Oracle® Fusion Middleware

Oracle Identity Governance Bundle Patch Readme

OIM BUNDLE PATCH 12.2.1.4.220703

F58867-01

July 2022

Oracle Identity Governance Bundle Patch Readme

This document is intended for users of OIM BUNDLE PATCH 12.2.1.4.220703. It contains the following sections:

> **Note:**
>
> For issues documented after the release of OIM BUNDLE PATCH 12.2.1.4.220703, 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
- Access Policy Harvesting to Enable Account Data Update
- Bulk Load Utility for Loading Accounts
- Steps to Map the Role and employeeType Attributes
- SSO Full User Reconciliation
- Major Enhancements in Bundle Patch 12.2.1.4.220413
- Major Enhancements in Bundle Patch 12.2.1.4.211010
- 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 13.9.4.2.5. 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 12.2.1.4.220703 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.

- Understanding the Process Sequence With an Example
- 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

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 server, WebLogic Admin Server, and SOA Managed Server.
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 with WebLogic Admin Server, oim_server1, and soa_server1 running. The rest of the servers on other nodes can be down.

   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.

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 p34345277_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 p34345277_122140_Generic.zip
   > ```

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

   ```
   cd PATCH_TOP/34345277
   ```

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.

> **Note:**
>
> For clustered and multinode installation of Oracle Identity Governance, perform the step described in this topic on the ORACLE_HOME_A directory on which Oracle Identity Governance is installed. This is because you need to run the `patch_oim_wls` script from the node with WebLogic Admin Server, oim_server1, and soa_server1 installed. In the `patch_wls_oim.profile` file, mention the host and port of the Oracle Identity Governance server and SOA server running on the first node. When you run the script, only WebLogic Admin Server, oim_server1, and soa_server1 should be running, and the rest of the servers can be down.

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
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

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

Parameter	Description	Sample Value
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
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

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

Parameter	Description	Sample Value
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
ATP-D	Set the value to false if DB type is not ATP-D. Set this to true if underlying DB type is ATP-D.	true
TNS_ADMIN	Set this value only if the value of ATP-D is true. Set this value to the TNS String as provided by DB Admin, for example, fmwatpdedic2_tp?TNS_ADMIN=/home/opc. Here, /home/opc is the path of the wallet zip that is downloaded. If you are using some other predefined service, then provide the path to that service.	fmwatpdedic2_tp?TNS_ADMIN=/home/opc

Note:

Update 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.

> **Note:**
>
> For clustered and multinode installation of Oracle Identity Governance, perform the steps described in this topic on the ORACLE_HOME_A directory on which Oracle Identity Governance is installed. In other words, run the `patch_oim_wls` script from the node with WebLogic Admin Server, oim_server1, and soa_server1 installed. When you run the script, only WebLogic Admin Server, oim_server1, and soa_server1 should be running, and the rest of the servers can be down.

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.

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/34345277
   ```

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

   ```
   opatch rollback -id  34345277
   ```

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.

> **Note:**
>
> - The newer CertificationProcess 2.2 version composite which is deployed as a post patch automation from this patch onwards needs to be undeployed if the patch is rolled back.
> - Previous version of the CertificationProcess composite must be activated.

You must adhere to the following list to undeploy the patch:

- You can no longer configure and monitor this revision of the application.

- You can no longer process instances of this revision of the application.
- The state of currently running instances is changed to aborted and no new messages sent to this composite are processed.
- The instance state of the undeployed composite application is set to aborted. The instance state is available in the instance listing, and you can access audit trail and flow trace details.
- If you undeploy the default revision of the SOA composite application (for example, 2.0), the next active, available revision of the application is automatically designated as the new default (for example, 1.0).
- A warning message is displayed at the end of this wizard when you undeploy the default composite revision.
  If no active revision is available and the default revision is undeployed, your composite may be unable to process new incoming requests. It is recommended that you have at least one active revision of this composite deployed before you undeploy the default revision.

  If you undeploy this revision and no active revisions of this composite are found, a retired revision is automatically designated as the new default revision. A warning message is displayed after this wizard closes. Although all currently executing instances complete normally in retired composites, they cannot process any incoming requests. To process new incoming requests for this composite after the current default revision is undeployed, you must deploy a new revision or reactivate a previously retired revision.

For information about instance, fault, and rejected message states that are updated to aborted during undeployment, see Updating Instance, Fault, and Rejected Message States to Aborted During Undeployment or Redeployment.

> **Note:**
>
> If you want to undeploy and then redeploy an existing revision of this application, do not use this wizard. Instead, use the Redeploy SOA Composite wizard. The Redeploy SOA Composite wizard enables you to redeploy an existing revision of a SOA composite application and remove (overwrite) the older, currently deployed version of the revision.

To undeploy applications:

> **Note:**
>
> You can undeploy multiple SOA composite applications together if they are located in the same SOA folder. For information, refer Managing SOA Folders and Work Manager Groups.

Once the current version is undeployed, previously retired composite needs to be activated. For more information, refer Managing the State of Deployed SOA Composite Applications.

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 Bundle Patch 12.2.1.3.180713
- Updating Oracle Identity Governance Web Applications
- Prerequisites of Applying the Bundle Patch

Installing a New Oracle Identity Governance Instance with Bundle Patch 12.2.1.3.180713

Perform the following steps to apply the bundle patch to a new Oracle Identity Governance instance. You can perform the same steps for clustered deployments.

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

1. Install Oracle WebLogic Server. See *Installing and Configuring Oracle Identity and Access Management* at the following URL:

   https://docs.oracle.com/en/middleware/idm/suite/12.2.1.3/inoam/index.html
2. Create the Oracle Identity Governance database schema. See *Installing and Configuring Oracle Identity and Access Management*.
3. Install SOA and Oracle Identity Governance. See *Installing and Configuring Oracle Identity and Access Management*.
4. Apply patch using Opatch, as described in Patching the Oracle Binaries (OPatch Stage).

   > **Note:**
   >
   > If you are creating a new environment, then it is recommended that this step is performed before creating or extending the domain with Oracle Identity Governance.
5. Create domain by launching configuration wizard as specified in the *Installing and Configuring Oracle Identity and Access Management*.
6. Start the WebLogic Admin Server and SOA Server.

Before starting the WebLogic Admin Server and SOA Server on Microsoft Windows, edit the startWeblogic.cmd file, and replace:

```
call "%COMMON_ORACLE_HOME%\bin\wlst.cmd"
%COMMON_ORACLE_HOME%\tools\configureSecurityStore.py -d
%DOMAIN_HOME% -m validate
```

With the following:

```
call "FULL_PATH_TO_WLST_SCRIPT\wlst.cmd"
%COMMON_ORACLE_HOME%\tools\configureSecurityStore.py -d
%DOMAIN_HOME% -m validate
```

Here, an example for *FULL_PATH_TO_WLST_SCRIPT* can be MW_HOME\oracle_common\common\bin\.

7. Use Oracle Universal Installer to configure Oracle Identity Governance by running config.sh.
8. Stop and restart the WebLogic Admin Server and SOA Server.
9. Fill in the patch_oim_wls.profile file by referring to Stage 2: Filling in the patch_oim_wls.profile File.
10. Run patch_oim_wls.sh (on UNIX) and patch_oim_wls.bat (on Microsoft Windows) to complete patching the domain. This step must be run on the ORACLE_HOME directory of the Oracle Identity Governance Managed Server. For more information, see Stage 3: Patching the Oracle Identity Governance Managed Servers (patch_oim_wls Stage).

> **Note:**
>
> Before running the patch_oim_wls script, make sure that WebLogic Admin server and SOA servers are in running state.

11. Stop and restart the WebLogic Admin Server, SOA Server, and Oracle Identity Governance server.

Postinstallation Configuration

After installing a new Oracle Identity Governance instance with Bundle Patch 12.2.1.3.180413, perform the following post installation configuration steps:

- Perform the following steps to seed the event handler for Application Onboarding:
  1. Go to, *MW_HOME*`/idm/server/apps/oim.ear/APP-INF/lib/`.
  2. Locate `BootStrapListener.jar`. Copy the `BootStrapListener.jar` file to a temporary folder, for example `temp_AoB`. Extract the jar files and locate `aob_adapters.xml` file in the `BootStrapListener.jar/scripts/` folder.

> **Note:**
>
> The jar file can be extracted using compression tool such as Zip,7–Zip or by using jar command `jar -xvf` .

3. Copy the `aob_adapters.xml` file to a local folder.
4. Using the Import option in Identity System Administration interface, import the `aob_adapters.xml` file into Oracle Identity Governance.

   For detailed steps for importing objects into Oracle Identity Governance, see Importing Deployments in *Administering Oracle Identity Governance*.
5. Remove the temporary folder `temp_AoB`.

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.

Access Policy Harvesting to Enable Account Data Update

As a fix for bug# 30978612 in the bundle patch, the new `XL.APHarvesting.AllowAccountDataUpdate` system property is available to update the account data with the policy defaults for the accounts linked to the access policies. This system property has the following details:

Name: `XL.APHarvesting.AllowAccountDataUpdate`

Keyword: `XL.APHarvesting.AllowAccountDataUpdate`

Default value: `FALSE`

When this system property is set to TRUE, the account data is updated with the policy defaults for the accounts linked to access policy. If set to FALSE or if the system property does not exist, the account data is not updated.

To enable updating the account data with the policy defaults for the accounts linked to the access policies, set the values of the `XL.APHarvesting.AllowAccountDataUpdate`, `XL.AllowAPHarvesting`, `XL.APHarvestRequestAccount`, `XL.APHarvestDirectProvisionAccount`, and `XL.AllowAPBasedMultipleAccountProvisioning` system properties to `TRUE`.

Bulk Load Utility for Loading Accounts

With the fix for bug# 30145982 in the bundle patch, the Bulk Load Utility for loading account data asks for the following input:

> **Note:**
>
> Running the Bulk Load Utility for account data has the following requirements:
>
> - Oracle Identity Governance server is running.
> - The `MW_HOME` and *`OIM_ORACLE_HOME`* paths must be accessible although they are running on different hosts.

1. Before running the utility, perform the following steps:
   a. Edit the oim_blkld_accounts.sh script, and add the following lines, and save the script.

      ```
      $MW_HOME/wlserver/server/lib/wlfullclient.jar
      $MW_HOME/oracle_common/modules/javax.management.j2ee.jar
      ```

   b. Generate wlfullclient.jar if it is not available in the MW_HOME/server/lib/ directory, and grant execute (755) permisssions to the file.
2. Enter the *`MW_HOME`* directory or Press [Enter] to accept the default.
3. Enter the *`OIM_ORACLE_HOME`* directory or Press [Enter] to accept the default.
4. Enter the hostname on which OIG is running :

   It is mandatory that OIG is running on the same host.
5. Enter the port where OIG server is running :

   The default port is 14000.
6. Enter the path of *`OIM_HOME`*.
7. Enter the OIG system administrator user name.
8. Enter the OIG system administrator password.

Steps to Map the Role and employeeType Attributes

If the bundle patch is applied after the OAM-OIG integration, then for the bug fix 31162758 to work, perform the following steps to map the `Role` attribute to the `employeeType` attribute:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab, and then click the **Applications** box to open the Applications page.
3. Search for **SSOTrusted-for-SSOTargetApp** and open it.
4. Click the **Schema** tab.
5. Map `Role` to `employeeType`.
6. Save the changes.

If the bundle patch is applied to OIG before the integration with OAM, then the manual mapping of the attributes are not required.

SSO Full User Reconciliation

For the bug fix 31605187 to work:

- If the bundle patch is applied after SSO integration, then the job parameter Incremental Recon Attribute value must be provided manually for the latest token value to get updated.
- If the bundle patch is applied before SSO integration, then manual steps are not required.

Major Enhancements in Bundle Patch 12.2.1.4.220413

The following are the major enhancements in Oracle Identity Governance 12.2.1.4.220413:

- Active Directory (AD) now supports adding groups as a member of other groups. For more information, see Predefined Scheduled Tasks.
- The new **MEMBERSHIP TYPE** column introduced in this patch appears at the end of the table for upgraded environment. To reposition the column, use the re-order column option.

Major Enhancements in Bundle Patch 12.2.1.4.211010

The following are the major enhancements in Oracle Identity Governance 12.2.1.4.211010:

- The Access Policy feature is enhanced to manage the evaluation of users in the **Disabled** status. See Evaluating Policies.
- The **Account Chooser** pop-up option is enhanced to display the **Account Type** along with the **Account Name** column while creating an Entitlement request. This helps users who access multiple accounts for the same application while requesting Entitlements.
- During certification to help reviewers for identifying the correct accounts, reviewers can use the Account Type option.
- The **Resource History** details of the Accounts section is enhanced to display the Entitlement Name and Request ID.
- **Manual Fulfillment** task, **Accounts** and **Entitlement** tabs under **User Access** UI are enhanced to display the Role Request ID.
- When users have entitlements provisioned outside of the Access Policies, a new option is provided which helps in keeping the account in the **Active** state. See Revoking or Disabling the Policy.
- The `updateRoleGrant` API of RoleManager is enhanced to start owner startDate and endDate attributes.

- The **Reconciliation Jobs** section of the Application Instance is enhanced with separate reconciliation jobs for defining and managing of the application instance during application on boarding. See Creating Application Instances.
- The Certification feature is enhanced to support mandatory certification comments on certify and non certify operations. The certification comments can also be mined from previous certifications and request justification. This helps the reviewer by providing better context about the access during certification. See About Pre-populate Certification Comments.

Major Enhancements in Bundle Patch 12.2.1.4.210708

The following are the major enhancements in Oracle Identity Governance 12.2.1.4.210708:

- To improve the reset password performance in Active Directory (AD) integration, a new system property is available which needs to be set to **True** and the certificate from the AD target needs to be imported. See the following topics:
  - Default System Properties in Oracle Identity Governance
  - Improving Reset Password Performance on AD Integration

Resolved Issues

The following section lists the issues resolved in Release 12.2.1.4.220703:

- Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220703
- Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220413
- Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220115
- Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.211010
- Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210708
- Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210428
- Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210112
- Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.201011
- 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 12.2.1.4.220703

Applying this bundle patch resolves the issues described in Table 1-2

Table 1-2 Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220703

BUG NUMBER	DESCRIPTION
31285681	THE ERROR POPUP "THE PASSWORD CHANGE OPERATION FAILED WHILE VALIDATING OLD PASS
32119840	CREATE USER WORKFLOW IS NOT TRIGGERED WHILE CREATING USER USING REST/SCIM API
32954733	DISCONNECTED ACCOUNT NOT PROVISIONED INTERMITTENTLY AFTER EVALUATE USER POL JOB
33216328	PUMA: IDA RULES VIOLATED COLUMN BLANKS OUT IN FIREFOX OR SAFARI BROWSERS
33247694	SCIM GROUPS/.SEARCH TOTALRESULTS IS FALSE
33445061	DUPLICATE ROLES APPEARING FOR SOME USERS IN USERS->ROLES
33451463	PUMA: EMPTY CUSTOM UDFS MARKED AS STRING "NULL" AFTER EXPORT/IMPORT
33461779	IAM-2050243 RAISED WHEN MODIFY USER ATTRIBUTE TRIGGERS ROLE/RULE EVALUATION
33504630	AFTER PATCH 29167604, CACHING OF USR_KEY FIXED IN 12.2.1.3, BUT NOT 12.2.1.4
33533162	OIM SERVER GOES TO WARNING STATE DUE TO HEAP SIZE GROWTH WHEN USER HAS MANY ADMIN ROLES
33539764	WHEN REQUEST IN INFORMATION REQUESTED STATE, REQUESTER CANNOT BE WITHDRAWN

Table 1-2 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220703

BUG NUMBER	DESCRIPTION
33541821	OIGOAMINTEGRATION.SH - ADDMISSINGOBJECTCLASSES DOES NOT ADD MISSING OBJECTCLASSES
33588973	A TIME LIMITATION OF MAXIMUM 6 MONTHS SHOULD BE ADDED ON THE PERIOD OF DELEGATIO
33656656	GROOVY TRANSFORMATION CAUSES TWO PROCESS TASKS TO BE RUN - 1ST BAD 2ND OK
33669502	OIM DISABLE REQUESTS SHOWING REQUEST COMPLETED, EVEN AFTER TASK FAILED
33790250	ROLE MEMBERSHIP END DATE ERROR MISLEADING
33889775	CANNOT RE-CREATE ROLE IN OIG 12C SSO ENVIRONMENT
33926014	MISSING FOREIGN KEY INDEXES AFTER UPGRADE TO OIM 12.2.1.4.X
33932731	CHANGEACCOUNTPASSWORD() API IS NOT WORKING WITH RACF TARGET WITH SPL CHARS PWD
33937973	OIG- ROLE CERTIFICATION ASSIGNMENT WITH PROXY SCENARIO
33945782	ENABLE USER REQUEST, ENABLES DELETED USER (DELETED TO ACTIVE)
33990557	ISSUE WITH 12C PROXY BASED FUNCTIONALITY
33997963	BULK LOAD UTILITY FAILS WITH "ORA-00907: MISSING RIGHT PARENTHESIS"

Note:

For more details, check Adding Missing ObjectClasses With OID for the workaround.

Table 1-2 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220703

BUG NUMBER	DESCRIPTION
33998355	DISC APP INSTANCE GOES TO PROVISIONED EVEN THOUGH NO LONGER IN AP
34028543	Fix for Bug 34028543
34030611	POLICY VIOLATION REMEDIATE OPTION IS GIVING ERROR "ENTITLEMENT KEY NULL NOT EXIST FOR USER KEY 11. COMMENTS : TESTING"
34035838	WHEN USERID REUSE CREATELDAPACCOUNTPOSTPROCESSHANDLER SEARCHKEYNOTUNIQUEEX ERROR
34049752	UI ROUNDS OFF THE CERTIFICATION CAMPAIGN TO 100 % COMPLETION WHEN IT IS AT 99.5%
34056111	FAILED TO RUN RETRY FAILED ORCHESTRATIONS SCHEDULED JOB
34089570	AFTER BUGFIX 34035838 THE SSOTARGET ACCOUNT IS LINKED VIA ORC_KEY TO OLD USER
34121706	SLOWNESS WHEN SELECTED ADMIN ROLE IN ORAGANIZATION MEMBERS PAGE
34130414	NO REQUESTID IS PRESENT IN CREATE USER RESPONSE OF CREATEUSER REST API
34150102	ORCLOAGINTEGRATIONADMIN ADMIN ROLE IS NOT SCOPED TO ANY ORG BY DEFAULT
34176248	CERT_TASK_ACTION.ACTION_DATE IS NULL ON CERTIFICATION RE-ASSIGNMENT
34181427	NPE IS THROWN DURING THE EBS RECON JOB RUN
34266397	ENTITLEMENT DELETED DOES NOT MOVE ENTRY FROM ENT_LIST TO ENT_LIST_HIST

Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220413

Applying this bundle patch resolves the issues described in Table 1-3

Table 1-3 Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220413

BUG NUMBER	DESCRIPTION
25109611	PASSWORD CHANGE REQUEST FOR XELSYSADM SHOULD BE SYNCED WITH CSF

Table 1-3 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220413

BUG NUMBER	DESCRIPTION
30546850	AOB: ERROR THROWN WHILE TRYING TO AUTO DISCOVER WHILE EDITING THE APPLICATION
30757118	DIAG: PATCH_OIM_WLS OVER-WRITES LOG FILE OF PREVIOUS BPS / ATTEMPTS
31005588	EVALUATE USER POLICIES JOB DELETES ENT_ASSIGN TABLE RECORDS AND RECREATES THEM ON USER EVALUATION
31159979	LOCK/UNLOCK USER THROWS JAVA.LANG.NULLPOINTEREXCEPTION: UICOMPONENT IS NULL
31873080	OIM DBUM USER DELETE RECON REVOKED TARGET ACCOUNT WITH EXPIRED & LOCKED STATUS
32539201	UPDATE ACTION SCRIPT DO NOT PASS THE REQUIRED ATTRIBUTES
32666165	ADMIN ROLE ACCESS POLICY VIEWER ALLOWS USER TO START CHANGING
32720089	AOB:TARGET ATTRIBUTE NAME VALUES GIVEN IN SCHEMA MAPPINGS ARE NOT GETTING SAVED
32986671	SELF-SERVICE CONSOLE CRASHES WITH "AN UNRESOLVABLE ERROR HAS OCCURRED. PLEASE CONTACT YOUR ADMINISTRATOR FOR MORE INFORMATION." WHEN TOGGLING THE "CHANGE PASSWORD SECTION"
33129060	ACCESS POLICY SHOULD NOT HONOR THE DELETED ENTITLEMENTS MAPPED TO IT FOR ROLE BASED PROVISIONING
33171832	PUMA: IDENTITY AUDIT VIOLATION COMPLETED BY AN ADMIN DOES NOT RESULT IN COMPLETION
33171971	PUMA: TARGET ACCOUNT IS EMPTY IN REMEDIATION APPROVAL TASKS
33275507	ACCOUNT END DATE CAN BE SET HIGHER THEN THE USER END DATE
33279653	ISSUE WITH THE CREATE USER APPROVAL WORKFLOW-DUPLICATE REQUEST
33284404	UPDATED TASKS ARE FAILING AFTER APPLYING IDM SBP
33351565	FLATFILE ENT RECON DISPLAY NAMES WITH SPECIAL CHARACTERS INCORRECTLY LOADED
33399996	OIM CLONE CONNECTOR SHOULD REPLACE ALL OCCURRENCES OF OLD NAME

Table 1-3 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220413

BUG NUMBER	DESCRIPTION
33400563	BENEFICIARYLOGINID AND REQUESTERLOGINID IS STILL NOT CONVERTED INTO POLISH LOCAL
33412499	ROLE SYNC MISSING WHEN LDAPSYNC IS REPLACED WITH CONNECTORS
33449308	NEED A SERVICE OR API THAT CAN VALIDATE ANSWER FOR USER/LOGIN QUESTIONS
33472511	UPG - XELSYSADM PASSWORD IN NOT IN SYNC WITH CSF KEYSTORE
33487303	ATPS: BULK LOAD UTILITY IS NOT WORKING WITH ATPS SETUP
33494174	VIEW ANALYTICS FOR ROLE CHANGES DOES NOT WORK IN POLISH LANGUAGE
33495897	RESOURCE HISTORY IS NOT DISPLAYED COMPLETELY AFTER PATCH 30119475
33505020	PUMA: UI REMOVING RULE BASED ROLE MEMBERSHIPS UPON INITIATION OF DELAY DELETION
33505355	POST OCT SPB "OBPASSWORDCHANGE" FLAG NOT GETTING RESET BUG 33393102 CONTINUES...
33536274	Fix for Bug 33536274
33537410	PUMA: MANAGER UNABLE TO VIEW COMPLETE/EXPIRED CERTS WHEN A PROXY IS ASSIGNED
33584027	USERS SHOWING UP TWICE IN LOG FILE IN PROXY RELATED ERROR MESSAGE
33586166	REQUEST.GETAPPROVALDATA() FAILS IN 12C, SAME CODE WORKS IN 11G
33587015	PATCH_OIM_WLS.SH SCRIPT HANG AFTER APPLIED THE IDM_SPB_12.2.1.4.211014
33625845	DISABLE/DELETE SCHEDULED JOB NOW REMOVES ROLES FROM DISABLED USERS IN 12C
33644344	RECONCILED ENTITLEMENTS SHOULD BE HANDLED VIA ACCESS POLICY USING APH
33652287	PUMA: EXPORT/IMPORT OF ACCESS POLICIES DOES NOT MIGRATE CHECK BOX VALUE
33652306	PUMA: SYSTEM PROPERTIES IMPORT FROM ONE ENV TO THE OTHER IS NOT WORKING
33653708	FORM IS CORRUPTING AFTER AOB TEMPLATE/SCHEMA CHANGES

Table 1-3 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220413

BUG NUMBER	DESCRIPTION
33655238	GETTING NO ENUM CONSTANT ERROR FOR ORGANIZATION TYPE AFTER APPLYING OIM BUNDLE PATCH 12.2.1.4.211010
33673956	APP INSTANCE CERTIFICATION PERFORMANCE ISSUE
33676752	ER 32288237 REPLACED SSO PASSWORD HANDLER AND INTRODUCED PROB WITH EXPIRY DATE
33684726	USR_PWD_CREATION_DATE NULL CREATING NEW USER W/O PASSWORD
33692276	USER DETAIL SHOWS EMPTY IN USER CERTIFICATION WHILE MODIFYING [ROWS DISPLAYED]
33694284	WRONG WORDING ON CONFIRMATION DIALOG WHEN CLAIMING OPEN CERTIFICATIONS
33697050	NEW PROVISIONING API TO RETURN THE LIST OF USERS PROVISIONED WITH SPECIFIED APP INSTANCE
33711997	AOB: AUTHORITATIVE APP ATTRIBUTE NAME VALUES GIVEN IN SCHEMA MAPPINGS ARE NOT GE
33735241	Fix for Bug 33735241
33738824	USERMANAGER.DELETE RETURNS USERMANAGERRESULT WITH NULL STATUS
33745642	RECON DATA PURGE IS COMPLETED WITH ERROR(S) ORA-06502 AT OIM_SP_RECON_ARCHPURGE
33768054	CHILD FORM IS CORRUPTING AFTER AOB TEMPLATE/SCHEMA CHANGES
33780050	INDIRECT ROLES NOT POPULATED IN OIMASSERTIONLOGINMODULE AND OIMAUTHLOGINMODULE
33791086	ROLE NOT ADDED TO TABLE PENDING_ROLE_GRANTS WHEN END DATE SET BY APPROVER
33793732	BROKEN HYPERLINK IN TRACK REQUESTS PAGE : FIREFOX
33796313	ORG SEARCH ERROR WHEN THERE IS A LARGE AMOUNT OF ORGS
33862402	NO OPTION TO SELECT THE DISPLAY NAME OF THE ROLE UNDER MANAGE --> USERS -->ROLES
33909965	REGRESSION OF BUG 33279653

Table 1-3 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220413

BUG NUMBER	DESCRIPTION
33934140	NOSUCHMETHODERROR ACCOUNTHANDLERUTIL.CREATEUSER IN SEEDOIMDATAINTARGETLDAPIMPL
33946147	OIG-CONFIG-UTILITY.SH IS NOT RUNNING IN APRIL BP, IT IS THROWING ERRORS WHILE RUNNING THE UTILITY
33946292	CLASSPATH.SH IN APRIL BP IS STILL REFERING THE OLD JAR REFERENCES
33989996	INTEROP: WHEN WE SET PASSWORD EXPIRY DATE TO BLANK AND TRY TO RESET THE PASSWORD IT IS STILL NOT WORKING IN PS4 + APRIL BP (33929963)
34011734	BENEFICIARYLOGINID AND REQUESTERLOGINID IS STILL NOT CONVERTED INTO POLISH LOCAL
34035584	DESIGN CONSOLE FORMS NOT OPENING IN LATEST BP
34062173	IN WINDOWS, DESIGN CONSOLE ADAPTER FACTORY FORM IS NOT OPENING IN LATEST BP, IN LOGS IT IS THROWING ERROR '.NOCLASSDEFFOUNDERROR

Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220115

Applying this bundle patch resolves the issues described in Table 1-4

Table 1-4 Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220115

Bug	Bug Abstract
30200580	DIAG: ORACLE.IAM.APPLICATION.IMPL ERROR CONSUMES STACK ON TRANSFORMATION
31155251	REQUESTS GETS FAILED IN IDENTITY MANAGER
31895248	REGRESSION BUG 29750388 : SEARCH IN "REQUEST FOR OTHERS" IS NOT WORKING
32331154	NON REQUESTABLE ROLES DOESN'T APPEAR IN THE USER CERTIFICATION
32390472	OIG PRE-UPGRADE REPORTS INCORRECTLY IDENTIFIES 19C DB AS UNSUPPORTED VERSION FOR OIM 11GR2PS3 WHILE UPGRADING TO 12C

Table 1-4 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220115

Bug	Bug Abstract
32492120	PROVISIONING TASKS - OPEN TASKS - EDIT FORM RENDERS DATES INCORRECTLY USING 2 DIGIT YY
32540331	SEARCH BUTTON NOT EASILY VISIBLE IN THE SYSADMIN LOOKUP UI
32760053	OIM DN GENERATION LOGIC FAILS TO GENERATE DN USING ESCAPE CHARS
33060231	BULK REVOKE ENTITLEMENTS REQUEST SHOWS JBO ERRORS, INCORRECT ACCOUNTS
33066536	OIM TRUSTERD DELETE RECON UNEXPECTED TO DELETE OIM USERS
33086686	EXTEND FIX OF BUG 31038511 TO ALL TYPE OF CERITIFICATIONS - SEE EH 27284033
33113521	PROXY USER WRONG MESSAGE
33171625	CHALLENGE QUESTIONS GIVES ERROR WHEN USER DEFINED IS SELECETD IN PASSWORD POLICY
33190066	12.2.1.4.0 OIM: ATPSCERT: ATP S: RCU PRE-REQ FAIL FOR OIM SCHEMA WITH ATP S DB
33246155	PUMA: PREVENTATIVE SCAN NOT WORKING WHEN A ROLE IS ALREADY REQUESTED
33319198	DELETED USER ACCOUNT CLEAN UP JOB DOESN'T WORK IF DUPLICATE ACCOUNTS EXISTS
33350167	ANYTIME A WORKFLOW IS ACCESSED IN THE OIG UI WE GET SERIALIZABLE ERRORS
33379590	CLASSCASTEXCEPTION: INTEGER TO STRING WITH INTEGER UDF WITH IN MEMBERSHIP RULE
33404573	12.2.1.4.0 OIM:FMWATPS ATPSCERT HOT: Pop-ups seen in RCU log-Error creating PL/SQL Object's: OIM_SP_MANAGEENTITLEMENT,OIU_UPDATE
33407956	Fix for Bug 33407956
33417218	OIG 12CPS4 OCT BP , ROLLBACK REAPPLY IS CHANGING THE STATUS OF CERTIFICATION TO STALE
33419121	MODIFY ADF CACHE SIZE CONFIGURATION FOR TABS

Table 1-4 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.220115

Bug	Bug Abstract
33428494	UPDATES TO USER (USR) NOT PROPAGATED TO ACCOUNTS IN 'PROVISIONING' STATUS
33440181	JOB DELETED USER ACCOUNT CLEAN UP JOB FAILS IF ANY UD TABLE CONTAINES ONLY PK AND FK COLUMNS
33449049	USER CREATION FAILS IN OIM AD SETUP WITH PATCH 33429084
33452123	USER ROLE GOT REVOKED, FOR A VALID 'USER MEMBERSHIP RULE'
33462000	JPS-CONFIG.XML CONTAINS LEFT OVER OAM 11G INFO CAUSING ISSUES WITH 12C
33465669	NPE ERROR WHILE STARTING OIM AFTER UA IF ORACLE_HOME IS INVALID
33471784	BOOTSTRAP PROCESS FAILS DURING DEPLOYSOACOMPOSITES DUE TO CONNECTION NOT AVAILABLE
33474286	VALIDATION OF OPSS VERSION NEEDED IN PRE-UPGRADE REPORT
33629042	USER CERTIFICATION CREATION WITH OPTION "RETAIN EXPIRY DATE" GIVES NULLPOINTEREXCEPTION IN SCHEDULED JOB

Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.211010

Applying this bundle patch resolves the issues described in Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.211010

Table 1-5 Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.211010

Bug Number	Description
22780597	UPDATEROLEGRANT DOES NOT HANDLE THE STARTDATE / ENDDATE ATTRIBUTES
27432438	ALL THE FIELD LENGTHS IN THE USR TABLE SHOULD MATCH WITH THE CERT_USER TABLE
28078904	PREVENT APPLICATION INSTANCES REVOKE WHEN ENTITLEMENTS OUTSIDE ROLE EXIST
28545612	ENT_ASSIGN_HIST DOESN'T SAY HOW THE USER ACCESS IS PROVISIONED
28882181	ARM_AUD TABLE NOT UPDATED DURING ADMIN ROLE ASSIGNMENT

Table 1-5 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.211010

Bug Number	Description
29167604	SERVER CACHING AUTH BETWEEN SELFREGISTRATION AND CREATE USERS REST CALLS
29950705	ALL ACCESS POLICY ENTITLEMENT REQUEST SHOULD HAVE REQUESTER DETAILS SIMILAR TO OTHER REQUESTS
30043034	OIM USER FORM DATE UDF ATTRIBUTE NOT FUNCTIONING PROPERLY IN SSO ENV
31038511	CERTIFICATION REASSIGNED OR DELEGATED RESETS TIME SEE EH 27284033
31140352	ADD FEATURE FOR ARCHIVING AND PARTITIONING ENT_ASSIGN_HIST TABLE
31464255	SOD VALIDATION AGAINST ENTITLEMENTS WHICH ARE REQUESTED
31771784	IDENTITY AUDIT RULE DESCRIPTION IS LIMITED TO 256 CHARS
31784882	CUSTOM TASKFLOW MESSAGE OVERWRITTEN BY DEFAULT MESSAGE
31786287	BULK OPS IS MASKING PASSWORD CHANGE SEE BUG 31687980)
31934316	MANDATORY CERTIFICATION COMMENTS FOR ALL CERT LINE ITEMS
31940390	PUMA: ENTS ASSIGNED OUTSIDE OF ACCESS POL ARE LEFT STRANDED AFTER ROLE REMOVAL
31995394	OIM 12C PS3 EXPORT/IMPORT TOOL NOT WORKING PROPERLY
32258285	PROVISIONING OPEN TASKS SEARCH DOES NOT GET THE TASK STATUS TRANSLATED TO POLISH
32305321	CLARIFICATIONS ON USAGE OF THE LOCAL TEMPLATE ADD ATTACHMENT API.
32324514	INTERFACE PROVISIONINGSERVICE.GETACCOUNTSPROVISIONEDTOUSER THROWS NPE
32379310	CERT EVENT LISTENER TRIGGERED FOR CERTIFIED USERS EVEN WHEN NO CHANGES ARE MADE WHEN CERT OPTION PREVENT SELF CERTIFICATION ENABLED
32416424	PUMA: DISPLAY ACCOUNT TYPE IN OIM ACCOUNT CHOOSER POPUP
32488483	SERVICE ACCOUNT CHECKBOX IS NOT CHECKED WHEN REQUEST MADE VIA REST API

Table 1-5 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.211010

Bug Number	Description
32523570	ACTION COMMENTS DUPLICATED FOR REJECT,ESCALATE OPERATIONS DURING APPROVALS THROUGH REST API
32542298	SSOTRUSTED-FOR-SSOTARGET ORGANIZATION NAME RECON FIELD SCHEMA PROPERTY ENABLE / DISABLE NOT HONORED
32545659	BUG 30516224 CONTINUED -- NEED SUPPORT FOR PERIOD CHARACTER
32567175	REVIEWER "SEARCH FOR A ROLE" NOT WORK
32586438	PROCESS TRIGGER NOT FIRING FOR END DATE
32619046	AOB DBAT CONNECTOR LOCKING THE TARGET SYSTEM USER ACCOUNT
32644878	HOW TO CONFIGURE OHS FOR CERTAIN LOCATIONS NOT DOCUMENTED IN THE HA GUIDE?
32670128	ADDING ADDITIONAL ENTITLEMENTS TO AP DOESN'T RE-EVALUATE AND ADD TO USER
32682939	PUMA: MANAGER WITH ACTIVE PROXY DOES NOT GET ACTIONABLE EMAIL ABOUT APPROVAL ASSIGNMENT
32683903	DIAGNOSIBILITY : NOT ABLE TO EDIT IT RESOURCE
32710101	ISSUE AUDIT MESSAGE TASK DOES NOT PROCESS AUDIT DATA FOR FEW USERS
32710741	SSOTRUSTEDFORSSOTARGET RECON EVENT FAILS WITH INVALID MANAGERLOGIN ERROR
32716632	UNABLE TO CHANGE THE LOOKUP NAME FOR A CLONED CONNECTOR
32717850	DISABLED USERS SHOULD NOT BE EVALUATED BY ACCESS POLICY
32726134	DIAG:CERTIFICATIONCOMPLETIONUPDATE RUNNABLE.RUN PRINTS "NULL" INSTEAD OF ERROR
32739740	CANNOT SORT OPERATIONS IN WORKFLOW AFTER APPLYING PATCH 31797847
32747711	OAM / OIM AD MODIFIED USER IS RECONCILED LIKE {BASE=DISPLAYNAME}
32764420	NEED WORKING EXAMPLE OF SCHEDULERSERVICE.CREATESCHEDULE DTASK(ST)

Table 1-5 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.211010

Bug Number	Description
32769357	POST PROCESS CODE IS NOT GETTING INVOKED WHEN USER UNLOCK IS DONE ON UI.
32827236	SCREEN PACKAGE THAT IS REQUIRED FOR OIM-OAM INTEGRATION IS DEPRECATED IN RHEL8
32830574	SCRIPT UPDATE_OIM_AUTHENTICATE_PROVIDER FAILS IF THE DOMAINS FOLDER NOT PRESENT
32843595	ORGANIZATION TYPE/STATUS IN MANAGE - APPLICATION AREA PAGES NOT TRANSLATED TO BROWSER LOCAL
32880383	SUNSET JOB UNABLE TO REMOVE ACCESS IF THE ENTITLEMENT REQUEST IS APPROVED AFTER
32902773	IAM-2050243 FAILED WHILE DISABLING USER WHEN WORKFLOWS ENABLED IS FALSE AFTER BP
32903652	UNINSTALLCONNECTOR DELETE ONE RESOURCEOBJECT RESULT IN ALL ITRESOURCE OF SAME CONNECTOR TYPE REMOVED
32939218	NULL DATES ARE STORED AS 01-JAN-1970 (JAVA EPOCH) IN AUDIT TABLES
32977106	PASSWORD VALIDATION FAILS IF IT HAS LEADING/TRAILING SPACES UNDER MY INFO PAGE
32998646	USERMANAGER.DELETE(USER_LOGIN,TRUE) FAILS WITH INVALID NUMBER ERROR
33000675	DIAG: NEED DIAGNOSTIC PATCH IN ACCESSPOLICYSERVICEIMPL.UPDATEACCESSPOLICY/PROCESSWITHOUTRESULT
33005552	NPE IN DELAYED DELETE USER WITH JOB HISTORY JOB USERAUDITHANDLER
33018171	ISSUE WITH ORGANIZATION BULK LOAD WHEN SPECIAL CHARACTER / ARE PRESENT
33066442	DELEGATED CERTIFICATIONS NOT FILLING IN CERT_TASK_ACTION.ACTION_DATE
33069593	FORGOT PASSWORD RESET FAILS WITH VAGUE GUI ERROR MESSAGES
33069995	"COMMON NAME" NOT POPULATED DURING NON-SSO TRUSTED RECON IN 12CPS4 SSO ENV
33088894	REQUEST JUSTIFICATION FIELD NEEDS TO BE IN LOCAL LANGUAGE

Table 1-5 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.211010

Bug Number	Description
33091106	ERROR ON "OFFLINE DATA PURGE FRAMEWORK" UTILITY IN OIG 12CPS4
33097801	REST API FAILS TO COMPLETE CERTIFICATION WITHOUT PASSWORD IN PS4
33102762	AOB: FLAT FILE TARGET RECON JOB NOT WORKING CORRECTLY WITH INSTANCE APP
33103959	DUPLICATE TASK DEFINITION IN TASK.XML AFTER UPGRADE FROM 12.2.1.3 TO 12.2.1.4
33112078	EMAIL NOTIFICATION ATTACHED TO ASSIGNMENT TAB OF PROCESS TASK IS NOT TRIGGERING
33119876	NEED TO SHOW APPLICATION INSTANCE DISPLAY NAME IN THE ERROR MESSAGE SHOWN IN UI (AS PER BUG 30952309)
33120542	PREUPGRADEUTILITY IS FAILING WITH COMPATABLE_PARAMETER_CHECK ERROR
33129135	PROMPTING FOR PASSWORD UPDATE WHILE UPDATING THE BASIC INFO IN MY INFO TAB
33137945	TESTCASE FAILURES IN ACCESS POLICY MODULE AFTER THE FIX 31995394
33150481	IN AN SSO INTEG OIM-OAM ENV, UPDATING THE USR_COMMON_NAME NULLS USR_LDAP_GUID
33160341	DOES NOT BEGIN WITH OPERATOR IN AUDIT RULE DOES NOT WORK FOR BLANK VALUES
33165095	ORGANIZATION SEARCH ERROR IN OIM 12.2.1.4.210428
33165837	SUBMIT REQUESTS REST API IS ALWAYS SUBMITTING THE REQUEST FOR ASSIGN ROLE ONLY
33174111	UNABLE TO CLOSE RECON EVENTS AFTER RUNNING OFFLINE DATA PURGE JOB USING API
33182890	ORCHESTRATION OFFLINE PURGE FOR RETENTION PERIOD 365 DAYS IS NOT WORKING
33214891	USER CREATION FAILS IN OIM 12C WHEN REQUESTENTITY API IS USED
33225499	DISABLED USERS WITH PAST END DATE NOT GETTING USR_AUTOMATICALLY_DELETE_ON SET

Table 1-5 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.211010

Bug Number	Description
33243897	AOB: SETTINGS TAB NOT DISPLAYING RECON JOBS WHILE CREATING INSTANCE APPLICATION OF AUTH APP OR EDITING AUTH APP OR ITS INSTANCE APP
33255209	SOA WORKFLOW IS ACCESSED WHEN WORKFLOWS ENABLED IS FALSE UNDER PATCH 32902773
33275455	OIM DELETE USER OPTION IS FAILING AFTER BP 210708 WITH WORKFLOW ENABLE = FALSE
33276969	POST UPGRADE 12CPS4 OIM SERVERS GOING TO WARNING STATE AND AUTO-HEALED
33279285	THE OIG.BENEFICIARYMANAGERAPPROVALWORKFLOWS SYSTEM PROPERTY IS MISSING IN LATEST SHIPHOME
33292833	REST: THE OPERATION PARAMTER MUST BE OPTIONAL IN THE ROLE REQUEST
33305314	CUSTOM EMAIL NOTIFICATIONS GET NO PARAMETER WHEN TEMPLATE TYPE SET TO TEXT/PLAIN
33321617	UNABLE TO CREATE ROLE WHEN ENFORCESINGLEACCOUNTPERAPPLICATIONREQUEST IS SET TO TRUE
33404123	SYSTEM PROPERTY WORKFLOW ENABLE = FALSE IS PARTIALLY CASE SENSITIVE

Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210708

Applying this bundle patch resolves the issues described in Table 1-6.

Table 1-6 Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210708

Bug Number	Description
28433832	PROCESS TASKS ARE NOT TRIGGERED WHEN THERE ARE DUPLICATE ENTRIES IN LOOKUP
30516224	IDENTITY AUDIT RULES CONTAINING SPECIAL CHARS DO NOT RAISE POL. VIOLATION
30641393	REST USER SEARCH ON DATE ATTRIBUTE DOES NOT FILTER ON TIMEZONE

Table 1-6 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210708

Bug Number	Description
30952309	ENTITLEMENT REQUEST STUCK IN REQUEST AWAITING DEPENDENT REQUEST COMPLETION
31724255	Fix for Bug 31724255
31781952	OIM_SP_CERT_ARCHPURGE STORED PROCEDURE INCORRECTLY ARCHIVING CERTS_USER ROW
32043090	CATALOG REQUEST PROFILES NOT DISPLAYING VALUES DURING CATALOG REQUEST
32288237	PERFORMANCE ISSUE WITH PASSWORD RESET IN SSO ENVIRONMENT (12C) **Note:** For details, see Improving Reset Password Performance on AD Integration.
32306365	PUMA: ROLES ARE REMOVED WHEN USERS ARE SOFT DELETED USING DELAY DELETE
32408854	PUMA: TEST CONNECTION FAILS FOR DBUM INSTANCE
32461462	OIM API NOT EXPOSING METHOD TO DECRYPT ENCRYPTED UDF
32635254	OIM CN GENERATION LOGIC FAILS TO GENERATE UNIQUE CN USING SPECIAL CHARS
32680717	PUMA: LDAP USER SEARCH DELETE RECON BEHAVE DIFFERENTLY THAN USER
32704620	REVOKING ROLE VIA CERTIFICATION PROCESS IS NOT GENERATING REQUEST TO REMOVE ROLE
32705847	ATTRIBUTE VALUES IS NOT VISIBLE IN PENDING VIOLATION TASK VIEW

Table 1-6 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210708

Bug Number	Description
32739454	PRE-UPGRADE REPORTS CONTAINS UNWANTED OIM12CPS3 BP02 INFORMATION
32742292	ONEHOP IS THROWING NPE WHILE UPGRADING ORACLE IDENTITY MANAGER SCHEMAS USING THE UPGRADE ASSISTANT STEP
32763040	OUTOFMEMORY EXCEPTION WHILE ADDING MEMBERS TO ADMIN ROLE
32806846	MULTIPLE MANUAL REVOKE ENTITLEMENT TASKS GENERATED FOR ACCESS POLICY DISABLE
32881765	RESOURCE HISTORY NOT LOADING WITH LOAD BALANCER URL IN OIG 12CPS4 CLUSTER ENV
32984575	UNABLE TO CREATE THE APPLICATION INSTANCE FOR DBUM CONNECTOR

Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210428

Applying this bundle patch resolves the issues described in Table 1-7.

Table 1-7 Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210428

Bug Number	Description
16755363	IDMUPG:PS5-PS6:OIM UPGRADE SCRIPT THROWS NPE AFTER APPLYING PATCH 16609934
25386874	ER: NEED CONSISTENCY IN INTEGRATED OIM AND OAM FOR LANGUAGE PREFERENCE
28819255	CREATION OF THOUSANDS OF UNEXPLAINED UPDATE TASKS
29973037	OIM 11.1.2.3.X AUDIT - UPA TABLE IS NOT RECORDING DELTA INFORMATION PROPERLY
30013863	CAN'T CHANGE/UPDATE ATTRIBUTES ON AOB SCHEMA
30054791	ADMIN ROLE ACCESS POLICY VIEWER ALLOWS USER TO START CHANGING
30107277	CONNECTOR UNINSTALLATION FROM AOB DELETES ADAPTERS AS WELL.
30110645	AOB: REMOVAL OF A CHILD FORM REMOVES TASKS FROM OTHER APPLICATIONS

Table 1-7 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210428

Bug Number	Description
30141533	CREATE ADMIN ROLE ERROR
30155470	OIG 12.2.1.3.190624 REST API REQUESTS RETURNING ERROR WITH CUSTOM COMPOSITE
30201821	[ROLECERT]: PROXY USER SHOULD BE CERTIFIED BY THE CERTIFIER'S MANAGER
30265046	OIG SUBMIT BUTTON OF IDENTITY FIRST LOGIN PAGE SHOULD BE THE LAST READING ORDER
30272992	FEW REQUESTS MOVED TO FAILED STATUS WITH AUTO APPROVAL WORKFLOW
30465556	CERTIFICATION FAILS IF CATEGORY_COUNT_OPTION IS TO 1 OR 0
30581388	ADVANCED SEARCH WITH CHECKBOXES LEADS TO ERROR: JAVA.LANG.BOOLEAN CANNOT BE CAST
30586440	NPE ERRORS WHILE CREATE ADMIN ROLE ERROR
30628628	PROCESS PENDING ROLE GRANTS WHEN ROLE IS DELETED
30674852	ROLE CERTIFICATION FAILS USING ACCESS POLICY WITH MULTIPLE APPLICATION INSTANCES WITH THE SAME ENDPOINT
30719311	PASSWORD POLICY RULE "MINIMUM PASSWORD AGE (DAYS)" IS NOT HIGHLIGHTED
30773475	OIM ORGANIZATION GETTING DISABLED INTERMITTENTLY IN PRODUCTION .
30844901	PRE-POPULATING ATTRIBUTES NOT WORKING FOR USERS IMPORTED VIA BULK LOAD UTILITY
30901352	SCIM DOES NOT RETURN CORRECT USERS WHEN USING ENDPOINT /IAM/ GOVERNANCE/SCIM/V1/U
30908422	ROLE CATEGORY CONSIDERED DUPLICATE IN UI
31060268	OIG12C: ALLOWS YOU TO UPDATE AN EXISTING AP AND ADD 2ND APP FOR SAME RO
31342188	USER IS NOT CREATING IN LDAP POST SOA APPROVAL
31353225	FILTER IN SSO FULL AND INCREMENTAL RECON JOB DOES NOT WORK.

Table 1-7 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210428

Bug Number	Description
31397729	DIAG:QUARTZTRIGGERLISTENER.TRIGGERMISFIRED DOES NOT DISPLAY TRIGGER NAME
31467891	ACCESS POLICY EVALUATION INITIATES PROCESS TASKS FOR NULL CHECKBOX VALUES
31525878	OIM 12C SSO USER TARGET RECON OVERWRITING "ORGANIZATION NAME" VALUE WITH "XELLERATE USERS" DEFAULT VALUE
31576436	EVENTFAILEDEXCEPTION AND REQUESTSERVICEEXCEPTION IS SEEN IN THE LOG AFTER THE REQUEST STATUS TASK IS EXPIRED
31592160	TRACK: OIM DATA PURGE JOB FAILS WHILE PURGING THE RECON DATA FROM RA TABLES
31626677	OIMDBPLUGIN NOT INTERPRETING ESCAPED PARENTHESIS IN GROUP NAMES IN LDAP QUERY CORRECTLY
31634715	OIM 12.2.1.4.0:OIG RCU SQL MODIFICATIONS REQUIRED TO SUPPORT OIG DB ON ATP-D AND ATP-S
31656655	MISSING REQESTER ID LEADS TO REQUEST FAIL
31637673	VIEW FORM OR EDIT FORM IS BLANK FROM OPEN TASKS PAGE
31683884	"FOR REPORTEES" OPTION IS NOT TRANSALATED TO BROSWER LANAGUGE
31732078	IAM-3054101 : THE LOGGED-IN USER DOES NOT HAVE VIEWSEARCHENTITY PERMISSION
31748217	ADF: ACCESS POLICY APPLICATION FORM FORCING TO ENTER AS FIRST VALUE THE FIELD MARKED AS ACCOUNT DISCRIMINATOR BEFORE ANY LOOKUP
31765258	UPDATING CERTIFICATION LINE ITEM USING REST RETURN HTTP ERROR 500 "GETSINGLERESULT() DID NOT RETRIEVE ANY ENTITIES."
31786528	POST PROCESS ENVENT HANDLER NOT TRIGGERING ADD ROLE TO USER TASK ON SSO TARGET
31821244	ADDING ENTITLEMENT TO ACCESS POLICY AND EVALUATING TRIGGERS UPDATE TO PROC FORM.

Table 1-7 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210428

Bug Number	Description
31828240	PASSWORD CHANGED ON AD IS NOT PROPOGATING TO OTHER TARGET USING AD PWD SYNC
31838518	AUTOMATICALLY UNLOCK USER SCHEDULE JOB RESETS OBLOGINTRYCOUNT BUT NOT OBLOCKEDON
31883989	ADD SUPPORT FOR ONE-HOP UPGRADE FROM 11GR2PS3 TO 12CPS4
31903352	OIM HANDLING OF DISABLED USERS IN WORKFLOWS
31916340	LDAPCONTAINERRULES.XML NOT HONORING CREATE AND MODIFY OPERATIONS MOVING USER BACK TO DEFAULT OU
31922997	PUMA:UNABLE TO PROVISION/REVOKE ENTITLEMENT FROM FLAT FILE DISCONNECTED APP
31928115	SSO INCREMENTAL RECON CAUSES OBPASSWORDEXPIRYDATE TO DECREASE BY ONE DAY
31936434	HTTP 403 WHEN EDITING AN IT RESOURCE OR INSTALL A CONNECTOR
31941035	EXCEPTIONS ARE LOGGED DURING EXECUTION OF SCRIPT OIMBULKLOAD FOR AOB
31944823	CREATE INSTANCE FROM ACTION MENU FOR FLAT FILLE CONNECTOR CREATES APP WITH APP_INSTANCE_IS_SOFT_DELETE SET TO 1
31984036	CANNOT DISABLE OBJECT INSTANCE AS IT IS ALREADY DISABLED
31988157	REJECTED TASK ASSIGNED DATE CHANGES IF TASK IS ASSIGNED TO USER OR GROUP
31988511	REQUEST ID AFTER BEING APPROVED IS CREATED AGAIN UNDER PENDING APPROVAL
32012695	12C ACCOUNTS BULK LOAD FROM DB TO AOB APPINST FAILS WITH: JAVA.LANG.REFLECT.INVOCATIONTARGET EXCEPTION
32016431	UNABLE TO CHANGE FLAT FILE DURING FLAT FILE APPLICATION INSTANCE CREATION

Table 1-7 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210428

Bug Number	Description
32018230	DISAPPEARING REPORTS IN BI PUBLISHER - ONLY IDENTITY AUDIT REPORTS SHOW WHEN UI
32065363	PREVENT SELF CERTIFICATION IS NOT WORKING ON REASSIGNMENT OF ENT TYPE CERT
32086855	CERTIFICATION ROLE POLICY TAB ENTITLEMENT URL SHOW NO ENTITLEMENT DETAILS
32119749	BPEL TASK MAPPING GET ERASED WHEN THE COMPOSITE IS INVOKED
32178264	"BULK LOAD POST PROCESS" JOB SETTING DIFFERENT PWDS FOR OIM USER -VS- SSOTARGET
32180926	SOD CHECK NOT REQUIRED FOR OIM ROLES
32285418	TRACK REQUEST FOR REPORTEES NOT TRANSLATED TO POLISH
32307183	12C PS4 UPG DOESN'T UPDATE OIM-CONFIG.XML OR WORKFLOWS WITH VERSION6 DEFAULT COMPOSITES
32322591	AUTO-LOGIN FUNCTIONALITY NOT WORKING FOR OIM OAM INTEGRATED ENVIRONMENT
32364874	"TEST CONNECTION" FAILS WHEN OIM UI IS LAUNCHED WITH NON .COM OR .EDU URL
32386512	PRE-UPGRADE REPORT SHOWS "OBSELETE" REPORTS NO LONGER REQUIRED.
32393962	SSOTARGET PROVISIONING TRANSFORMATION SCRIPT TRUNCATING DATE CAUSING INCONSISTENCY BETWEEN USR_PWD_EXPIRE_DATE AND OBPASSWORDEXPIRYDATE
32400979	CERTIFYING ACCESS POLICY ATTACHED TO ROLE VIA REST THROWS JAVA.LANG.NULLPOINTEREXCEPTION HTTP ERROR CODE 500
32429894	PROB IN SAVING "ORGANIZATION NAME" AS RECONCILIATION RULE UNDER AD GROUP IN DC
32485920	CERTIFICATION TASK ASSIGNED ONLY TO PROXY OF MANAGER OF MANAGER DISABLED BUT NOT TO MANAGER OF MANAGER DISABLED
32497804	RESOURCE HISTORY - DATE ASSIGNED FIELD SHOWS IN GMT TIMEZONE

Table 1-7 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210428

Bug Number	Description
32513700	INCONSISTENCY DATE FORMAT BETWEEN TRACK REQUESTS AND REQUEST DETAILS FOR REQUESTED DATE FIELD
32527571	WRONG KEY WHEN FETCH THE ERROR MESSAGE TRIGGERS MISSINGRESOURCEEXCEPTION
32534109	CAN'T CHANGE/UPDATE ATTRIBUTES ON AOB SCHEMA
32535086	ORGANIZATION SEARCH IS NOT WORKING FOR END USER OTHER THAN XELSYSADM
32549885	BUG IN ACCESSPOLICYSERVICE API, FUNCTION GETACCESSPOLICY LIMIT TO 1024
32582603	ROLE CERTIFICATION COMPLETION THROWS EXCEPTION WHEN USING ACCESS POLICY WITH MULTIPLE APP INSTANCES WITH THE SAME ENDPOINT
32631765	DATE ASSIGNED COLUMN ONLY THE DATE IS DISPLAYED, TIMESTAMP MISSING

Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210112

Applying the bundle patch resolves the issues described in Table 1-8.

Table 1-8 Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210112

Bug Number	Description
25790911	JAVA SCHEDULERSERVICE:GETLASTHISTORYOFJOB API CAUSING OUT OF SEQUENCE ISSUES WITH RAC DB
27511207	ACCOUNT END-DATE IS NOT CLEARED POST ENABLING THE ACCOUNT
28025965	LIBRARIES (.JAR)FOR MANAGED BEANS AND TASK FLOWS ARE MISSING IN 12C
28361656	EMPEMPLOYMENT.STARTDATE INVALIDDATAFORMATEXCEPTION
28374155	12C SCIM API RETURNS ITEMSPERPAGE INSTEAD OF TOTALRESULTS
30446841	IDENTITY AUDIT RULES CONTAINING SPECIAL CHARACTERS DO NOT RAISE POLICY VIOLATION
30484714	REFRESHROW ISSUE WITH OJDBC8
30587375	DEADLOCK CAUSING STUCK THREADS
30517242	OIMADMINPASSWD_WLS.SH FAILS ON IBM AIX WITH IBM JAVA JRE

Table 1-8 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.210112

Bug Number	Description
30808736	RECONCILIATION OF A USER STATUS FROM ACTIVE DIRECTORY DOES NOT SET OBUSERACCOUNTCONTROL IN LDAP
30835811	APPROVAL CHILD TASKS STATUS DOES NOT SHOW WITH BROWSER IN ITALIAN LANGUAGE
30883086	UNSUPPORTEDOPERATIONEXCEPTION ON MODIFYING USER WHEN USING UDF NUMBER IN ROLE MEMBERSHIP RULE
30932205	OIM REQUEST FAILED WITH MESSAGE IAM-2050126 : INVALID OUTCOME COM.ORACLE.BPEL.CLIENT.BPELFAULT
30992823	Fix for Bug 30992823
31161987	PASSWORD RESET IN MYINFORMATION SUBMIT BUTTON
31373822	NEED SPECIAL HANDLING OF INT ON FORM WHEN NO VALUE PASSED
31420786	ACCESS POLICY DOES NOT REMOVE ENTITLEMENT WHEN 2 CHILDFORMS ARE UPDATED TOGETHER
31530459	IPV6: PURGECACHE UTILITY IS NOT WORKING WITH IPV6 ENABLED SETUP
31645106	HARVESTED ENTS INCLUDED WHEN ENTITLEMENTS PROVISIONED BY AP UNCHECKED
31622015	WRONG NUMBER OF ROWS DISPLAYED ON THE CERTIFICATION TABLE
31641120	CONFIG UPGRADE FAILING IF SCHEMA SUFFIX OTHER THAN _OIM USED
31668539	EVALUATE USER ACCESS POLICY JOB STUCK AND CAUSING OIM SERVER TO GO INTO WARNING
31678727	OAM OIM 12CPS3 USER IS SHOWING STATUS AS UNLOCKED IN OIM CONSOLE EVEN IT IS LOCKED
31723765	DISABLEPOWEREDBYHEADER, SOAPRESTART BOOTSTARP FAILED WITH LOCALSVCTBLDATASOURCE DS ERROR
31956134	ATTEMPT TO PACK THE DOMAIN AFTER 12.2.1.3 UPGRADE FAILS DUE TO COMPONENT VERSION MISMATCHES
31969309	FIX FAIL BUG 31180365 ON 12CPS4 BP
31979466	PUMA: ACCOUNT CHOOSER POPUP DURING CHECKOUT KEEPS EXPANDING TILL REACH THE WINDOW LENGTH
32085862	FAILED TO REGISTER LIBRARY EXTENSION-NAME: ORACLE.IDM.IDS.CONFIG.UI: MUST PROVIDE SPECIFICATION-VERSION FOR LIBRARY
32254565	WHEN USER HAS NO ACCOUNT, CALL MADE TO INVOKE TRIGGERPOSTPROCESSHANDLER FAILS
32102761	PRE UPGARDE REPORT FAILS IF STAGING-MODE IS EMPTY
32103803	UPGRADE WITH REMOVED ITR PASSWORDS LEAD TO POST CREATE EVENT HANDLER KEEPS TRIGGERING

Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.201011

Applying this bundle patch resolves the issues described in Table 1-9.

Table 1-9 Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.201011

Bug Number	Description
26308544	DELETED ENTITLEMENTS IN ACCESS POLICY ARE NOT REMOVED IN TARGET APPLICATION
29404814	CERTIFYING 20K USERS WITH 20K ACCOUNTS AND 100K ENTITLEMENTS FAILS IN SELF-SERVICE
29603087	SELF REGISTRATION DOES NOT TRIGGER ROLE MEMEBERSHIP
30062969	TRUSTED RECON OF MANAGER DOES NOT PROPAGATE TO SSOTARGET
30145982	12C ACCOUNTS BULK LOAD TO AOB APPINST FAILS: "ONE OR MORE INPUT REQUIRED PARAM.
30202020	[ROLECERT]: NO CERTIFICATION TASK CREATED FOR PROXY USER'S MANAGER
30239831	CONT: ADAPTER FACTORY GENERATING INVALID JAVA CODE.
30414695	ISSUE WITH OFFLINE CERTIFICATION COMMENTS FIELD LENGTH WHEN UPDATING FROM EXCEL
30500178	XL.CATALOGSEARCHRESULTCAP NOT ONLY AFFECT THE UI BUT ALSO INTERNAL PROCESSING

Note:

See Bulk Load Utility for Loading Accounts for information about the input required for loading account data by using the Bulk Load Utility.

Table 1-9 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.201011

Bug Number	Description
30546975	WHILE WITHDRAWING A REQUEST, THE CONFIRMATION BOX IS APPEARING WITH A BIG DIALOG
30716490	UNABLE TO PROCESS BATCH UPDATE IF ANY SSOTARGET IN PROVISIONING STATUS FOR USER
30717640	RULEENGINEEXCEPTION: INVALID RULE EXPRESSION - NOT_IN
30717793	CLONED DISCONNECTED PROVISIONING COMPOSITE FAILS AT ASSIGNREQUESTINPUT STAGE
30738489	REQUESTS/PENDING REQUESTS GET ERROR IF SECOND MANAGER IS DISABLED
30838859	[ROLECERT]: FUTURE STARTING PROXY USER RECEIVES CERTIFICATION
30865103	DELETE TASK NOT TRIGGERED ON ATTRIBUTE SET AS NOT ENTITLEMENT IN CHILD FORM
30865689	ISSUE AUDIT MESSAGES JOB DOES NOT PROCESS AUD_JMS - ORA-01403: NO DATA FOUND
30866653	ACCESS DENIED ERROR WHEN CALLING CREATEITRESOURCEINSTANCE FROM SCHEDULED TASK
30893984	APPLICATION INSTANCE SORT ORDER IN USER CERTIFICATION NOT ALPHABETICAL
30910129	DUPLICATE ACCESS POLICY NAME ERROR NOT CLEAR
30925400	CRYPTIC ERROR MESSAGE WHEN REQUEST FAILS
30930007	EXPERIENCING VERY SLOW PERFORMANCE WHEN SCANNING SOD POLICIES WITH 4.5K RULES.
30942250	CREATE ADMIN ROLE THROWS: JBO-29000: UNEXPECTED EXCEPTION CAUGHT: JAVA.LANG.NULLPOINTEREXCEPTION
30977436	USER ASSIGNED TO A ROLE WITH THE "+" CHAR IN THE NAME CAN'T ACCESS WORKLISTAPP

Table 1-9 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.201011

Bug Number	Description
30978612	AP HARVESTING SYNC ATTRIBUTES/ ENTITLEMENTS TO MATCH WITH THE ACCESS POLICY **Note:** See Access Policy Harvesting to Enable Account Data Update for information about the XL.APHarvesting.AllowAccountData Update system property for enabling account data update.
31057153	OIM 12C SSOTARGET APPLICATION PROFILE MODIFY NOT TAKING PATH IN LDAPCONTAINERRULES
31111401	ADMIN ROLE: JUMPING FROM SUMMARY PAGE BACK TO FIRST PAGE RESULTS IN LOST DATA
31114189	INTEGER FIELDS WITH NO VALUE DEFAULTING TO 0 FOR APPS CREATED USING AOB

Table 1-9 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.201011

Bug Number	Description
31162758	OIM 12C SSO USER TARGET RECON OVERWRITING ROLE VALUE SAVED ON OIM USER WITH DEFAULT VALUE
31177214	UNABLE TO ADD EMPLOYEE TYPE AS DISPLAY DATA IN THE INFORMATION WINDOW
31180365	UPGRADE FROM 11.1.2.3 TO 12.2.1.3: STRINGINDEXOUTOFBOUNDSEXCEPTION: STRING INDEX OUT OF RANGE: -19
31193971	ENTITLEMENT CERTIFICATIONS ARE NOT GETTING GENERATED FOR SOME OF THE CERTIFIERS.
31202544	NON REQUESTABLE ROLES INCONSISTENT BEHAVIOR IN CERT DEFN "CONTENT SELECTION"
31254720	DIAG: POOR LOGGING IN OIMDATAPROVIDER
31292576	PASSWORD CHANGE FLOW ISSUES AFTER FIX 30809484
31316925	ENT CERT SHOULD BE CREATED FOR CERTIFIER FOR REMAING ENT WHICH ARE CORRECT
31351771	INCONSISTENT VALUES IN THE REQUEST STATUS FILTER FROM TRACK REQUESTS PAGE

Note:

See Steps to Map the Role and employee Type Attributes for information about the manual steps required for the bug fix to work.

Table 1-9 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.201011

Bug Number	Description
31375771	SSO TARGET APPLICATION FAILS TO GET PROVISIONED WITH MANAGER ATTRIBUTE.
31434988	ENT_ASSIGN_HIST DOESN'T SAY IF THE ENTITLEMENT WAS PROVISIONED OR INPROGRESS
31464420	DISABLE USER TASK IS GETTING TRIGGERED FOR PROVISIONING ACCOUNTS
31555186	CERTIFY OIM OAM INTEGRATION ON SOLARIS
31605168	INTEROP: UPDATING ROLE NAME IN TARGET LDAP AND RECONCILE DID NOT UPDATE THE ENTILEMENTS IN INTEROP ENV
	Note: See Revoking Membership Does Not Work for the known issue about the bug fix.
31605187	INTEROP:SSO FULL USER RECON DID NOT UPDATE WITH LAST TOKEN VALUE
	Note: See SSO Full User Reconciliation for the manual steps required for the bug fix to work.

Table 1-9 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.201011

Bug Number	Description
31670117	INTEROP: ERROR COMING ON MODIFYING ROLE IN INTEROP AD ENVIRONMENT

Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200624

Applying this bundle patch resolves the issues described in Table 1-10.

Table 1-10 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
30216857	SETCHALLENGERESPONSESFORLOGGEDINUSER - CHALLENGE QUESTIONS PROVIDED ARE NOT DEFI
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 RESROUCES 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 FUNTIONALITY
30896936	PUMA: CUSTOM MESSAGE NOT DISPLAYED WHEN COMPLETING MANUAL TASK
31184149	PERFORMANCE ISSUE IN OIMDATAPROVIDER.GETARRAYFORHIERAR

Table 1-10 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200624

Bug Number	Description
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 1-11.

Table 1-11 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
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)

Table 1-11 (Cont.) Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200505

Bug Number	Description
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 1-12.

Table 1-12 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 AUTOCOMMITED 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/idmrn/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 12.2.1.4.210708). 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:

- Adding Missing ObjectClasses With OID
- Entitlement Type Not Available for Certification Reports
- Errors Related to the For Reportees Feature
- Identity Self Service and Identity System Administration Not Accessible
- Revoking Membership Does Not Work
- Upgrade Assistant Fails With StringIndexOutOfBoundsException
- Error on Running Bulk Load on ATP-D Setup

Adding Missing ObjectClasses With OID

As a workaround for the bug 33541821, while running `OIGOAMIntegration.sh` for adding the missing ObjectClasses with OID *only*, if you encounter the following error, then re-run the command and add the missing objectClasses.

Context Initialization Error

Solution:uncomment line number 227 in `_OIGOAMIntegration.sh:`

read `-p "Enter OID's ORACLE_HOME": ORACLE_HOME`

> **Note:**
>
> You have to input the OID MW_HOME from the command line.

Entitlement Type Not Available for Certification Reports

In this patch, the feature **Entitlement Type** is introduced. The Certification UI and the Certification report does not display **Entitlement Type** details.

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.

Revoking Membership Does Not Work

As part of the bug fix for 31605168, the entitlements are now updated with new role names, but the revoking of membership is not working.

Upgrade Assistant Fails With StringIndexOutOfBoundsException

Running the Upgrade Assistant for upgrading Oracle Identity Manager 11*g* Release 2 (11.1.2.3.0) to Oracle Identity Governance 12c (12.2.1.4) fails with the following error:

```
[2020-04-14T16:03:48.087-04:00] [Framework] [ERROR] [] [upgrade.Framework] [tid:
XX] [ecid: XXXX] [[
  java.lang.StringIndexOutOfBoundsException: String index out of range: -19
  at java.lang.String.substring(String.java:1967)
  at oracle.iam.oimupgrade.mrua.OIMMRUA.readiness(OIMMRUA.java:345)
  at oracle.ias.update.plugin.Plugin.readiness(Plugin.java:595)
  at oracle.ias.update.plan.PlanStep.readiness(PlanStep.java:730)
  at
oracle.ias.update.PhaseProcessor$ReadinessProcessor.runStepPhase(PhaseProcessor.j
ava:873)
  at oracle.ias.update.PhaseProcessor.runStep(PhaseProcessor.java:369)
  at
oracle.ias.update.PhaseProcessor$ExtendedRunnable.run(PhaseProcessor.java:1058)
  at
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
  at
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
  at java.lang.Thread.run(Thread.java:748)
]]
```

The issue takes place during the MDS backup. The cause of the error is the MDS JDBC URL used, which is in the form:

```
jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)
(HOST=xxxx)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=xxxx)
      (PORT=1521))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=xxxx)
(FAILOVER_MODE=(TYPE=select)(METHOD=basic))))
```

The upgrade tool does not expect complex URLs with something before the address field.

To workaround this issue, remove `(LOAD_BALANCE=ON)` from the JDBC URL.

Error on Running Bulk Load on ATP-D Setup

When you run the Bulk Load utility on ATP-D by using wallet, the utility exits with the following error:

```
./oim_blkld_usr_load.sh: line 260: /home/opc/db18c/bin/sqlplus: Permission denied
./oim_blkld_usr_load.sh: line 311: /home/opc/db18c/bin/sqlplus: Permission denied
./oim_blkld_usr_load.sh: line 336: /home/opc/db18c/bin/sqlplus: Permission denied
./oim_blkld_usr_load.sh: line 361: /home/opc/db18c/bin/sqlplus: Permission denied
./oim_blkld_usr_load.sh: line 386: /home/opc/db18c/bin/sqlplus: Permission denied
./oim_blkld_usr_load.sh: line 411: /home/opc/db18c/bin/sqlplus: Permission denied
./oim_blkld_usr_load.sh: line 436: /home/opc/db18c/bin/sqlplus: Permission denied
./oim_blkld_usr_load.sh: line 462: /home/opc/db18c/bin/sqlplus: Permission denied
./oim_blkld_usr_load.sh: line 486: /home/opc/db18c/bin/sqlplus: Permission denied
```

To workaround this issue:

1. Log in to Oracle WebLogic Administration Console as an administrator.
2. Click **Services**, **Datasources**.
3. Select the **oimOperationsDB** datasource.
4. Click **Connection Pool**, and check the URL value. It is similar to the following:

   ```
   jdbc:oracle:thin:@(DESCRIPTION=(CONNECT_TIMEOUT=120)(RETRY_COUNT=20)
   (RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3)(ADDRESS_LIST=(LOAD_BALANCE=on)
   (ADDRESS=(PROTOCOL=TCP)(HOST=abc.example.com)(PORT=1521)))
   (CONNECT_DATA=(SERVICE_NAME=db.example.com)))
   ```

5. Use the hostname, port, and service name from the URL value to run the Bulk Load utility.

Related Documents

For more information, see the following resources:

- Oracle Fusion Middleware Documentation

  This contains documentation for all Oracle Fusion Middleware 12*c* 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 12.2.1.4.220703
F58867-01