Oracle® Fusion Middleware

Oracle Identity Governance Bundle Patch Readme

12c (12.2.1.3.180713)

E97639-03

October 2018

Oracle Identity Governance Bundle Patch Readme

This document is intended for users of Oracle Identity Management 12c (12.2.1.3.180413). It contains the following sections:

- Understanding Bundle Patches
- 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
- Configuring Oracle Identity Governance-Oracle Access Manager Integration (Optional)
- Changes in Track Request Functionality
- IP Filter Related Updates
- 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.

- Bundle Patch
- Patch Set Exception
- Patch Set

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.

Bundle Patch Requirements

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

- Confirm you are applying this bundle patch to an Oracle Identity Governance 12.2.1.3.0 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 12.2.1.3.0. 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.

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.

Applying the Bundle Patch to an Existing Instance

Applying Oracle Identity Governance Release 12.2.1.3.180413 patch 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 rollback to the previous release.

• Stage 1: 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

Stage 1: 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 p27861122_122130_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 p27861122_122130_Generic.zip
    > ```

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

    ```
    cd PATCH_TOP/27861122
    ```

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

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

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

    ```
    opatch apply
    ```

> **✏ Note:**
>
> - Ensure the OPatch executables appear in your system PATH.
>
> - 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.

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/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/ 1.9.8.0.0/apache-ant-1.9.8/ For Windows: %MW_HOME% \oracle_common\modules\third party\org.apache.ant\1.9.8.0.0\ apache-ant-1.9.8\
java_home	Location of the JDK/JRE installation that is being used to run the Oracle Identity Governance domain.	For Linux: $MW_HOME/ oracle_common/jdk/ For Windows: %MW_HOME% \oracle_common\jdk\
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
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.	N/A
oim_serverurl	URL to navigate to Oracle Identity Governance.	t3:// oimhost.example.com:14000
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
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.	N/A

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

Parameter	Description	Sample Value
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.	N/A
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.	N/A
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
wls_serverurl	URL to navigate to WLS Console	t3://wlshost.example.com:7001

> **✎ 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:

   ```
   setenv PATH $JAVA_HOME/bin:$PATH
   ```

   For Microsoft Windows:

   ```
   set JAVA_HOME=VALUE_OF_JAVA_HOME
   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 in domain home:

   IAMGovernanceDomain/servers/oim_server1/tmp/_WL_user/ oracle.iam.console.identity.self-service.ear_V2.0

   Here, oim_server1 is the weblogic manged 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.
>
> - Ignore the following exception traces in the patch_oim_wls.log file:
>
> ```
> [java] Aug 11, 2015 3:45:28 AM
> oracle.jdbc.driver.OracleDriver registerMBeans
>     [java] WARNING: Error while registering Oracle JDBC
> Diagnosability MBean.
>     [java] java.security.AccessControlException: access
> denied (javax.management.MBeanTrustPermission register)
>     [java] at
> java.security.AccessControlContext.checkPermission(AccessCon
> trolContext.java:374)
> ```

6. Stop and start WebLogic Admin Server, SOA Servers, and Oracle Identity
   Governance Servers.

   - 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 Stage 1: Patching the Oracle
   Binaries (OPatch Stage) for more information.

3. Run 'Opatch apply' on ORACLE_HOME_B. See Stage 1: 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/27861122
```

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

```
opatch rollback -id 27861122
```

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.

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
- Postinstallation Configuration
- Updating Oracle Identity Governance Web Applications

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 Stage 1: 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
   ```

ORACLE®

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.

Configuring Oracle Identity Governance-Oracle Access Manager Integration (Optional)

This bundle patch release supports integration of Oracle Identity Governance (OIG) and Oracle Access Manager (OAM) using Connectors. For more information see, Integrating Oracle Identity Governance and Oracle Access Manager Using LDAP Connectors in *Integration Guide for Oracle Identity Management Suite*.

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.

In the search result table, user has to select a Show list option and click **Search**. Oracle Identity Governance will not trigger a search action until user clicks on **Search**.

IP Filter Related Updates

IP Filter (IPF) related updates are not part of the Oracle Identity Governance bundle patch release. For instructions on how to download and applying the IPF one-off bundle patch, see My Oracle Support document ID 2383246.1.

Major Enhancements in Release 12.2.1.3.180713

In the Self Service Roles page, when you create a UDF to add a Checkbox type attribute in the Catalog Attributes tab, the Apply button is enabled when navigating between the attributes tab of the role. To overcome this issue, a new change listener `catReqBean.checkBoxChangeListener` is introduced in this bundle patch release.

Resolved Issues

The following section lists the issues resolved in Release 12.2.1.3.180713:

Resolved Issues in Release 12.2.1.3.180713

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

Table 1-2   Resolved Issues in Release 12.2.1.3.180713

Bug Number	Description
27000479	JAVA.LANG.NOCLASSDEFFOUNDERROR: COM/ORACLE/OIM/GCP/ RESOURCECONNECTION/RESOURCECO
27067961	ENTITLEMENTS OUTSIDE ROLES OPTION NOT WORKING WITH DISPLAYNAME TRAILING SPACES
27078300	ENTITLEMENTS OUTSIDE ROLES CERT OPTION NOT TAKING INTO ACCOUNT INDIRECT ROLES
27098131	ENTITLEMENTS OUTSIDE ROLES OPTION NOT SHOWING APPLICATION INSTANCE
27100241	UNABLE TO DISPLAY DATA IN THE INFORMATION WINDOW
27177740	CLEAR TEXT PASSWORD CAUSING SRGSECCHECK/PSWDCHECK DIF (40+)
27181614	SCIM - CREATE USER FAILS IF ACTIVE ATTRIBUTE IS INCLUDED IN THE REQUEST
27196097	ROLE HIERARCHY TAB NOT SHOWING ALL PARENT ROLES
27273838	ROLE CAN'T BE ASSIGNED TO A DISABLED USER, IF UNCHECK GRANT DURATION CHECKBOX
27350190	ADD CONNECTOR VERSION PARAMETER TO AUTOMATION SCRIPT
27366933	REGRESSION FOR BUG 27040809

Table 1-2 (Cont.) Resolved Issues in Release 12.2.1.3.180713

Bug Number	Description
27423854	INCORRECT DEFAULT LOCATION OF CONNECTOR BUNDLE IN SSOINTG-CONFIG.PROPERTIES
27423992	SSOINTG-CONFIG.PROPERTIES SHOULD BE IGNORED WHEN RUNNING A SINGLE COMMAND
27438385	BI REPORT ORPHANED ACCOUNT SUMMARY NOT WORKING
27439501	PREUPGRADE ADMIN USERS UNABLE TO EDIT IT RESOURCES AFTER UPGRADE
27466871	ATTRIBUTE MODIFICATION INCONSISTENT FOR MYPROFILE AND USERS SECTION
27558461	OIM UNEXPECTED REVOKE ROLES
27564325	REGRESSION FOR PSE 27542629 FOR BASE BUG 27139050 ON TOP OF 11.1.2.3.170718OIMBP
27567365	CONFIGURELDAPCONNECTOR.SH FAILS - INVALID VERSION
27567443	ERROR IAM-3040026 OCCURES WHENEVER THE CHOOSEN QUESTIONS IS INTERNATIONALIZED
27617274	PARAMETER OIM_SERVER_NAME MISSING IN CONFIG FILE
27626487	NO ATTRIBUTE ORACLECONTEXT IN AD SHOULD NOT BE AN ERROR
27638151	ADDMISSINGOBJECTCLASSES HAS NO CONFIG FILE AND ASSUMES CONNECTION PARAMETERS
27638236	CONFIGURESSOINTEGRATION FAILS - COMMAND NOT FOUND
27697060	NO ATTRIBUTE SYSTEMIDPOLICY IN AD SHOULD NOT BE AN ERROR
27712164	OIM-OAM: IDM STAGE 8 SHIPHOME CAN NOT RUN OIGOAMINTEGRATION.SH
27719473	CONFIGURESSOINTEGRATION DOES NOT RETURN WRONG STATUS WHEN IDENTITY SERVER DOWN
27762094	WEBLOGIC_IDM DID NOT ADD IN IDM ADMINISTRATORS GROUP WHEN PREPAREIDSTORE FOR AD
27772143	ICONS MISSING FROM UI CONSOLE
27799154	OIM_SERVER_NAME VALUE IS NOT EFFECTIVE

Table 1-2　(Cont.) Resolved Issues in Release 12.2.1.3.180713

Bug Number	Description
27806091	OIM-OAM-AD: CONFIGURELDAPCONNECTOR FAILED WITH FILENOTFOUNDEXCEPTION
27939257	USRPROCESSTRIGGER IS GETTING NULL POINTER EXCEPTION

Resolved Issues in Release 12.2.1.3.180413

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

Table 1-3　Resolved Issues in Release 12.2.1.3.180413

Bug Number	Description
25323654	AOB: TEST CONNECTION IS SUCCESS EVEN IF INVALID VALUES IN BASIC CONFIG
25996056	NOTSERIALIZABLEEXCEPTION EXCEPTIONS BEING LOGGED WHEN ACCESSING WORKFLOW
26165573	EXTENSION TO THE FOLLOWING BUG 25727240 (REFRESH MATERIALIZED VIEW)

> **✎ Note:**
>
> For manual steps on how to apply changes done for Bug Fix 26165573, see My Oracle Support document ID 2383245.1.

26186971	Fix for Bug 26186971
26188366	Fix for Bug 26188366

Table 1-3   (Cont.) Resolved Issues in Release 12.2.1.3.180413

Bug Number	Description
26288324	THE ENTITLEMENT GETPROVISIONED EVEN IF GRANT END DATE IS PASSED AT APPROVE TIME
26427097	DELETING APP INSTANCE RESULTS IN JAVA.LANG.STRINGINDEXOUTOFBOUNDS EXCEPTION
26474713	AOB: PROVIDE FEATURE TO ADD NEW CONFIGURATION PROPERTIES IN ADVANCED SETTINGS
26500524	AOB: SAP AC UM AND UME FORM FIELDS ARE UPDATED BLANK AFTER RUN USER RECON
26522972	AOB: REVOKE ACCOUNT IS NOT WORKING IN SAP AC UM & UME
26616250	TARGET USER RECON IS FAILING FOR CI BASED INSTALLATION
26681376	PUBLISH IN TOP AND SUB ORGANIZATIONS BY OIM API IS TAKING LONG TIME
26729272	NOTSERIALIZABLEEXCEPTION RETURNVALUEROW WHILE EDIT WORKFLOW RULES IN OIM CLUSTER
26932665	DEPENDENT REQUEST DETAILS NOT VISIBLE DUE TO SCROLLBAR MISSING
26967104	AOB: DISPLAY NAME OPTION NOT COMING WHILE ADDING NEW ADVANCED CONFIG ATTRIBUTE
26967178	AOB: OPTION NOT COMING TO ADD ADV CONFIG ATTRIBUTE IF NO ATT EXISTS IN TEMPLATE
26982896	MANAGER INFORMATION SHOWING BLANK IN USER CERTIFICATION ON THE UI
27025473	LIGHT WEIGHT AUDIT PUREGE - REMOVE AUDIT LOG ENTRIES JOB IS RUNNING TOO LONG
27026427	KSS NOT UPDATED FROM DEFAULT-KEYSTORE.JKS BREAKS JWT
27113693	UPGRADE ASSISTANT READINESS CHECK FAILED DUE TO OIM 11.1.1.3.0 TEMPLATE
27119830	RECONFIG DOMAIN DOESN'T TAKE OIM 11.1.1.X VERSION APPS INTO CONSIDERATION

ORACLE®

Table 1-3   (Cont.) Resolved Issues in Release 12.2.1.3.180413

Bug Number	Description
27145500	ERROR DUE TO CHANGES IN "SOAOIMLOOKUPDB" DATASOURCE IN 12CPS3
27166581	RESOURCE HISTORY SHOWS INCORRECT ENTITLEMENT NAME AFTER BP 26858666 (OCT-17)
27168000	LIBRARY ORACLE.IDM.IPF WAS TARGETED TO OIM AND SOA CLUSTER INSTEAD OF ADMINSERVE
27200817	SEARCH SELECTIONS DO NOT WORK FOR CREATE/MANAGE USER IF CLICK BACK TO USERS LIST
27279346	AOB: APPLICATION CREATION FAILING WITH USER NOT HAVING SYSTEM ADMIN PERMISSION
27384225	AFTER APPLYING OCTOBER BP POLICY VIOLATIONS IS NOT DETECTING ANY VIOLATIONS
27510030	POLICY VIOLATION NOT THROWN FOR DISABLED ACCOUNT
27564429	AOB: SAP UM USER DELETE RECON IS NOT WORKING IN 12C WITH LATEST BP
27567130	CONFIGURELDAPCONNECTOR.SH FAILS

Resolved Issues in Release 12.2.1.3.180109

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

Table 1-4   Resolved Issues in Release 12.2.1.3.180109

Bug Number	Description
23110063	IMPLEMENTATION OF BULK ATTRIBUTES UPDATE FOR AN ACCOUNT IMPACTS OTHER ACCOUNTS
23337308	CERTIFICATION COLUMN NAME "CREATED BY" AND "UPDATED BY" DISPLAYS USR_KEY
25540355	PS3PARITY:"USER TYPE" VALUE DOESN'T GET SELECTED ON FIRST ATTEMPT
26164709	LOG4J.JAR NOT UPDATED IN SETENV.BAT
26434476	WAITING ON ENTITLEMENT STATUS, PATCH 25292874

Table 1-4   (Cont.) Resolved Issues in Release 12.2.1.3.180109

Bug Number	Description
26592805	USERS SHOULD NOT BE ABLE TO REVOKE ENT THAT IS PART OF ROLE FROM THEIR MY ACCESS
26615293	SEARCH ON CERTIFICATION DEFINITION CONTENT SELECTION PAGE RETURNS ONLY 28 ROLES
26625354	CERTIF ROLE POLICY TAB CATALOG INFO ENTITLEMENT URL SHOW NO ENTITLEMENT DETIALS
26639196	REPLACE EXISTING SEARCH IN CERT. DEF FLOW RESULTS IN ERROR PAGE AND NPE
26732357	CERTIFCATION RESET STATUS CAUSING NPE
26808282	DATASOURCE CONNECTION LEAK AFTER BUG 20293874
26811926	LIBRARIES FOR MANAGED BEANS AND TASK FLOWS ARE MISSING IN 12C
26863966	SEARCH RETURNS REQUESTS FOR REPORTEES AND NON-REPORTEES FOR R2PS2
26895672	OAM_OIM_OVD_OID_UPG: USER CREATION IS FAILED
27025966	THIS IS THE TRACKER BUG FOR EPIC OIM-11380
27037128	Fix for Bug 27037128
27110896	BE CONSISTENT WITH SPECIFYING PARAMETERS IN OAM/OIM INTEGRATION
27112593	ERROR WHEN GETTING CONNECTOR SERVER DETAILS BY NON SYSTEM ADMINISTRATOR
27119849	NLS : ISSUE WHILE SETTING CHALLENGE QUESTIONS WHEN FIRST LOGIN
27133948	OIM-OAM-OUD: ADMIN FAILED TO UNLOCK A SELF LOCKED ACCOUNT
27139528	Fix for Bug 27139528
27175826	OIM-OAM-AD: CONFIGURELDAPCONNECTOR FAILED CONNECTOR PACKAGE IS NOT AVAILABLE
27203691	OIM-OAM-OUD: SSO GROUP MEMBERSHIP INCREMENTAL RECONCILIATION DO NOT WORK
27298564	REPLACE EXISTING SEARCH IN CERT DEF FLOW RESULTING CERT IS NOT GETTING GENERATED

Table 1-4   (Cont.) Resolved Issues in Release 12.2.1.3.180109

Bug Number	Description
27300245	OIM-OAM-OID: USER SESSION IS NOT TERMINATED WHEN IT IS DELETED BY ADMIN
27313843	12C BP01: USER SESSION IS NOT TERMINATED WHEN IT IS LOCKED OR DISABLED BY ADMIN

Known Issues and Workarounds

Known issues and their workarounds in Oracle Identity Governance Release 12.2.1.3 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/middleware/12213/idmsuite/IDMRN/toc.htm

> **Note:**
>
> Some known issues listed in the Release Notes for Oracle Identity Management may have been resolved by this Bundle Patch (Oracle Identity Governance Release 12.2.1.3.180713). 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:

- LDAP User Create and Update Reconciliation Job Fails in Integrated and Upgraded Environment
- IT Resource Password is Updated as Null
- Recommendations for Upgrade
- Oracle Identity Governance Server URL is Inaccessible After Rollback
- Role Hierarchy Tab shows only 301 Roles

LDAP User Create and Update Reconciliation Job Fails in Integrated and Upgraded Environment

Issue

Impacted Releases: 12*c* Release (12.2.1.3.0)

When Oracle Identity Governance Release 11.1.2.3 deployment is integrated with
Oracle Access Management, libOVD, and Oracle Unified Directory, and upgraded
to Release 12*c* (12.2.1.3.0), the LDAP User Create and Update Reconciliation
scheduled job run fails with the following error when a new user is created and its
status is set to locked in the system:

```
[2017-06-05T23:39:53.833-07:00] [oim_server1] [ERROR] []
[oracle.iam.ldapsync.scheduletasks.user] [tid: OIMQuartzScheduler_Worker-8]
[userId: oiminternal] [ecid: b2fc7981-724e-474c-b009-8a5e2d915d52-000008e9,0]
[APP: oim] [partition-name: DOMAIN] [tenant-name: GLOBAL] An error occurred
while processing the data that is retrieved from LDAP to create a
reconciliation event.[[
oracle.iam.ldapsync.exception.ReconEventCreationException:
Thor.API.Exceptions.tcAPIException: Exception occurred while inserting data
into table RA_LDAPUSER due to java.sql.SQLException: execute, Exception =
null
        at
oracle.iam.ldapsync.scheduletasks.user.LDAPUserChangesReconTask.createUserReco
nciliationEvent(LDAPUserChangesReconTask.java:435)
        at
oracle.iam.ldapsync.scheduletasks.user.LDAPUserChangesReconTask.processResult(
LDAPUserChangesReconTask.java:179)
        at
oracle.iam.ldapsync.scheduletasks.user.LDAPUserChangesReconTask.execute(LDAPUs
erChangesReconTask.java:132)
...
Caused by: Thor.API.Exceptions.tcAPIException: Exception occurred while
inserting data into table RA_LDAPUSER due to java.sql.SQLException: execute,
Exception = null
        at
oracle.iam.reconciliation.impl.ReconOperationsServiceImpl.createReconciliation
Event(ReconOperationsServiceImpl.java:431)
        at
oracle.iam.reconciliation.impl.ReconOperationsServiceImpl.createReconciliation
Event(ReconOperationsServiceImpl.java:418)
...
Caused by: oracle.iam.reconciliation.exception.ReconciliationException:
Exception occurred while inserting data into table RA_LDAPUSER due to
java.sql.SQLException: execute, Exception = null
        at
oracle.iam.reconciliation.impl.ReconOperationsServiceImpl$1.process(ReconOpera
tionsServiceImpl.java:489)
        at
oracle.iam.reconciliation.impl.ReconOperationsServiceImpl$1.process(ReconOpera
tionsServiceImpl.java:467)
        at
oracle.iam.platform.tx.OIMTransactionCallback.doInTransaction(OIMTransactionCa
llback.java:13)
        at
oracle.iam.platform.tx.OIMTransactionCallback.doInTransaction(OIMTransactionCa
llback.java:6)
        at
org.springframework.transaction.support.TransactionTemplate.execute(Transactio
nTemplate.java:130)
        at
oracle.iam.platform.tx.OIMTransactionManager.executeTransaction(OIMTransaction
Manager.java:47)
```

```
        at
oracle.iam.reconciliation.impl.ReconOperationsServiceImpl.reconEvent(ReconOper
ationsServiceImpl.java:467)
        at
oracle.iam.reconciliation.impl.ReconOperationsServiceImpl.createReconciliation
Event(ReconOperationsServiceImpl.java:406)
        at
oracle.iam.reconciliation.impl.ReconOperationsServiceImpl.createReconciliation
Event(ReconOperationsServiceImpl.java:429)
        ... 44 more
Caused by: oracle.iam.platform.utils.SuperRuntimeException:
java.sql.SQLException: execute, Exception = null
        at
oracle.iam.reconciliation.dao.event.EventMgmtDao.create(EventMgmtDao.java:244)

        at
oracle.iam.reconciliation.impl.ReconOperationsServiceImpl$1.process(ReconOpera
tionsServiceImpl.java:478)
        ... 52 more
Caused by: java.sql.SQLException: execute, Exception = null
        at
weblogic.jdbc.wrapper.JDBCWrapperImpl.invocationExceptionHandler(JDBCWrapperIm
pl.java:143)
        at
weblogic.jdbc.wrapper.Statement.invocationExceptionHandler(Statement.java:142)

        at
weblogic.jdbc.wrapper.PreparedStatement.invocationExceptionHandler(PreparedSta
tement.java:100)
        at
weblogic.jdbc.wrapper.PreparedStatement.execute(PreparedStatement.java:125)
        at
oracle.iam.reconciliation.dao.event.EventMgmtDao.create(EventMgmtDao.java:234)

        ... 53 more
Caused by: java.lang.NullPointerException
        at
oracle.jdbc.driver.OracleSql.setNamedParameters(OracleSql.java:174)
        at
oracle.jdbc.driver.OracleCallableStatement.execute(OracleCallableStatement.jav
a:4229)
        at
oracle.jdbc.driver.OraclePreparedStatementWrapper.execute(OraclePreparedStatem
entWrapper.java:1080)
        at
weblogic.jdbc.wrapper.PreparedStatement.execute(PreparedStatement.java:119)
        ... 54 more
```

Workaround

As a workaround to this issue, before running the `LDAP User Create and Update Reconciliation` scheduled job:

1. Login to My Oracle Support website at:

   https://support.oracle.com

2. Search and download JDBC patch p26400304_122130_Generic.zip.

3. Apply the JDBC patch.

4. Run the `LDAP User Create and Update Reconciliation` scheduled job.

IT Resource Password is Updated as Null

Issue

Impacted Releases: 12c Release (12.2.1.3.0)

When Oracle Identity Governance is upgraded from Release 11*g* (11.1.2.3.0) to Release 12*c* (12.2.1.3.0), password of IT resources like Directory Server, Email Provider Definition - UMS, and OIA-ITRes are updated in Credential Store (CSF) as Null. This causes LDAP operations associated with these IT resources to fail.

Workaround

After upgrade, bring OIG Server up and immediately reset password for these IT resources types, Directory Server, Email Provider Definition - UMS, and OIA-ITRes.

To reset the IT resources password:

1. Login to Oracle Identity System Administration.

2. Locate the IT Resource for which you want to reset the password.

3. For Directory Server edit the **Admin Password** parameter value and for Email Provider Definition - UMS and OIA-ITRes edit the **Password** parameter value.

For detailed steps on how to search and modify IT Resources parameters, see Managing IT Resources in *Administering Oracle Identity Governance.*

Recommendations for Upgrade

Few upgrade bugs are resolved in this bundle patch release, 27113693, 27119830, 27145500, and 27168000. See Resolved Issues in Release 12.2.1.3.180413.

Pre-upgrade report will be generated if any of the issue stated in above bugs exists in a Oracle Identity Manager 11gR2PS3 setup prior to upgrading it to Oracle Identity Governance 12.2.1.3.0 version. For automated fix of these upgrade bugs, please apply the Bundle Patch Release 12.2.1.3.180413 binaries on top of Oracle Identity Governance 12.2.1.3.0 binaries and then proceed with Oracle Identity Governance 12.2.1.3.0 upgrade process. Steps for manual fix are present in pre-upgrade reports.

Oracle Identity Governance Server URL is Inaccessible After Rollback

Issue

Impacted Releases: 12c Release (12.2.1.3.0)

When Oracle Identity Governance Bundle Patch is rolled back, the previous version of Oracle Identity Governance is restored. When you try to access the OIG Server URL it is inaccessible as the `/db/oim-config.xml` file is overwritten.

Workaround

Workaround for this problem is to restore the base version of the `/db/oim-config.xml` file. For example, if you want to rollback Oracle Identity Governance Bundle Patch 12.2.1.3.180111, then before rollback, import the Oracle Identity Governance 12.2.1.3.0 base version `/db/oim-config.xml` file from the backup created before applying the Oracle Identity Governance Bundle Patch 12.2.1.3.180111. Then rollback the bundle patch.

Role Hierarchy Tab shows only 301 Roles

Issue

Impacted Releases: 12c Release (12.2.1.3.180713)

In the Role Hierarchy page, the Define Role Hierarchies panel shows only 301 roles.

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, 12c (12.2.1.3.180713)
E97639-03