# Oracle® Fusion Middleware

Identity Management Release Notes

11*g* Release 1 (11.1.1.9)

**E54530-03**

December 2017

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

Oracle Fusion Middleware Identity Management Release Notes, 11*g* Release 1 (11.1.1.9)

E54530-03

# Contents

## 1 Introduction

## 2 Oracle Internet Directory

## 3 Oracle Identity Federation

## 4 Oracle Security Developer Tools

## 5 Oracle Platform Security Services

## 6 Oracle Directory Integration Platform

## 7 Oracle Virtual Directory

# Preface

This preface includes the following sections:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions

## Audience

This document is intended for users of Oracle Fusion Middleware 11*g* Release 1 Patch Set 9 (11.1.1.7).

## Documentation Accessibility

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

### Access to Oracle Support

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

## Related Documents

For more information, see these Oracle resources:

- *Oracle Fusion Middleware Documentation on Oracle Fusion Middleware Disk 1*
- *Oracle Fusion Middleware Documentation Library 11g Release 1 Patch Set 9 (11.1.1.7)*
- Oracle Technology Network at `http://www.oracle.com/technology/index.html`

## Conventions

The following text conventions are used in this document:

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

# 1 Introduction

This chapter introduces the Release Notes for 11g Release 1 (11.1.1). It includes the following sections:

## 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 that you review its contents before installing, or working with the product.

**Note:** In addition, Oracle recommends that you read the *Oracle Fusion Middleware Infrastructure Release Notes* for release information regarding:

- Installation and Configuration Issues
- Upgrade and Migration Issues
- Oracle Fusion Middleware Administration
- High Availability and Enterprise Deployment

## 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 topics:

- Section 1.4.1, "Where to Find Oracle Fusion Middleware Certification Information"
- Section 1.4.2, "Certification Exceptions"

### 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.

> **Note:** 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.

There are no known issues at this time.

## 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

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

*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.<br>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 the following error:<br>`java.lang.NumberFormatException` |

## 1.6 Licensing Information

Licensing information for Oracle Fusion Middleware is available at:

`https://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 Internet Directory

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

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

## 2.1 General Issues and Workarounds

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

- Section 2.1.1, "Substring Filter Not Supported for Collective Attributes"
- Section 2.1.2, "Search on rootDSE `lastchangenumber` Attribute Works For One Attribute At A Time"
- Section 2.1.3, "Search with Filter Containing AND Operation of Collective Attributes Not Supported"
- Section 2.1.4, "Oracle Database Requires Patch to Fix Purge Job Problems"
- Section 2.1.5, "ODSM Does Not Create Entry of Custom objectclass With Custom Mandatory Field"
- Section 2.1.6, "ODSM Adds Fake Entries to the Chained Container and Displays Duplicate Entries During Export"
- Section 2.1.7, "Oracle Internet Directory Upgrade from 10.1.4.3 to 11.1.1.9.0 Fails During Configuration on AIX"
- Section 2.1.8, "ODSM Problems in Internet Explorer 7"
- Section 2.1.9, "Cloned Oracle Internet Directory Instance Fails or Runs Slowly"
- Section 2.1.10, "Oracle Internet Directory Fails to Start on Solaris SPARC System Using ISM"
- Section 2.1.11, "Custom Audit Policy Settings Fail When Set Through Enterprise Manager"
- Section 2.1.12, "Deleting Mandatory `attributeTypes` Referenced by `objectClass` is Successful"
- Section 2.1.13, "Oracle Unified Directory 11.1.2.0 `orclguid` Attribute is Not Mapped for Server Chaining"
- Section 2.1.14, "ODSM Browser Window Becomes Unusable"

### 2.1.1 Substring Filter Not Supported for Collective Attributes

Oracle Internet Directory does not provide support for substring filter for collective attributes. For instance, the following substring filter is not supported:

```
tenantguid=*234*
```

However, the equality filter for instance, `tenantguid=12345` is supported for collective attributes.

### 2.1.2 Search on rootDSE `lastchangenumber` Attribute Works For One Attribute At A Time

If you perform `ldapsearch` on rootDSE to fetch the `lastchangenumber` attribute along with other attributes, then `lastchangenumber` is not retrieved.

For instance, when you run the following command then `lastchangenumber` attribute is not retrieved:

```
ldapsearch -p port -D "cn=orcladmin" -w password -b "" -s base "objectclass=*"
changelog lastchangenumber
```

The workaround for this problem is to perform `ldapsearch` on rootDSE only for `lastchangenumber` attribute as follows:

```
ldapsearch -p <port> -h <hostname> -b ' ' -s base '(objectclass=*)'
lastchangenumber

lastchangenumber=4714
```

### 2.1.3 Search with Filter Containing AND Operation of Collective Attributes Not Supported

When the search filter contains only collective attribute expressions, and an AND (&) operation is performed, then the server does not return expected results.

For example, if you run the following commands having collective attributes only, then if you run an AND operation, the server fails to return the desired result.

```
ldapsearch -b 'cn=u1,cn=collandbug' '&(description=coll1 desc)
(description=coll2 desc)' dn
```

### 2.1.4 Oracle Database Requires Patch to Fix Purge Job Problems

Some versions of Oracle Database, such as 10.1.0.5.0rec.jul10, 10.2.0.4.5.psu, 10.2.0.5.1psu, 11.1.0.7.4psu, and 11.2.0.1.2psu require a patch to fix Oracle Internet Directory purge job problems.

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.

If you are experiencing the preceding purge job problems with any of the listed Oracle Database versions, then apply the latest Patch Set Update (PSU) for your Oracle Database that fixes RDBMS bug 9294838. If so, apply the RDBMS patch for your database. You can apply the patch after you have installed Oracle Internet Directory.

### 2.1.5 ODSM Does Not Create Entry of Custom objectclass With Custom Mandatory Field

On the Schema tab, create a custom attribute and a custom objectclass, and also select custom attribute as indexed. Now, on the Data Browser tab if you create an entry of `objectclass="custom object class"` then it does not allow you to enter the mandatory value in the custom attribute field.

There is no workaround for this issue.

### 2.1.6 ODSM Adds Fake Entries to the Chained Container and Displays Duplicate Entries During Export

In ODSM, when you set up server chaining with Oracle Directory Server Enterprise Edition (ODSEE) as the backend the following issues emerge:

- If you create an entry through ODSM, then ODSM pretends to add the entry to the remote server through chaining. However, the entry does not get added on the remote server, ODSEE.
- If you add the preceding entry directly to the remote backend, and navigate to the parent entry through the Data Explorer tab, and then export to LDIF the same entry, you will see duplicate entries.

### 2.1.7 Oracle Internet Directory Upgrade from 10.1.4.3 to 11.1.1.9.0 Fails During Configuration on AIX

This issue occurs when you upgrade Oracle Internet Directory from 10.1.4.3 to 11.1.1.9.0 on AIX. The upgrade fails during configuration with the following error:

```
javax.net.ssl.SSLException: Received fatal alert: illegal_parameter
```

The workaround for this issue is to add the java option to disable ECDH ciphers while configuring Oracle Internet Directory 11.1.1.9.0, as shown in the following example:

```
ORACLE_HOME/config.sh -Doracle.ldap.odi.sslsocketfactory.disable-ecc=true
```

### 2.1.8 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.

### 2.1.9 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*.

### 2.1.10 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.

## 2.1.11 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*.

### 2.1.12 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.

### 2.1.13 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.

### 2.1.14 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.

### 2.1.15 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.

### 2.1.16 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.

### 2.1.17 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 percentage 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*.

## 2.2 Configuration Issues and Workarounds

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

- Section 2.2.1, "Accept TLS Protocol for SSL support"
- Section 2.2.2, "TLSv1.2 Protocols and Ciphers Cannot be Configured from EM"
- Section 2.2.3, "ODSM Security Page Loads With Error When Accessed from EM"

### 2.2.1 Accept TLS Protocol for SSL support

While configuring Oracle Internet Directory in SSL mode, if SSLv3 is disabled and you try to enable the TLS mode only, then the Oracle Internet Directory configuration hangs. This happens when `orclsslciphersuite` attribute is populated with unsupported cipher suites.

The workaround is to remove the unsupported cipher suite from the `orclsslciphersuite` attribute. For more information about the supported cipher suite list, see "Supported Cipher Suites" in Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory.

In addition, you must completely disable SSLv3, and enable TLS for configuring Oracle Internet Directory in SSL mode. For enabling only TLS (and disabling SSLv3), you need to modify the value of `orclcryptoversion` attribute to `28`. This value refers to TLS 1.0, TLS 1.1, or TLS 1.2. For more information, see "Supported Protocol Versions" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

Run the `ldapmodify` command to update the value of `orclcryptoversion` to `28` as follows:

```
ldapmodify -D "cn=orcladmin" -q -p portNum -h hostname -f ldifFile
```

Here `ldifFile` contains:

```
dn: cn=oid1,cn=osdldapd,cn=subconfigsubentry
changetype: modify
replace: orclcryptoversion
orclcryptoversion: 28
```

### 2.2.2 TLSv1.2 Protocols and Ciphers Cannot be Configured from EM

From EM, when you navigate to OID -> Administration -> Server Properties page, on the General tab, change SSL settings link, there is only one protocol version v1. There is no way to configure TLSv1.1,TLSv1.2 Protocols and corresponding ciphers.

The workaround is to use `ldapmodify` command to configure TLS protocols.

For more information, see "Configuring SSL by Using LDAP Commands" in the *Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

### 2.2.3 ODSM Security Page Loads With Error When Accessed from EM

From EM, Directory Service Manager, when you select the Security tab, the Security tab opens in the popup window, but soon after that, an error is thrown on the page as follows:

"An unresolvable error has occurred. Please contact your administrator for more information"

**Note:** This issue is intermittent.

As a workaround, when the error screen comes up, clicking on Back, will take us to the ODSM. Further navigation from the same page will not throw any errors.

## 2.3 Documentation Errata

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

- Section 2.3.1, "New Superuser Account Must be Direct Member of `DirectoryAdminGroup` Group"
- Section 2.3.2, "Server Restart After Adding an Encrypted Attribute is Not Documented"
- Section 2.3.3, "Setting Up Oracle Internet Directory SSL Mutual Authentication"
- Section 2.3.4, "Replication Instructions in Tutorial for Identity Management are Incomplete"

### 2.3.1 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.

### 2.3.2 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*.

### 2.3.3 Setting Up Oracle Internet Directory SSL Mutual Authentication

Neither the *Administrator's Guide for Oracle Internet Directory* nor the *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/`

### 2.3.4 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. If the new consumer node has pre-loaded data, then various conflict resolution and invalid attribute name format messages will appear in the replication logs.

For more information, see Section 40.1.7, "Rules for Configuring LDAP-Based Replication," in the *Administrator's Guide for Oracle Internet Directory*.

# 3

# Oracle Identity Federation

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

# 4

# Oracle Security Developer Tools

This chapter describes issues associated with Oracle Security Developer Tools. There are no known issues at this time.

# 5 Oracle Platform Security Services

This chapter describes notes on topics associated with Oracle Platform Security Services (OPSS), in the following sections:

- Configuration Issues and Workarounds
- 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*

## 5.1 Configuration Issues and Workarounds

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

- Section 5.1.1, "Script libovdconfig.bat Does Not Support a Space in File Path"
- Section 5.1.2, "Issues in IGF/IDS Group APIs with ADAM Directory"
- Section 5.1.3, "IDS/libOVD Issue During pasteConfig Operation"
- Section 5.1.4, "Oracle Fusion Middleware Audit Framework"
- Section 5.1.5, "Trailing '\n' Character in Bootstrap Key"
- Section 5.1.6, "Users with Same Name in Multiple Identity Stores"
- Section 5.1.7, "Script listAppRoles Outputs Wrong Characters"
- Section 5.1.8, "Propagating Identities over the HTTP Protocol"
- Section 5.1.9, "Pool Configuration Missing in Identity Store"
- Section 5.1.10, "JNDI Connection Exception and JDK Version"
- Section 5.1.11, "Using Third-Party CA Signed Certificates"

### 5.1.1 Script libovdconfig.bat Does Not Support a Space in File Path

On the Microsoft Windows platform, the `libovdconfig.bat` script does not work if the path to your Java installation in the `-jreLoc` option includes a space character. For example, `C:\Program Files\Java\jdk1.7.0_21`.

The workaround is to provide the path to your Java installation in DOS 8.3 format.

For example:

```
-jreloc C:\Progra~1\Java\jdk1.7.0_21
```

### 5.1.2 Issues in IGF/IDS Group APIs with ADAM Directory

If you use ADAM as a backend authenticator, then it causes the following issues with IGF/IDS APIs:

- If you set the extended property `group.member.attrs` to `member` or `uniquemember`, delete relationship fails.

  The workaround is to comment the `member` to `uniquemember` mappings in the mappings.os_xml file.

- If you set the extended property `group.member.attrs` to `member`, search entity relationship does not return anything.

  The workaround is to set the `group.member.attrs` property to `uniquemember`. However, ADAM does not support `groupOfUniquenames` out-of-the-box.

### 5.1.3 IDS/libOVD Issue During pasteConfig Operation

During T2P paste operation, if you configure an IDS store in the source environment, and use the same IDS store in the target environment without moving it then the following error message appears when you perform the `pasteConfig` operation:

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

The workaround is to locate the `configProperty` element in the generated moveplan.xml file under the `configGroup` element for `LIBOVD_ADAPTERS`. It represents the IDS store that you do not plan to move. Now, comment out multiple lines of the `configProperty` element for the associated IDS store in the move plan.

**Note:** You must perform the steps mentioned in the workaround before running the `pasteConfig` command.

### 5.1.4 Oracle Fusion Middleware Audit Framework

This section describes configuration issues for the Oracle Fusion Middleware Audit Framework. It contains these topics:

- Section 5.1.4.1, "Configuring Auditing for Oracle Access Manager"
- Section 5.1.4.2, "Audit Reports do not Display Translated Text in Certain Locales"
- Section 5.1.4.3, "Audit Reports Always Display in English"
- Section 5.1.4.4, "Audit Store Does not Support Reassociation through EM"
- Section 5.1.4.5, "OWSM Audit Events not Audited"

#### 5.1.4.1 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.

#### 5.1.4.2 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.

#### 5.1.4.3 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.

#### 5.1.4.4 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.

#### 5.1.4.5 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.

### 5.1.5 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.

### 5.1.6 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.

### 5.1.7 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.

## 5.1.8 Propagating Identities over the HTTP Protocol

This section includes the following additions, corrections, and new information in the following sections:

- Section 5.1.8.1, "Addition to Section Propagating Identities over the HTTP Protocol"
- Section 5.1.8.2, "Correction to Section Client Application Code Sample"
- Section 5.1.8.3, "Correction to Section Keystore Service Configuration"
- Section 5.1.8.4, "Updating the Trust Service Configuration Parameters"

### 5.1.8.1 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.

### 5.1.8.2 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.

### 5.1.8.3 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`.

### 5.1.8.4 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"
```

### 5.1.9 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.

### 5.1.10 JNDI Connection Exception and JDK Version

JNDI Connections throw the following exception: `javax.naming.NamingException: LDAP response read timed out, timeout used:-1ms.`

This error is encountered if your domain is configured to use an LDAP-based security store and it is running any of the following JDK versions: Java SE 6u85, 7u72, or 8u20.

To work around this issue, update JDK to Java SE 6u95, 7u80, or 8u45. For certified JDK versions, see Oracle Fusion Middleware 12c Certifications at `http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html`.

### 5.1.11 Using Third-Party CA Signed Certificates

Production environments are advised to use third-party CA signed certificates in their deployments. To set up a third-party CA signed certificate:

1. Generate a key pair in KSS using a specified alias.
2. Generate a CSR the key pair.
3. Submit the new CSR to a third-party CA. The CA will sign the public key in the CSR and return a CA signed certificate and its own certificate to be included as trust.

> **Note:** Some CAs return a single certificate chain containing both the CA signed certificate and its own certificate, instead of two separate certificates.

4. Import the CA signed certificate or the certificate chain using the alias specified to generate the key pair.
5. Import the CA signed certificate as a trusted certificate using a new alias.

## 5.2 Documentation Errata

This section contains corrections to documentation errors. It includes the topics:

- Section 5.2.1, "Updated Configuration for Role Category"
- Section 5.2.2, "Demo CA Certificate not for Production Use"
- Section 5.2.3, "Incorrect Link to ILM Content"

### 5.2.1 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.

### 5.2.2 Demo CA Certificate not for Production Use

In the *Oracle Fusion Middleware Application Security Guide*, Part Number E55398-01, 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.

### 5.2.3 Incorrect Link to ILM Content

In the *Oracle Fusion Middleware Application Security Guide*, part number E55398-01, 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

# 6

# Oracle Directory Integration Platform

This chapter describes issues associated with Oracle Directory Integration Platform. It includes the following topics:

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

## 6.1 General Issues and Workarounds

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

- Enabling the Domain-Wide Administration Port on Oracle WebLogic Server Prevents use of the DIP Command Line Interface
- LDIF Files That Contain Non-ASCII Characters Will Cause the testProfile Command Option to Fail if the LDIF File has Native Encoding
- Running the testProfile Command with LDIF Files Option Fails in Advance Mode
- Some Changes May Not Get Synchronized Due to Race Condition in Heavily-Loaded Source Directory
- manageSyncProfiles Utility Prompts for Wrong Password
- Schema Error Messages may Appear after Upgrade

### 6.1.1 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.

### 6.1.2 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 the section "10.1.5.2 Running DIP Tester From the WLST Command-Line Interface" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

### 6.1.3 Running the testProfile Command with LDIF Files Option Fails in Advance Mode

When running DIP Tester from a command-line in advance mode, the `manageSyncProfiles testProfile` command will fail if the `-ldiffile` option is specified and may synchronize the wrong operation. To resolve this issue, run the `manageSyncProfile updatechgnum` command.

For more information, see the section "10.1.5.2 Running DIP Tester From the WLST Command-Line Interface" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

### 6.1.4 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.

> **Note:** This issue only occurs if you are using Oracle Internet Directory as the back-end directory.

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.

### 6.1.5 manageSyncProfiles Utility Prompts for Wrong Password

When you run the `manageSyncProfiles` utility to synchronize with a database, the `manageSyncProfiles register` prompts for the connected directory password. Ensure that you specify the connected database password and not the directory password.

### 6.1.6 Schema Error Messages may Appear after Upgrade

After upgrading from Oracle Directory Integration Platform 11.1.1.7.0 environment, when you run the `dipConfigurator update` command successfully, it may throw schema error messages. You can ignore these messages.

> **Note:** This issue only occurs if you are using Oracle Unified Directory or Oracle Directory Server Enterprise Edition as the back-end directory.

## 6.2 Configuration Issues and Workarounds

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

- If Oracle Internet Directory is the Back-End Directory then do not use localhost as Oracle Internet Directory Hostname When Configuring Oracle Directory Integration Platform
- You may Need to Restart the Directory Integration Platform After Running dipConfigurator Against Oracle Unified Directory
- When Configuring a Profile, you may Need to Scroll Past a Section of Whitespace to View Mapping Rules
- Resource Usage Charts will not Display if Multiple IDM Domains are Running on the Same Host

### 6.2.1 If Oracle Internet Directory is the Back-End Directory then 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.

### 6.2.2 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.

### 6.2.3 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.

### 6.2.4 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.

## 6.3 Provisioning Issues

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

- Modification may not Propagate Using Interface Protocol (Inbound) Version 3.0
- Provisioning from Oracle Internet Directory (Back-End Directory) to an Application May Fail

### 6.3.1 Modification may not Propagate Using Interface Protocol (Inbound) Version 3.0

When an inbound provisioning profile with interface protocol version 3.0 is configured with Oracle Internet Directory (Back-End Directory), then modification fails to propagate. For more information, see `http://support.oracle.com/`.

### 6.3.2 Provisioning from Oracle Internet Directory (Back-End Directory) to an Application May Fail

If you delete a provisioning profile for Oracle Internet Directory, and recreate it with same name, then the provisioning from Oracle Internet Directory to an application may fail. To resolve this issue, create a provisioning profile and specify a new name. For more information on creating a provisioning profile, see "Managing Provisioning Profiles Using manageProvProfiles" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

## 6.4 Documentation Errata

There are no known documentation issues at this time.

# 7 Oracle Virtual Directory

This chapter describes issues associated with Oracle Virtual Directory.

This chapter includes the following topics:

## 7.1 General Issues and Workarounds

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

### 7.1.1 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.

### 7.1.2 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.

### 7.1.3 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.

### 7.1.4 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.

### 7.1.5 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.

### 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 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.

To work around this issue, 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.

### 7.1.8 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.

### 7.1.9 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

### 7.1.10 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)

#### 7.1.10.1 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 7–1 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 7–2 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.

## 7.1.11 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 issue, 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*.

## 7.1.12 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.

### 7.1.13 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.

### 7.1.14 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.

### 7.1.15 ODSM Version 11.1.1.7.0 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.

### 7.1.16 ODSM Version 11.1.1.9.0 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, 11.1.1.6.0, or 11.1.1.7.0

Oracle Directory Services Manager Version 11.1.1.9.0 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, 11.1.1.6.0, or 11.1.1.7.0.

Changes introduced in Oracle Directory Services Manager Version 11.1.1.9.0 improve configuration auditing, and these changes require that you use Oracle Virtual Directory 11.1.1.9.0.

### 7.1.17 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.

### 7.1.18 Creating an Attribute/Object Class Throws NPE Error

After upgrading Oracle Directory Services Manager, creating an attribute or an objectclass causes an NPE error.

To work around this issue, refresh the entries by clicking **Refresh** every time the creation fails.

### 7.1.19 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.

### 7.1.20 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.

### 7.1.21 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.

### 7.1.22 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.

### 7.1.23 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.

### 7.1.24 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.

### 7.1.25 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.

### 7.1.26 Online Help Section is Not Working

The Oracle Directory Services Manager online help section does not work in Internet Explorer 10 (IE10) web browsers.

### 7.1.27 Protocol Error LDAPException in ODSM-OVD after Changing OVD Config and Restart

If you modify Oracle Virtual Directory server configuration properties in Enterprise Manager, restart Oracle Virtual Directory through Enterprise Manager, and then try to view the Oracle Virtual Directory container in ODSM, then a protocol error LDAPException occurs.

To work around this issue, perform a command-line search before viewing Oracle Virtual Directory in ODSM.

### 7.1.28 Java Runtime Environment Has SSLv3 Disabled By Default

Starting with JDK 7u75 and JDK 6u91, the Java Runtime Environment has SSLv3 disabled by default. For more information about this change, see `http://www.oracle.com/technetwork/java/javase/documentation/cve-2014-3566-2342133.html`.

If you apply either of these Java updates, then any attempt to connect to Oracle Virtual Directory with SSLv3 will fail.

To work around this issue, configure the client LDAP application to use a different protocol. You may need to check whether any fixes are available that enable your client LDAP application to use a different protocol.

## 7.2 Configuration Issues and Workarounds

There are no known configuration issues at this time.

## 7.3 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
- targetDNfilter Samples Do Not Work

### 7.3.1 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*.

### 7.3.2 targetDNfilter Samples Do Not Work

The following sample values, as noted in the "Configuration Parameters" **targetDNfilter** section of the *Oracle® Fusion Middleware Administrator's Guide for Oracle Virtual Directory*, do not work and should be removed.

- *,cn=xxx,dc=yyy
- *cn=xxx,dc=yyy

Only the cn=xxx,dc=yyy format is supported.