

Oracle Identity Governance Bundle Patch Readme

This document is intended for users of OIM BUNDLE PATCH 12.2.1.4.200624. It contains the following sections:

 **Note:**

For issues documented after the release of OIM BUNDLE PATCH 12.2.1.4.200624, see My Oracle Support Document 2602696.1 at <https://support.oracle.com/>.

- [Understanding Bundle Patches](#)
- [Recommendations](#)
- [Bundle Patch Requirements](#)
- [Prerequisites of Applying the Bundle Patch](#)
- [Applying the Bundle Patch to an Existing Instance](#)
- [Removing the Bundle Patch](#)
- [Applying the Bundle Patch to a New Instance](#)
- [Changes in Track Request Functionality](#)
- [Resolved Issues](#)
- [Known Issues and Workarounds](#)
- [Related Documents](#)
- [Documentation Accessibility](#)

Understanding Bundle Patches

This section describes bundle patches and explains differences between bundle patches, patch set exceptions (also known as one-offs), and patch sets.

- [Stack Patch Bundle](#)
- [Bundle Patch](#)
- [Patch Set Exception](#)
- [Patch Set](#)

Stack Patch Bundle

Stack Patch Bundle deploys the IDM product and dependent FMW patches using a tool. For more information about these patches, see *Quarterly Stack Patch Bundles (Doc ID 2657920.1)* at <https://support.oracle.com>.

Bundle Patch

A bundle patch is an official Oracle patch for an Oracle product. In a bundle patch release string, the fifth digit indicated the bundle patch number. Effective November 2015, the version numbering format has changed. The new format replaces the numeric fifth digit of the bundle version with a release date in the form "YYMMDD" where:

- YY is the last 2 digits of the year
- MM is the numeric month (2 digits)
- DD is the numeric day of the month (2 digits)

Each bundle patch includes the libraries and files that have been rebuilt to implement one or more fixes. All of the fixes in the bundle patch have been tested and are certified to work with one another. Regression testing has also been performed to ensure backward compatibility with all Oracle Mobile Security Suite components in the bundle patch.

Patch Set Exception

In contrast to a bundle patch, a patch set exception addressed only one issue for a single component. Although each patch set exception was an official Oracle patch, it was not a complete product distribution and did not include packages for every component. A patch set exception included only the libraries and files that had been rebuilt to implement a specific fix for a specific component.

Patch Set

A patch set is a mechanism for delivering fully tested and integrated product fixes. A patch set can include new functionality. Each patch set includes the libraries and files that have been rebuilt to implement bug fixes (and new functions, if any). However, a patch set might not be a complete software distribution and might not include

packages for every component on every platform. All of the fixes in a patch set are tested and certified to work with one another on the specified platforms.

Recommendations

Oracle has certified the dependent Middleware component patches for Identity Management products and recommends that you apply these certified patches. For more information about these patches, see *Certification of Underlying or Shared Component Patches for Identity Management Products (Doc ID 2627261.1)* at <https://support.oracle.com>.

Bundle Patch Requirements

You must satisfy the following requirements before applying this bundle patch:

- Verify that you are applying this bundle patch to an Oracle Identity Governance 12.2.1.4.0 installation.

 **Note:**

When installing OPatch, you might find that interim or one off patches have already been installed.

- Download the latest version of OPatch. The OPatch version for this bundle patch is 13.9.4.2.2. However, Oracle recommends using the latest version of OPatch to all customers. To learn more about OPatch and how to download the latest version, refer to the following:

You can access My Oracle Support at <https://support.oracle.com>.

- Verify the OUI Inventory. To apply patches, OPatch requires access to a valid OUI Inventory. To verify the OUI Inventory, ensure that ORACLE_HOME/OPatch appears in your PATH for example:

```
export PATH=ORACLE_HOME/OPatch:$PATH
```

Then run the following command in OPatch inventory

```
opatch lsinventory
```

If the command returns an error or you cannot verify the OUI Inventory, contact Oracle Support. You must confirm the OUI Inventory is valid before applying this bundle patch.

- Confirm the `opatch` and `unzip` executables exist and appear in your system PATH, as both are needed to apply this bundle patch. Execute the following commands:

```
which opatch
which unzip
```

Both executables must appear in the PATH before applying this bundle patch.

- Ensure that there are no pending JMS messages in Oracle Identity Governance server. You can monitor JMS messages with WebLogic console.

Applying the Bundle Patch to an Existing Instance

Applying OIM BUNDLE PATCH 12.2.1.4.200624 is done in the following stages:

Note:

Before performing the steps to apply the bundle patch, create a backup of the database, as stated in [Prerequisites of Applying the Bundle Patch](#) which will help you roll back to the previous release.

- [Patching the Oracle Binaries \(OPatch Stage\)](#)
- [Stage 2: Filling in the patch_oim_wls.profile File](#)
- [Stage 3: Patching the Oracle Identity Governance Managed Servers \(patch_oim_wls Stage\)](#)
- [Understanding the Process Sequence With an Example](#)

Patching the Oracle Binaries (OPatch Stage)

This section describes the process of applying the binary changes by copying files to the `ORACLE_HOME` directory, on which Oracle Identity Governance is installed. This step must be executed for each `ORACLE_HOME` in the installation topology nodes irrespective of whether Oracle Identity Governance server is being run in the node or not.

Perform the following steps to apply the bundle patch to an existing Oracle Identity Governance instance:

1. Stop the Admin Server, all Oracle Identity Governance managed servers, and all SOA managed servers.
2. Create a directory for storing the unzipped bundle patch. This document refers to this directory as `PATCH_TOP`.

3. Unzip the patch zip file in to the PATCH_TOP directory you created in step 2 by using the following command:

```
unzip -d PATCH_TOP p31537918_122140_Generic.zip
```

 **Note:**

On Windows, the unzip command has a limitation of 256 characters in the path name. If you encounter this issue, use an alternate ZIP utility, for example 7-Zip to unzip the zip file.

Run the below command to unzip the file:

```
"c:\Program Files\7-Zip\7z.exe" x p31537918_122140_Generic.zip
```

4. Move to the directory where the patch is located. For example:

```
cd PATCH_TOP/31537918
```

5. Set the ORACLE_HOME directory in your system. For example:

```
setenv ORACLE_HOME /u01/Oracle/Middleware
```

6. Ensure that the OPatch executables are present in your system PATH. To update the PATH environment variable to include the path of Opatch directory, run the following command:

```
export PATH=$ORACLE_HOME/Opatch:$PATH
```

7. Apply the bundle patch to the ORACLE_HOME using the following command for Oracle Identity Governance:

```
opatch apply
```

 **Note:**

If OPatch fails with error code 104, cannot find a valid oraInst.loc file to locate Central Inventory, include the -invPtrLoc argument, as follows:

```
opatch apply -invPtrLoc ORACLE_HOME/oraInst.loc
```

When OPatch starts, it will validate the patch and ensure there are no conflicts with the software already installed in the ORACLE_HOME. OPatch categorizes two types of conflicts:

- Conflicts with a patch already applied to the ORACLE_HOME. In this case, stop the patch installation and contact Oracle Support.

- Conflicts with subset patch already applied to the ORACLE_HOME. In this case, continue the install, as the new patch contains all the fixes from the existing patch in the ORACLE_HOME. The subset patch will automatically be rolled back prior to the installation of the new patch.

 **Note:**

For clustered and multi-node installation of Oracle Identity Governance, this step must be run on all the ORACLE_HOME directories on which Oracle Identity Governance is installed.

8. Start all the servers in the OIG domain, which are the Admin Server, SOA Server, and Oracle Identity Governance Server.

Stage 2: Filling in the patch_oim_wls.profile File

Using a text editor, edit the file `patch_oim_wls.profile` located in the directory `ORACLE_HOME/idm/server/bin/` directory and change the values in the file to match your environment. The `patch_oim_wls.profile` file contains sample values.

[Table 1-1](#) lists the information to be entered for the `patch_oim_wls.profile` file. This file is used in next stage of the bundle patch process.

Table 1-1 Parameters of the patch_oim_wls.profile File

Parameter	Description	Sample Value
ant_home	Location of the ANT installation. It is usually under MW_HOME.	For Linux: \$MW_HOME/ oracle_common/modules/ thirdparty/org.apache.ant/ 1.10.5.0.0/apache-ant-1.10.5/ For Windows: %MW_HOME%/ oracle_common/modules/ thirdparty/org.apache.ant/ 1.10.5.0.0/apache-ant-1.10.5/
java_home	Location of the JDK/JRE installation that is being used to run the Oracle Identity Governance domain.	For Linux: <JAVA_HOME_PATH> consumed by \$MW_HOME For Windows: <JAVA_HOME_PATH> consumed by %MW_HOME%
mw_home	Location of the middleware home location on which Oracle Identity Governance is installed.	For Linux: /u01/Oracle/ Middleware For Windows: C:\Oracle\MW_HOME\
oim_oracle_home	Location of the Oracle Identity Governance installation.	For Linux: \$MW_HOME/idm For Windows: %MW_HOME% \idm

Table 1-1 (Cont.) Parameters of the patch_oim_wls.profile File

Parameter	Description	Sample Value
soa_home	Location of the SOA installation.	For Linux: \$MW_HOME/soa For Windows: %MW_HOME%\soa
weblogic.server.dir	Directory on which WebLogic server is installed.	For Linux: \$MW_HOME/wlserver For Windows: %MW_HOME%\wlserver
domain_home	Location of the domain home on which Oracle Identity Governance is installed.	\$MW_HOME/user_projects/domains/base_domain
weblogic_user	Domain administrator user name. Normally it is weblogic, but could be different as well.	weblogic
weblogic_password	Domain admin user's password. If this line is commented out, then password will be prompted.	NA
soa_host	Listen address of the SOA Managed Server, or the hostname on which the SOA Managed Server is listening. Note: If the SOA Managed Server is configured to use a virtual IP address, then the virtual host name must be supplied.	oimhost.example.com
soa_port	Listen port of the SOA Managed Server, or SOA Managed Server port number.	8001 Only Non-SSL Listen port must be provided.
operationsDB.user	Oracle Identity Governance database schema user.	DEV_OIM
OIM.DBPassword	Oracle Identity Governance database schema password. If this line is commented out, then the password will be prompted when the script is executed.	NA
operationsDB.host	Host name of the Oracle Identity Governance database.	oimdbhost.example.com
operationsDB.serviceName	Database service name of the Oracle Identity Governance schema/database. This is not the hostname and it can be a different value as well.	oimdb.example.com

Table 1-1 (Cont.) Parameters of the patch_oim_wls.profile File

Parameter	Description	Sample Value
operationsDB.port	Database listener port number for the Oracle Identity Governance database.	1521
mdsDB.user	MDS schema user	DEV_MDS
mdsDB.password	MDS schema password. If this line is commented out, then password will be prompted.	NA
mdsDB.host	MDS database host name	oimdbhost.example.com
mdsDB.port	MDS database/Listen port	1521
mdsDB.serviceName	MDS database service name	oimdb.example.com
oim_username	Oracle Identity Governance username.	System administrator username
oim_password	Oracle Identity Governance password. This is optional. If this is commented out, then you will be prompted for the password when the script is executed.	NA
oim_serverurl	URL to navigate to Oracle Identity Governance.	t3:// oimhost.example.com:14000
wls_serverurl	URL to navigate to WLS Console	t3:// wlshost.example.com:7001
opss_customizations_present =false	Enables customizations related to authorization or custom task flow. Set this value to true to enable customization.	true

 **Note:**

Updated the parameter value as per the setup used and then execute the patch_oim_wls.sh file.

Stage 3: Patching the Oracle Identity Governance Managed Servers (patch_oim_wls Stage)

Patching the Oracle Identity Governance managed servers is the process of copying the staged files in the previous steps (stage 1) to the correct locations, and running SQL scripts and importing event handlers and deploying SOA composite. For making MBean calls, the script automatically starts the Oracle Identity Governance Managed Server and SOA Managed Server specified in the patch_oim_wls.profile file.

This step is performed by running `patch_oim_wls.sh` (on UNIX) and `patch_oim_wls.bat` (on Microsoft Windows) script by using the inputs provided in the `patch_oim_wls.profile` file. As prerequisites, the WebLogic Admin Server, SOA Managed Servers, and Oracle Identity Governance Managed Server must be running.

To patch Oracle Identity Governance Managed Servers on WebLogic:

1. Make sure that the WebLogic Admin Server, SOA Managed Servers, and Oracle Identity Governance Managed Server are running.
2. Set the following environment variables:

For LINUX or Solaris, set the `JAVA_HOME` environment variable:

```
export JAVA_HOME=<JAVA_HOME_PATH>
export PATH=$JAVA_HOME/bin:$PATH
```

For Microsoft Windows:

```
set JAVA_HOME=<JAVA_HOME_PATH>
set ANT_HOME=\PATH_TO_ANT_DIRECTORY\ant
set ORACLE_HOME=%MW_HOME%\idm
```

 **Note:**

Make sure to set the reference to JDK binaries in your `PATH` before running the `patch_oim_wls.sh` (on UNIX) or `patch_oim_wls.bat` (on Microsoft Windows) script. This `JAVA_HOME` must be of the same version that is being used to run the WebLogic servers. The `JAVA_HOME` version from `/usr/bin/` or the default is usually old and must be avoided. You can verify the version by running the following command:

```
java -version
```

3. Execute `patch_oim_wls.sh` (on UNIX) or `patch_oim_wls.bat` (on Microsoft Windows) to apply the configuration changes to the Oracle Identity Governance server. On Linux systems, you must run the script in a shell environment using the following command:

```
sh patch_oim_wls.sh
```

 **Note:**

For EDG implementations, this script must be run against the `mserver` domain directory rather than the `server` domain directory.

4. Delete the following directory from OIG domain home:
`$DOMAIN_HOME/servers/oim_server1/tmp/_WL_user/
oracle.iam.console.identity.self-service.ear_V2.0`
Here, `oim_server1` is the weblogic managed server used for OIG.
5. To verify that the `patch_oim_wls` script has completed successfully, check the `ORACLE_HOME/idm/server/bin/patch_oim_wls.log` log file.

 **Note:**

On running the `patch_oim_wls` script, the `$DOMAIN_HOME/servers/MANAGED_SERVER/security/boot.properties` file might be deleted. If you use a script to start the Managed Server and use the `boot.properties` file to eliminate the need of entering the password in the script, then create a new `boot.properties` file.

In an EDG environment, the `boot.properties` file is in `MSERVER_HOME/servers/MANAGED_SERVER/security`.

6. Stop and start WebLogic Admin Server, SOA Server, and Oracle Identity Governance Server.
 - Shutting down Oracle Identity Governance server might take a long time if it is done with `force=false` option. It is recommended that you force shutdown Oracle Identity Governance server.
 - The `patch_oim_wls` script is re-entrant and can be run again if a failure occurs.

Understanding the Process Sequence With an Example

If you have `ORACLE_HOME_A` and `ORACLE_HOME_B`, and `ORACLE_HOME_A` is running WebLogic Admin Server, `oim_server1`, and `soa_server1`, and `ORACLE_HOME_B` is running `oim_server2` and `soa_server2`, then the following is the process sequence to apply the bundle patch to the Oracle Identity Governance instance:

1. Shutdown the Oracle Identity Governance, and ensure that the WebLogic Admin Server and SOA managed servers are running.
2. Run 'Opatch apply' on `ORACLE_HOME_A`. See [Patching the Oracle Binaries \(OPatch Stage\)](#) for more information.
3. Run 'Opatch apply' on `ORACLE_HOME_B`. See [Patching the Oracle Binaries \(OPatch Stage\)](#) for more information.
4. Fill-in the `patch_oim_wls.profile` file and run `patch_oim_wls` on `ORACLE_HOME_A` or `ORACLE_HOME_B`.

See [Stage 2: Filling in the patch_oim_wls.profile File](#) for information on filling in the `patch_oim_wls.profile`.

See [Stage 3: Patching the Oracle Identity Governance Managed Servers \(patch_oim_wls Stage\)](#) for information about running `patch_oim_wls`.

5. Restart the managed servers on all the nodes.

Removing the Bundle Patch

If you must remove the bundle patch after it is applied, then perform the following steps:

Note:

For clustered installations, perform steps 1 through 3 on all nodes in the cluster.

1. Perform the same verification steps and requirement checks that you made before applying the bundle patch. For example, backup the XML files and import them to a different location, verify the OUI Inventory and stop all services running from the ORACLE_HOME.
2. Move to the directory where the bundle patch was unzipped. For example:

```
cd PATCH_TOP/31537918
```

3. Run OPatch as follows to remove the bundle patch:

```
opatch rollback -id 31537918
```

4. Restore ORACLE_HOME, the WebLogic domain home from the backup created before applying the patch.
5. Restore the Oracle Identity Governance database using the backup you created in Step 1 of [Applying the Bundle Patch to an Existing Instance](#).
6. Start all servers in OIG domain, which are WebLogic Admin Server, SOA Server, and Oracle Identity Governance Server.

Applying the Bundle Patch to a New Instance

Perform the following steps to apply the bundle patch to a new instance:

- [Installing a New Oracle Identity Governance Instance with OIM BUNDLE PATCH 12.2.1.4.200624](#)
- [Updating Oracle Identity Governance Web Applications](#)
- [Prerequisites of Applying the Bundle Patch](#)

Installing a New Oracle Identity Governance Instance with OIM BUNDLE PATCH 12.2.1.4.200624

You can install a new Oracle Identity Governance instance with the bundle patch in any one of the following ways:

- [Using the Quickstart Installer](#)
- [Using the Generic Installer](#)

Using the Quickstart Installer

To install a new instance of Oracle Identity Governance with the bundle patch by using the Quickstart installer:

Note:

For clustered deployments, perform the steps provided in this section on each node in the cluster.

1. Start the installation by referring to [Installing Oracle Identity Governance Using Quickstart Installer](#) of *Installing and Configuring Oracle Identity and Access Management*. Before creating the database schema, apply the patch by using OPatch, as described in [Patching the Oracle Binaries \(OPatch Stage\)](#). Then, continue with schema creation.

Note:

It is recommended that this step is performed before creating or extending the domain with Oracle Identity Governance.

2. Create the domain by launching the configuration wizard, as specified in [Configuring and Updating the Oracle Identity Governance Domain](#) of *Installing and Configuring Oracle Identity and Access Management*.
3. Run the `offlineConfigManager` command to perform post configuration tasks. See [Running the Offline Configuration Command](#) in *Installing and Configuring Oracle Identity and Access Management*.
4. Start the WebLogic Admin Server, SOA Server, and OIG server.
5. Verify that you are able to log in to Oracle Identity Self Service or Oracle Identity System Administration.
6. Login to Oracle Enterprise Manager Fusion Middleware Control, and invoke the `OIMSOAIntegrationMBean` to integrate OIG with SOA. See [Integrating Oracle Identity Governance with Oracle SOA Suite](#) in *Installing and Configuring Oracle Identity and Access Management*.

Using the Generic Installer

To install a new instance of Oracle Identity Governance with the bundle patch by using the generic installer:

 **Note:**

For clustered deployments, perform the steps provided in this section on each node in the cluster.

1. Start the installation by referring to [Configuring the Oracle Identity Governance Domain](#) of *Installing and Configuring Oracle Identity and Access Management*. Before creating the database schema, apply the patch by using Opatch, as described in [Patching the Oracle Binaries \(OPatch Stage\)](#). Then, continue with schema creation.

 **Note:**

It is recommended that this step is performed before creating or extending the domain with Oracle Identity Governance.

2. Create the domain by launching the configuration wizard, as specified in [Configuring the Domain](#) of *Installing and Configuring Oracle Identity and Access Management*.
3. Run the `offlineConfigManager` command to perform post configuration tasks. See [Running the Offline Configuration Command](#) in *Installing and Configuring Oracle Identity and Access Management*.
4. Start the WebLogic Admin Server, SOA Server, and OIG server.
5. Verify that you are able to log in to Oracle Identity Self Service or Oracle Identity System Administration.
6. Login to Oracle Enterprise Manager Fusion Middleware Control, and invoke the `OIMSOAIntegrationMBean` to integrate OIG with SOA. See [Integrating Oracle Identity Governance with Oracle SOA Suite](#) in *Installing and Configuring Oracle Identity and Access Management*.

Updating Oracle Identity Governance Web Applications

The procedure described in this section is applicable only when installing bundle patches for Oracle Identity Governance and not for installing patch set updates.

For updating your web applications on Oracle WebLogic Server:

1. Stop Oracle Identity Governance Managed Server.
2. Login to WebLogic Administrative Console.
3. Click **Lock & Edit**.
4. Go to **Deployments**.

5. Select the **oracle.iam.ui.view** and **oracle.iam.ui.model** app, and click **Update**. Complete the steps of the wizard by clicking **Next**. Do not change anything.
6. Click **Apply Changes**.
7. Start Oracle Identity Governance Managed Server.

Prerequisites of Applying the Bundle Patch

Before applying the bundle patch, perform the following prerequisites:

- This patch process makes changes to Oracle Identity Governance database schema (such as adding/modifying data), Oracle Identity Governance Meta Data Store (MDS) database schema (such as adding/modifying data), domain configuration changes, and other binary changes in the file system under ORACLE_HOME on which Oracle Identity Governance is installed. It is mandatory to create a backup of the following:
 - Oracle Identity Governance, MDS, and Service-Oriented Architecture (SOA) database schemas. For example, the database schema can be DEV_OIM, DEV_MDS schemas used by Oracle Identity Governance. Simple export of the schemas is sufficient.
 - The ORACLE_HOME directory on which Oracle Identity Governance is installed, for example, /u01/Oracle/Middleware.
 - Oracle Identity Governance WebLogic Domain location, for example, /u01/Oracle/Middleware/user_projects/domains/IAMGovernanceDomain/.
 - The UNIX user applying opatch must have read, write, and execute permissions on both ORACLE_HOME as well as WEBLOGIC_DOMAIN_HOME. You can verify this manually in the file system for DOMAIN_HOME and ORACLE_HOME.
- If you have customized the event handler file metadata/iam-features-configservice/event-definition/EventHandlers.xml in your setup, then perform the following steps to ensure that the upgrade does not override any customization done to this file:
 1. Export the metadata/iam-features-configservice/event-definition/EventHandlers.xml file from MDS, and create a backup of this file.
 2. After upgrading and running all the post install steps, export the new metadata/iam-features-configservice/event-definition/EventHandlers.xml file, merge your customization to this new file, and import it back to MDS.

Note:

For more information on MDS Utilities, see [MDS Utilities and User Modifiable Metadata Files](#).

Changes in Track Request Functionality

Track Request functionality will change after this Bundle Patch is applied.

When a user performs a search in Self Service tab, Track Requests page, and in the search result table, applies Show list option as **For Reportees**, all the requests raised by or for the logged in user and user's direct and indirect reportee are displayed.

 **Note:**

- The Organization Name field works only with the For Reportees feature.
- While using the Organization Name search criteria, at least one direct reportee should be associated with the organization. See [Errors Related to the For Reportees Feature](#) for the error message that is displayed when an organization name outside the reportee's organization is entered.
- Only two levels of reportees are considered, direct reportees and their immediate reportees
- The total number of direct reportees and indirect reportees must not exceed 1000. See [Errors Related to the For Reportees Feature](#) for the error message that is displayed if the number of direct reportees and indirect reportees are more than 1000.

Resolved Issues

The following section lists the issues resolved in Release 12.2.1.4.200624:

- [Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200624](#)
- [Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200505](#)
- [Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200206](#)

Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200624

Applying this bundle patch resolves the issues described in [Table 1-2](#).

Table 1-2 Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200624

Bug Number	Description
29055661	PASSWORD POLICY DOES NOT MATCH BETWEEN OIM AND AD CAUSING ISSUES DURING PASSWORD SYNC
30007378	REASSIGN THE REVIEWER ON CERTIFICATION FAILED ON PREVENTING SELF CERTIFICATION
30097140	SLOWNESS OPENING USER DETAILS ADMIN ROLES TAB
30153927	APPROVAL DETAILS INCORRECT AFTER REVOKING ROLE BY XELSYSADMIN AND ANOTHER USER

Table 1-2 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200624

Bug Number	Description
30216857	SETCHALLENGERESPONSESFORLOGGEDINUSER - CHALLENGE QUESTIONS PROVIDED ARE NOT DEFINED
30343249	WHILE DELETING ORGANIZATION USERS REMAIN IN ACTIVE STATE
30343784	ACCESS POLICY NOT REVOKING ENTITLEMENTS ON ALREADY DISABLED USERS
30376706	ROLEMANAGER GRANTROLE SQLEXCEPTION: EXCEEDED MAXIMUM VARRAY LIMIT
30391615	ROLE WITH RULE FOR DATE FIELD IS NOT ASSIGNED TO USER
30420218	OIM/OAM INTEGRATION USER SESSION LOST AFTER ANY USER DATA EDITED
30439939	AP HARVESTING DOES NOT WORK FOR RESOURCES WITH MULTIPLE PROVISIONING WORKFLOWS
30506899	DELETE RECONCILIATION LEAVES PROVISIONING OPEN TASKS IN LIMBO STATE.
30517366	DELEGATE THE REVIEWER ON CERTIFICATION FAILED ON PREVENTING SELF CERTIFICATION
30757297	DISCONNECTED APPLICATION NOT TRIGGERING UPDATE TASK ON CHILD FORM
30788834	DIAG: NEED SOME TRACE LOGGING IN THE SCIM FUNCTIONALITY
30896936	PUMA: CUSTOM MESSAGE NOT DISPLAYED WHEN COMPLETING MANUAL TASK
31184149	PERFORMANCE ISSUE IN OIMDATAPROVIDER.GETARRAYFORHIERAR
31477738	UNABLE TO CREATE RULE MEMBERSHIP WITH DATE DATA TYPE

Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200505

Applying this bundle patch resolves the issues described in [Table 1-3](#).

Table 1-3 Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200505

Bug Number	Description
27074256	OIM-OAM-OID: SSO USER FULL RECONCILIATION DO NOT DELETE USER
27216374	OIM-OAM-AD: SSO GROUP HIERARCHY SYNC FULL RECON DO NOT WORK
30257502	USER SESSION IS NOT TERMINATED IN UPGRADED 12CPS4 ENV

Table 1-3 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200505

Bug Number	Description
30327749	ROLES CREATED IN OIM ARE SHOWN AS ENTITLEMENT IN CATALOG SEARCH
30330170	LDAP USER DELETE RECON JOB NOT AVAILABLE
30330745	ISSUE WITH USER-ROLE MEMBERSHIP RECON
30354276	REMOVE LDAPSYNC RELATED JOBS IN CONNECTOR BASED 12CPS4 OAM-OIG ENV
30555995	SSOTARGET AND SSOTRUSTED-FOR-SSOTARGET SHOULD NOT BE AVAILABLE FOR OTHER OIM OPERATIONS SUCH AS REQUEST
30654239	USER NOT SEEN IN USER CONTAINER AFTER APPROVING THE USER REG REQUEST IN ROLLING UPG ENV(11G-12CPS3-12CPS4))
30654620	USER NOT SHOWN AS LOCKED IN OIM AFTER PROVIDING WRONG PASSWORDS IN ROLLING UPG ENV(11G-12CPS3-12CPS4)
30654852	ROLE CREATED IN OIM IS NOT SEEN IN LDAP IN ROLLING UPG ENV(11G-12CPS3-12CPS4)
30655208	ROLE CREATED IN OUD IS NOT SEEN IN OIM IN ROLLING UPG ENV (11G-12CPS3-12CPS4)
30655442	SESSION TERMINATION FAILING IN ROLLING UPG ENV (11G-12CPS3-12CPS4)
30655935	ROLLING UPG(11G-12CPS3-12CPS4): SSOTARGET APP INSTANCE DOES NOT HAVE ANY ENTITLEMENTS IN 12CPS4
30855442	NOT ABLE TO ADD MEMBER IN EXISTING ROLES IN AD ROLLING UPGRADE ENV (11G-12CPS3-12CPS4)
30855747	CAN NOT ADD ROLE HIERARCHY FOR EXISTING ROLES IN AD ROLLING UPGRADE ENV(11G-12CPS3-12CPS4)
30855892	CAN NOT DELETE EXISTING ROLES IN AD ROLLING UPGRADE ENV(11G-12CPS3-12CPS4)
30857219	SSO GROUP HIERARCHY SYNC FULL RECONCILIATION JOB AND SSO GROUP HIERARCHY SYNC INCREMENTAL RECONCILIATION JOB FAILING IN AD ROLLING UPGRADE ENV
30864002	EXECUTION OF SSO GROUP HIERARCHY SYNC FULL RECONCILIATION IS SHOWN AS FAILED IN OUD BASED ROLLING UPGRADE ENV
30864119	EXECUTION OF SSO GROUP MEMBERSHIP FULL RECONCILIATION IS SHOWN AS FAILED IN OUD BASED ROLLING UPGRADE ENV
30868468	MODIFICATIONS TO NEWLY CREATED USER IS FAILING IN AD ROLLING UPGRADE ENV
31190098	INTEROP OIM_OAM_OUD IS BROKEN AFTER APPLYING PATCH 31178096
31198576	TC_CB_SAFE_BUG20134996_DIFFCASEINGROUPLOOKUP_XEL SYSADM.DIF IN LRG_OIM_12CPS4_DB_CUSTOMER_1 TOPO

Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200206

Applying this bundle patch resolves the issues described in [Table 1-4](#).

Table 1-4 Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200206

Bug Number	Description
29942217	IMPLEMENT BLIND/FILTERED SEARCH "FOR A REPORTEE" FOR A MANAGER
29972923	STEPS TO ROLLBACK AUTOCOMMITTED DDL OPERATIONS IN DB
30325576	PARTIAL FIX FOR BUG 28777983
30680152	ORGANIZATION SEARCH IN TRACK REQUESTS PAGE: ALL REQUESTS NOT DISPLAYED FOR ORGANIZATION NAME SEARCH IF NUMBER OF REQUESTS GREATER THAN 25
30680286	ORGANIZATION SEARCH IN TRACK REQUESTS PAGE: DOES NOT EQUAL OPERATOR NOT WORKING AS EXPECTED
30717520	ORGANIZATION SEARCH IN TRACK REQUESTS PAGE: BENEFICIARY NAME NOT LISTED

Known Issues and Workarounds

Known issues and their workarounds in Oracle Identity Governance Release 12.2.1.4.0 are described in the Oracle Identity Governance chapter of the *Release Notes for Oracle Identity Management* document. You can access the Release Notes document in the Oracle Identity Management Documentation library at the following URL:

<https://docs.oracle.com/en/middleware/idm/suite/12.2.1.4/idmrrn/index.html>

Note:

Some known issues listed in the Release Notes for Oracle Identity Management may have been resolved by this Bundle Patch (OIM BUNDLE PATCH 12.2.1.4.200624). Compare the issues listed in [Resolved Issues](#) of this document when reviewing the *Release Notes for Oracle Identity Management*.

This section describes the issues and workarounds in this BP release of Oracle Identity Governance:

- [Errors Related to the For Reportees Feature](#)
- [Identity Self Service and Identity System Administration Not Accessible](#)

Errors Related to the For Reportees Feature

While using the Organization Name search criteria, at least one direct reportee should be associated with the organization. When organization name outside the reportee's organization is entered, the following error message is displayed:

```
IAM-2053037 : An error occurred while searching for the reportees as the organization name is invalid or not associated with any reportee (This is EXPECTED). Atleast 1 direct reportee should belong to the org name being searched.
```

The total number of direct reportees and indirect reportees must not exceed 1000. For Reportees does not work if number of direct reportees and indirect reportees are more than 1000, and the following error message is displayed:

```
"IAM-2053036 : An error occurred while searching for the reportees as the reportee size exceeded the limit 1,200. Please retry with other search criteria"
```

Identity Self Service and Identity System Administration Not Accessible

After applying this bundle patch, OIG server deployments for Identity Self Service and Identity System Administration fails with `oracle.iam.ui.view` and `oracle.iam.ui.model` applications.

When you apply the bundle patch and update the Oracle Identity Governance web applications, the OIG system libraries `oracle.iam.ui.model(1.0,11.1.1.5.0)` and `oracle.iam.ui.view(11.1.1,11.1.1)` goes to the Prepared state. The `oracle.iam.console.identity.self-service.ear` and `oracle.iam.console.identity.sysadmin.ear` are referencing these two libraries, and therefore, cause the deployment failure.

To workaround this issues, manually delete the `oracle.iam.ui.model(1.0,11.1.1.5.0)` and `oracle.iam.ui.view(11.1.1,11.1.1)` libraries from deployments, and redeploy them in WebLogic Server Administration Console. To do so:

1. In WebLogic Server Administration Console, go to **Deployments**, and click **Lock and Edit**.
2. Select the **oracle.iam.ui.model(1.0,11.1.1.5.0)** library, and click **Delete**. Do the same for the **oracle.iam.ui.view(11.1.1,11.1.1)** library.
3. Click **Activate Changes**.
4. In Deployments, click **Lock and Edit**.
5. Click **Install**, install the `oracle.iam.ui.model(1.0,11.1.1.5.0)` as a library by following all the default settings, and select the OIM cluster/server as the target. Click **Finish and Save**. Repeat for the same for the `oracle.iam.ui.view(11.1.1,11.1.1)` library.
6. Click **Activate Changes**. The libraries are running in Active state.
7. In Deployments, click **Lock and Edit**, and then click the **Control** tab.
8. Select **oracle.iam.console.identity.sysadmin.ear**, which is in the Prepared state, and then select **Start / Serving all requests**.

9. Select **oracle.iam.console.identity.self-service.ear**, which is in the Prepared state, and then select **Start / Serving all requests**.
10. After the two applications go to the Active state, click **Release configuration**.

After the referenced libraries and the `oracle.iam.console.identity.self-service.ear` and `oracle.iam.console.identity.sysadmin.ear` applications go to the Active state, the system is up and running.

Related Documents

For more information, see the following resources:

- [Oracle Fusion Middleware Documentation](#)
This contains documentation for all Oracle Fusion Middleware 12c products.
- [Oracle Technology Network](#)
This site contains additional documentation that is not included as part of the documentation libraries.

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.

Oracle® Fusion Middleware Oracle Identity Governance Bundle Patch Readme, OIM BUNDLE PATCH 12.2.1.4.200624
F32653-02

Copyright © 2020, Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take

all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

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

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