Integration Platform is integrated with Novell eDirectory, or if you plan to integrate with Novell eDirectory later, edit the mapping rules in the `eDir` profile, otherwise the installation program will return this error message:

```
Map rules "orclodipattributemappingrules" have the following errors:
Attribute rule "0" has error: Invalid destination attribute's type: Expecting
'binary'; found 'string'.
```

If you have not yet integrated with Novell eDirectory, update the mapping file in the default template before registering a new profile.

Note: Refer to the "Updating Mapping Rules" section in the *Administrator's Guide for Oracle Directory Integration Platform* for information about how to modify an entry in a mapping rule file.

---

1. Update the mapping rules in the existing profile or new profile for the following entry:

   ```
   guid:1:binary:top:orclndsobjectguid:string:orclndsobject:bin2b64(guid)
   ```

   Replace it with this mapping:

   ```
   guid:1:binary:top:orclndsobjectguid:binary:orclndsobject:bin2b64(guid)
   ```

2. Save your changes.

10.2.2 Do not use localhost as Oracle Internet Directory Hostname When Configuring Oracle Directory Integration Platform

When configuring Oracle Directory Integration Platform against an existing Oracle Internet Directory—using either the installer's Install and Configure installation option or the Oracle Identity Management 11g Release 1 (11.1.1) Configuration Wizard—you must specify the hostname for Oracle Internet Directory using only its fully qualified domain name (such as myhost.example.com). *Do not* use `localhost` as the Oracle Internet Directory hostname even if Oracle Directory Integration Platform and Oracle Internet Directory are collocated on the same host.

If you use `localhost` as the Oracle Internet Directory hostname, you will not be able to start the Oracle WebLogic Managed Server hosting Oracle Directory Integration Platform.

10.2.3 You may Need to Restart the Directory Integration Platform After Running dipConfigurator Against Oracle Unified Directory

After running dipConfigurator against an Oracle Unified Directory (OUD) endpoint, if you are unable to open the Directory Integration Platform (DIP) UI in Enterprise Manger, stop and start DIP to fix the UI problem.

10.2.4 When Configuring a Profile, you may Need to Scroll Past a Section of Whitespace to View Mapping Rules

If you are using Internet Explorer to view the Directory Integration Platform (DIP) UI, you may need to scroll past a large blank space to see the profile mapping rules section. This issue is not known to affect other browsers.

10.2.5 Resource Usage Charts will not Display if Multiple IDM Domains are Running on the Same Host

If two `IDM` domains on the same host share the same `Oracle` home and are both configured to use `wls_ods1` managed servers, then the DIP home page will not display the resource usage charts if both instances are running at the same time.

10.3 Documentation Errata

There are no known documentation issues at this time.

11

Oracle Virtual Directory

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

11.1 General Issues and Workarounds

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

11.1.1 Oracle Virtual Directory Fails to Start When Unsupported Ciphersuite for Listener SSL Config is Selected in Enterprise Manager

When you create an Oracle LDAP listener in Enterprise Manager, and then edit the listener's Change SSL setting by selecting **Enable SSL** for any SSL authorization, Enterprise Manager selects the ciphersuite `TLS_DHE_RSA_WITH_AES_128_CBC_SHA256`. If this ciphersuite is selected, then Oracle Virtual Directory will fail to start-up entirely.

Oracle Virtual Directory supports the following protocols:

- TLSv1
- SSLv2Hello
- SSLv3

Note: For a complete list of the supported ciphers for each protocol, refer to the following location:

`http://www.openssl.org/docs/apps/ciphers.html`

To work around this issue, manually uncheck all of the ciphers listed for Enterprise Manager when configuring the ciphersuites.

11.1.2 EUS Adapter Creation Failed

When creating an EUS adapter using the wizard in Oracle Directory Services Manager, an error message periodically displays stating the adapters and ACLs were not created successfully.

To work around this issue, proceed as follows:

- If the error occurred while you were loading ACLs, and only partial ACLs were loaded during EUS configuration, then you can manually load the remaining ACLs by running this command:

  ```
  $ORACLE_HOME/bin/ldapmodify -c -v -h <ovd_host> -p <ovd_port> -D cn=orcladmin
  -w <orcladmin_password> -f
  $ORACLE_HOME/ovd/eus/eusACLTemplate.ldif
  ```

- If the error occurred during any other step, then manually clean up the partial configuration from Oracle Virtual Directory by using the following steps, and then reconfigure Oracle Virtual Directory for EUS.

  1. Delete all of the Local Store and LDAP EUS adapters created.
  2. Delete the LSA EUS adapter data files from the local file system.
  3. Undeploy the EUS py mapping based on your directory type (if it exists).
  4. Click the EUS wizard icon again to reconfigure.

11.1.3 Manually Edit adapters.os_xml File When Creating DB Adapter For Sybase

Creating a Database Adapter with Sybase as back-end causes Oracle Virtual Directory to fail with an `Invalid Database Connection` error.

To work around this issue, you can manually edit the `adapters.os_xml` file using the same Database connection information.

11.1.4 ODSM Version Does Not Change in Enterprise Manager after Patching ODSM to 11.1.1.6.0

The Oracle Directory Services Manager version shown in Enterprise Manager is the application version, which does not change when you patch Oracle Directory Services Manager.

The Oracle Lifecycle team requires all Enterprise Manager components to retain the same application version. However, because customers want to know which Oracle Directory Services Manager version they are using, Oracle Directory Services Manager maintains the actual (patch) version and Enterprise Manager maintains the application version, which causes this mismatch.

This issue is a known issue, starting with version 11.1.1.3.0.

11.1.5 ODSM Bug Requires Editing of odsmSkin.css File

Due to a misplaced comment in the file `odsmSkin.css`, some labels on the Oracle Directory Services Manager home page are not displayed correctly. Specifically, the labels in the diagram on the right are misplaced or missing.

To work around this issue, proceed as follows:

1. Stop the wls_ods1 managed server and the WebLogic Administration server.
2. Edit the file:

MW_HOME/user_projects/domains/*DOMAIN_HOME*/servers/*MANAGED_SERVER_NAME*/tmp/_WL_user/*ODSM_VERSION_NUMBER*/*RANDOM_CHARACTERS*/war/skins/odsmSkin.css

For example:

wlshome/user_projects/domains/base_domain/servers/wls_ods1/tmp/_WL_user/odsm_11.1.1.2.0/z5xils/war/skins/odsmSkin.css

Before editing, the odsmSkin.css file looks like this:

```
@agent ie /*========== Fix for bug#7456880 ==========*/
{
  af|commandImageLink::image,
  af|commandImageLink::image-hover,
  af|commandImageLink::image-depressed
  {
    vertical-align:bottom;
  }
}
```

Move the comment:

```
/*========== Fix for bug#7456880 ==========*/
```

so that it is above the line

```
@agent ie
```

After editing, the file should look like this:

```
/*========== Fix for bug#7456880 ==========*/
@agent ie
{
  af|commandImageLink::image,
  af|commandImageLink::image-hover,
  af|commandImageLink::image-depressed
  {
    vertical-align:bottom;
  }
}
```

3. Restart the WebLogic Administration server and the wls_ods1 managed server.

11.1.6 Oracle Directory Services Manager Browser Window is Not Usable

In some circumstances, after you launch Oracle Directory Services Manager from Fusion Middleware Control, then select a new Oracle Directory Services Manager task, the browser window might become unusable. For example, the window might refresh repeatedly, appear as a blank page, fail to accept user input, or display a null pointer error.

As a work around, go to the URL: http://*host*:*port*/odsm, where *host* and *port* specify the location where Oracle Directory Services Manager is running, for example, http://myserver.example.com:7005/odsm. You can then use the Oracle Directory Services Manager window to log in to a server.

11.1.7 Exceptions May Occur in Oracle Directory Services Manager When Managing Multiple Oracle Virtual Directory Components and One is Stopped

Under certain circumstances, when managing multiple Oracle Virtual Directory components from the same Oracle Directory Services Manager session, exception or

error messages may appear if you stop one of the Oracle Virtual Directory components. For example, you are managing Oracle Virtual Directory components named ovd1 and ovd2 from the same Oracle Directory Services Manager session. Both ovd1 and ovd2 are configured and running. If you stop ovd1, an exception or Target Unreachable message may appear when you try to navigate Oracle Directory Services Manager.

To work around this issue, exit the current Oracle Directory Services Manager session, close the web browser, and then reconnect to Oracle Virtual Directory components in a new Oracle Directory Services Manager session.

11.1.8 Identifying the DN Associated with an Access Control Point in Oracle Directory Services Manager

When you create an Access Control Point (ACP) using Oracle Directory Services Manager, the Relative Distinguished Name (RDN) of the DN where you created the ACP appears in the navigation tree on the left side of the screen. For example, if you create an ACP at the DN of **cn=ForExample,dc=us,dc=sales,dc=west**, then **cn=ForExample** appears in the navigation tree. After clicking an ACP in the navigation tree, its settings appear in the right side of the screen and the RDN it is associated with appears at the top of the page.

To identify the DN associated with an ACP, move the cursor over ("mouse-over") the ACP entry in the navigation tree. The full DN associated with the ACP will be displayed in a tool-tip dialog box.

Mousing-over ACPs in the navigation tree is useful when you have multiple ACPs associated with DNs that have identical RDNs, such as:

ACP 1 = cn=ForExample,dc=us,dc=sales,dc=west

ACP 2 = cn=ForExample,dc=us,dc=sales,dc=east

11.1.9 Issues With Oracle Virtual Directory Metrics in Fusion Middleware Control

This topic describes issues with Oracle Virtual Directory metrics in Fusion Middleware Control, including:

- Configuring Operation-Specific Plug-Ins to Allow Performance Metric Reporting in Fusion Middleware Control After Upgrading to 11g Release 1 (11.1.1)

11.1.9.1 Configuring Operation-Specific Plug-Ins to Allow Performance Metric Reporting in Fusion Middleware Control After Upgrading to 11g Release 1 (11.1.1)

If you upgraded an Oracle Virtual Directory Release 10g installation with plug-ins configured to execute on specific operations, such as add, bind, get, and so on, to 11*g* Release 1 (11.1.1), you may have to update those operation-specific plug-ins before you can use Fusion Middleware Control to view performance metrics.

After upgrading to 11*g* Release 1 (11.1.1) and performing some initial operations to verify the upgrade was successful, check the Oracle Virtual Directory home page in Fusion Middleware Control. You should see data for the Current Load and Average Response Time and Operations metrics.

If you do not see any data for these metrics, you must update the plug-ins configured to execute on specific operations. The work-around is to add the Performance Monitor plug-in to the operation-specific plug-in's configuration chain.

Perform the following steps to add the Performance Monitor plug-in to the operation-specific plug-in's configuration chain:

1. If the operation-specific plug-in is a Global-level plug-in, edit the server.os_xml file located in the *ORACLE_INSTANCE*/config/OVD/*NAME_OF_OVD_COMPONENT*/ directory.

   If the operation-specific plug-in is an adapter-level plug-in, edit the adapters.os_xml file located in the *ORACLE_INSTANCE*/config/OVD/*NAME_OF_OVD_COMPONENT*/ directory.

   Note: If multiple adapters are configured, you must perform steps 2 and 3 for every adapter configuration in the adapters.os_xml file.

2. Locate the `pluginChains` element in the file. For example, if the Dump Transactions plug-in is configured to execute on the get operation, you will see something similar to the following:

Example 11–1 Dump Transactions Plug-In Configured for get Operation

```
 <pluginChains xmlns="http://xmlns.oracle.com/iam/management/ovd/config/plugins">
  <plugins>
     <plugin>
       <name>Dump Transactions</name>

<class>com.octetstring.vde.chain.plugins.DumpTransactions.DumpTransactions</class>
       <initParams>
         <param name="loglevel" value="info"/>
       </initParams>
     </plugin>
     <plugin>
       <name>Performance Monitor</name>

<class>com.octetstring.vde.chain.plugins.performance.MonitorPerformance</class>
       <initParams/>
     </plugin>
  </plugins>
  <default>
     <plugin name="Performance Monitor"/>
  </default>
  <get>
     <plugin name="Dump Transactions">
       <namespace>ou=DB,dc=oracle,dc=com </namespace>
     </plugin>
   </get>
 </pluginChains>
```

3. Add the following Performance Monitor plug-in element within the operation-specific configuration chain:

   ```
   <plugin name="Performance Monitor"/>
   ```

   For example:

Example 11–2 Adding the Performance Monitor to the Operation-Specific Plug-In Configuration Chain

```
<pluginChains xmlns="http://xmlns.oracle.com/iam/management/ovd/config/plugins">
  <plugins>
     <plugin>
       <name>Dump Transactions</name>
```

```
<class>com.octetstring.vde.chain.plugins.DumpTransactions.DumpTransactions</class>
        <initParams>
          <param name="loglevel" value="info"/>
        </initParams>
      </plugin>
      <plugin>
        <name>Performance Monitor</name>

<class>com.octetstring.vde.chain.plugins.performance.MonitorPerformance</class>
        <initParams/>
      </plugin>
   </plugins>
   <default>
      <plugin name="Performance Monitor"/>
   </default>
   <get>
      <plugin name="Dump Transactions">
        <namespace>ou=DB,dc=oracle,dc=com </namespace>
      </plugin>
      <plugin name="Performance Monitor"/>
    </get>
  </pluginChains>
```

4. Save the file.
5. Restart Oracle Virtual Directory.

11.1.10 Using a Wildcard when Performing an LDAPSEARCH on a TimesTen Database Causes an Operational Error

Currently, a TimesTen bug is preventing wildcard searches (such as "`cn=t*`") from working in a Database adapter with TimesTen.

To work around this problem, enable the Case Insensitive Search option and create the necessary linguistic indexes for any database columns used in the search.

For more information, see the related TimesTen Enhancement Request, Bug# 9885055 and Section 12.2.2 "Creating Database Adapters for Oracle TimesTen In-Memory Database" in the *Oracle® Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

11.1.11 ODSM Version 11.1.1.4.0 Does Not Support OVD Versions 11.1.1.2.0 or 11.1.1.3.0

Oracle Directory Services Manager Version 11.1.1.4.0 does not support Oracle Virtual Directory Versions 11.1.1.2.0 or 11.1.1.3.0.

Changes introduced in Oracle Directory Services Manager Version 11.1.1.4.0 improve configuration auditing, and these changes require that you use Oracle Virtual Directory 11.1.1.4.0.

11.1.12 ODSM Version 11.1.1.5.0 Does Not Support OVD Versions 11.1.1.2.0, 11.1.1.3.0, or 11.1.1.4.0

Oracle Directory Services Manager Version 11.1.1.5.0 does not support Oracle Virtual Directory Versions 11.1.1.2.0, 11.1.1.3.0, or 11.1.1.4.0.

Changes introduced in Oracle Directory Services Manager Version 11.1.1.5.0 improve configuration auditing, and these changes require that you use Oracle Virtual Directory 11.1.1.5.0.

11.1.13 ODSM Version 11.1.1.6.0 Does Not Support OVD Versions 11.1.1.2.0, 11.1.1.3.0, 11.1.1.4.0, or 11.1.1.5.0

Oracle Directory Services Manager Version 11.1.1.6.0 does not support Oracle Virtual Directory Versions 11.1.1.2.0, 11.1.1.3.0, 11.1.1.4.0, or 11.1.15.0.

Changes introduced in Oracle Directory Services Manager Version 11.1.1.6.0 improve configuration auditing, and these changes require that you use Oracle Virtual Directory 11.1.1.6.0.

11.1.14 Oracle Virtual Directory Issues with IPv6 Stack on Windows Platforms Using JDK6

Running CRUD operations on Microsoft Windows platforms using JDK 6 causes an issue in NIO (non-blocking Input/Output) mode because an issue exists with non-blocking IO. The same problem happens for the IPv6 addresses in Windows dual-stack (IPv4/IPv6) systems.

Note: Support for IPv6 stack was added in JDK 7 Build b36.

For more information, refer to JDK Bug ID 6230761 (http://bugs.sun.com/view_bug.do?bug_id=6230761) and 4640544 (http://bugs.sun.com/view_bug.do?bug_id=4640544).

The Oracle Virtual Directory development team verified this use case with JDK 7 and confirmed that it works in Oracle Virtual Directory NIO mode.

Workaround:

Note: You must apply this workaround in the Oracle Virtual Directory server.

In the Oracle Virtual Directory server, turn off NIO mode by adding the `<useNIO>false</useNIO>` XML element in *<OracleInstance>*`/config/OVD/ovd1/listeners.os_xml` at the following location, then stop and restart the Oracle Virtual Directory server:

```
<ldap id="LDAP Endpoint" version="0">
    <port>6501</port>
    ...
    <socketOptions>
        ...
    </socketOptions>
    <useNIO>false</useNIO>
</ldap>
```

11.1.15 Users with Non-ASCII Names Might Encounter Problems when Using ODSM with SSO

When Oracle Directory Services Manager is configured to use Oracle Access Manager 11g Release 1 (11.1.1.2) for single sign-on, a user whose name contains non-ASCII characters might observe the following issues after logging in:

- The user name displayed on the Home page is garbled.
- Single sign-on connections to Oracle Virtual Directory servers do not appear in the list of connections.

11.1.16 Creating an Attribute/Object Class Throws NPE Error

After upgrading Oracle Directory Services Manager, creating an attribute or an objectclass causes an NPE error.

Workaround:

Refresh the entries by clicking **Refresh** every time the creation fails.

11.1.17 Patch Required to Enable Account Lockout Feature

An additional Patch 10365116 is required to enable the Account Lockout functionality.

In addition, Oracle Virtual Directory may not update the AD badpasswdcount until the account is fully locked out, which means AD badpasswdcount shows the correct number when it reaches the bad password count setting in AD.

11.1.18 ODSM Problems in Internet Explorer 7

The Oracle Directory Services Manager interface might not appear as described in Internet Explorer 7.

For example, the **Logout** link might not be displayed.

If this causes problems, upgrade to Internet Explorer 8 or 9 or use a different browser.

11.1.19 Strings Related to New Enable User Account Lockout Feature on EUS Wizard Are Not Translated

The new Enable User Account Lockout feature (and related messages) provided in the Oracle Virtual Directory EUS wizard have not been translated.

11.1.20 All Connections Created In ODSM 11.1.1.1.0 Are Lost After Upgrading to OVD or OID Version 11.1.1.7.0

Due to some deployment changes made to Oracle Directory Services Manager version 11.1.1.2.0, any connections created in Oracle Directory Services Manager version 11.1.1.1.0 will be lost when you upgrade to Oracle Virtual Directory version 11.1.1.7.0 or Oracle Internet Directory version 11.1.1.7.0.

Oracle Directory Services Manager resumes caching connection details the first time you connect again after upgrading to Oracle Virtual Directory version 11.1.1.7.0 or Oracle Internet Directory version 11.1.1.7.0.

11.1.21 Incorrect ODSM Version Displays in Enterprise Manager Console After OVD Upgrade

The Oracle Directory Services Manager version automatically displays as *11.1.1.2.0* in the Enterprise Manager console for all patch set releases. This Oracle Directory Services Manager version number does not increment to match the patch set version when you upgrade.

11.1.22 Oracle Virtual Directory Versions 11.1.1.6.0 and 11.1.1.7.0 Start-Up Fails on Windows

With versions 11.1.1.6.0 and 11.1.1.7.0 on Windows 2003 and 2008 machines (both 32-bit and 64-bit), starting Oracle Virtual Directory fails with an exception.

To work around this issue, perform the following steps *before* you start an instance containing Oracle Virtual Directory:

1. Locate the `cwallet.sso` file at

   `$`*`instance_home`*`\config\jps\bootstrap\cwallet.sso`

2. Add the `write` permission to the `SYSTEM` user's assigned privileges.
3. Start the Oracle Virtual Directory instance.

11.1.23 Connection Issues to OVD

In non-Linux environments, if you have any issues connecting to Oracle Virtual Directory from Oracle Directory Services Manager, LDAP tools, or any other applications, you must disable NIO in the non-SSL listener by using the following steps:

1. From a command window, stop Oracle Virtual Directory:

   `$`*`ORACLE_INSTANCE`*`/bin/opmnctl stopproc ias-component=ovd1`

2. Edit the `$`*`ORACLE_INSTANCE`*`/config/OVD/ovd1/listeners.os_xml` file as follows:

   a. Locate this LDAP non-SSL listener section:

   ```
   <ldap id="LDAP Endpoint" version="0">
         <port>6501</port>
         <host>0.0.0.0</host>
         .........
         .........
          <tcpNoDelay>true</tcpNoDelay>
          <readTimeout>0</readTimeout>
       </socketOptions>
    </ldap>
   ```

   b. Modify the section by adding `<useNIO>false</useNIO>`, as indicated:

   ```
    <ldap id="LDAP Endpoint" version="0">
         <port>6501</port>
         <host>0.0.0.0</host>
         .........
         .........
          <tcpNoDelay>true</tcpNoDelay>
          <readTimeout>0</readTimeout>
       </socketOptions>
       <useNIO>false</useNIO>
   ```

```
</ldap>
```

3. Start Oracle Virtual Directory:

```
$ORACLE_INSTANCE/bin/opmnctl startproc ias-component=ovd1
```

This modification should resolve the connection issues.

11.1.24 ODSM Version 11.1.1.70 Does Not Support OVD Versions 11.1.1.2.0, 11.1.1.3.0, 11.1.1.4.0, 11.1.1.5.0, or 11.1.1.6.0

Oracle Directory Services Manager Version 11.1.1.7.0 does not support Oracle Virtual Directory Versions 11.1.1.2.0, 11.1.1.3.0, 11.1.1.4.0, 11.1.1.5.0, or 11.1.1.6.0.

Changes introduced in Oracle Directory Services Manager Version 11.1.1.7.0 improve configuration auditing, and these changes require that you use Oracle Virtual Directory 11.1.1.7.0.

11.1.25 Modify Completes When Updating a Mandatory Attribute to Null

If a `modify` operation adds an attribute with an empty value, and the attribute type does not allow empty values, the operation no longer returns an error. For example, `ldapmodify ADD sn` with an empty value previously returned an Invalid Syntax error and now it does not return any errors. Other `modify` operation failures are properly reported.

11.1.26 Online Help Section is Not Working

The Oracle Directory Services Manager online help section does not work in Internet Explorer 10 (IE10) web browsers.

11.2 Configuration Issues and Workarounds

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

- Section 11.2.1, "Configuring an OVD/OID Adapter For SSL Mutual Authentication"

11.2.1 Configuring an OVD/OID Adapter For SSL Mutual Authentication

Neither *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory* nor *Oracle Fusion Middleware Administrator's Guide* describes how to set up an Oracle Virtual Directory/Oracle Internet Directory adapter for SSL Mutual Authentication. This information is provided in Note 1449118.1 and Note 1311791.1, which are available on My Oracle Support at:

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

11.3 Documentation Errata

This section describes documentation errata in the *Administrator's Guide for Oracle Virtual Directory*. It includes the following topics:

- Deploying Oracle Unified Directory with Oracle Virtual Directory

11.3.1 Deploying Oracle Unified Directory with Oracle Virtual Directory

You can deploy Oracle Unified Directory as an LDAP data source with Oracle Virtual Directory. For information about how to deploy Oracle Unified Directory with Oracle Virtual Directory, see "Creating LDAP Adapters" in the *Oracle® Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.