Oracle® Fusion Middleware

Oracle Identity Governance Bundle Patch Readme

OIM Bundle Patch 14.1.2.1.251017

G36971-02

October 2025

Oracle Identity Governance Bundle Patch Readme

This document is intended for users of OIM BUNDLE PATCH 14.1.2.1.251017. It contains the following sections:

Understanding Bundle Patches

This section describes Bundle Patches and explains differences between Stack Patch Bundles, Bundle Patches, interim patches (also known as one-offs) and Patch Sets.

Stack Patch Bundle

Copyright © 2025, Oracle and/or its affiliates.

Stack Patch Bundle deploys the IDM product and dependent FMW patches using a tool. For more information about these patches, see *Stack Patch Bundle for Oracle Identity Management Products (Doc ID 2657920.2)* 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 "YYMMDD" format 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 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 components in the Bundle Patch.

Each Bundle Patch is cumulative: the latest Bundle Patch includes all fixes in earlier Bundle Patches for the same release and platform. Fixes delivered in Bundle Patches are rolled into the next release.

Interim Patch

In contrast to a Bundle Patch, an interim patch addresses only one issue for a single component. Although each interim patch is an official Oracle patch, it is not a complete product distribution and does not include packages for every component. An interim patch includes only the libraries and files that have been rebuilt to implement a specific fix for a specific component.

Interim patch is also known as, security one-off, exception release, x-fix, PSE, MLR, or hotfix.

Patch Set

A Patch Set is a mechanism for delivering fully tested and integrated product fixes that can be applied to installed components of the same release. Patch Sets include all fixes available in previous Bundle Patches for the release. A Patch Set can also 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 fixes in the Patch Set have been tested and are certified to work with one another on the specified platforms.

Copyright © 2025, Oracle and/or its affiliates.

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 *Stack Patch Bundle for Oracle Identity Management Products (Doc ID 2657920.2)* 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 14.1.2.1.0 installation.

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

- Download the latest version of OPatch. Oracle recommends using the latest version of OPatch to all customers. To learn more about OPatch and how to download the latest version, see Using OUI NextGen OPatch 13 for Oracle Fusion Middleware 12c /14c (*Doc ID 1587524.1*) at https://support.oracle.com.

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

- Verify the Oracle Universal Installer (OUI) Inventory. To apply patches, OPatch requires access to a valid OUI Inventory. To verify the OUI Inventory, ensure that ORACLE_HOME/OPatch path appears in your system 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 that 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
  ```


Copyright © 2025, Oracle and/or its affiliates.

Both executables must appear in the environment variable 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 the Bundle Patch must have read, write, and execute permissions on both ORACLE_HOME as well as WebLogic DOMAIN_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 Deploying and Undeploying Customizations.

Applying the Bundle Patch to an Existing Instance

Applying OIM BUNDLE PATCH 14.1.2.1.251017 is done in the following stages:

Copyright © 2025, Oracle and/or its affiliates.

> **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

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 managed servers, the SOA managed servers and the Admin Server in this order.
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 script on ORACLE_HOME_A with WebLogic Admin Server, oim_server1, and soa_server1 running.

   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 script.
5. Restart the managed servers on all the nodes.

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.

Copyright © 2025, Oracle and/or its affiliates.

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

1. Stop all Oracle Identity Governance managed servers, all SOA managed servers and the Admin Server in this order.
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 p38552250_14.1.2.1.0_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
   > p38552250_14.1.2.1.0_Generic.zip
   > ```

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

   ```
   cd PATCH_TOP/38552250
   ```

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

   ```
   export 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
   ```


Copyright © 2025, Oracle and/or its affiliates.

> **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 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_oim_wls.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.

Copyright © 2025, Oracle and/or its affiliates.

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\apache-ant For Windows: %MW_HOME%\oracle_common\modules\thirdparty\org.apache.ant\apache-ant
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 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
domain_home	Location of the domain home on which Oracle Identity Governance is installed.	For Linux: $MW_HOME/user_projects/domains/base_domain For Windows: %MW_HOME%\user_projects\domains\base_domain
weblogic_user	Domain administrator username. 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

Copyright © 2025, Oracle and/or its affiliates.

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.	oimhost.example.com

Note

If the SOA Managed Server is configured to use a

Copyright © 2025, Oracle and/or its affiliates.

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

Parameter	Description	Sample Value
		virtualIPaddress, the entheviirtualhostnamemustbesuppl

Copyright © 2025, Oracle and/or its affiliates.

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

Parameter	Description	Sample Value
		i e d .
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	Hostname 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 hostname	oimdbhost.example.com
mdsDB.port	MDS database/Listen port	1521
mdsDB.serviceName	MDS database service name	oimdb.example.com
oim_username	Oracle Identity Governance username.	System administrator username
oim_password	Oracle Identity Governance password. This is optional. If this is commented out, then you will be prompted for the password when the script is executed.	NA
oim_serverurl	URL to navigate to Oracle Identity Governance.	t3:// oimhost.example.com:14000

Copyright © 2025, Oracle and/or its affiliates.

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

Parameter	Description	Sample Value
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 to the correct locations, 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) **or** 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.

Copyright © 2025, Oracle and/or its affiliates.

> **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
   ```


Copyright © 2025, Oracle and/or its affiliates.

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

4. Clear the following folders from the Oracle Identity Governance domain:

   $DOMAIN_HOME/servers/<oig_managed_server>/tmp

   $DOMAIN_HOME/servers/<oig_managed_server>/stage

   $DOMAIN_HOME/servers/<oig_managed_server>/cache

   Here, the <oig_managed_server> is the name of the WebLogic managed server used for Oracle Identity Governance.

5. To verify that the patch_oim_wls script has completed successfully, check the ORACLE_HOME/idm/server/bin/patch_oim_wls_YYYY-MM-DD_hh-mm-ss.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.

Applying the Bundle Patch to a New Instance

Perform the following steps to apply the Bundle Patch to a new instance:

- Installing a New Oracle Identity Governance Instance with OIM BUNDLE PATCH 14.1.2.1.251017

Installing a New Oracle Identity Governance Instance with OIM BUNDLE PATCH 14.1.2.1.251017

Copyright © 2025, Oracle and/or its affiliates.

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

- Using the Quickstart Installer
- Using the Generic Installer

Using the Quickstart Installer

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

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

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

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

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

Using the Generic Installer

Copyright © 2025, Oracle and/or its affiliates.

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

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

1. Start the installation by referring to Traditional Method of *Installing and Configuring Oracle Identity and Access Management*. Before creating the database schema, apply the patch by using OPatch, as described in Stage 1: Patching the Oracle Binaries (OPatch Stage). Then, continue with schema creation.

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

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

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

Copyright © 2025, Oracle and/or its affiliates.

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/38552250
```

3. Run OPatch as follows to remove the Bundle Patch:

```
opatch rollback -id 38552250
```

4. Restore ORACLE_HOME and the WebLogic domain home.
5. Restore the Oracle Identity Governance database using the backup you created in Step 1 of Applying the Bundle Patch to an Existing Instance.

Resolved Issues

The following section lists the issues resolved in Release 14.1.2.1.0:

- Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.251017
- Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.250708
- Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.250328

Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.251017

Applying this Bundle Patch resolves the issues described in the following table.

Table 1-2 Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.251017

Bug	Description
38264329	CVE-2025-61757
37738142	TRACK REQUEST SHOWS PAGE FULL OF SAME REQUEST
38206487	UNREGISTERED EVENT HANDLERS ARE TRYING TO BE RUN AND FAIL
35782191	TESTING AD CONNECTOR VIA AOB. CONNECTION FAILS. NEED BETTER (CLEARER) MESSAGE
37929656	ACCOUNT CONTEXT MENU INCONSISTENCY IN GERMAN LANGUAGE
38011656	PROXY EDIT ALLOWS OVERLAPPING DATES
38211304	JOBS NOT GETTING INTERRUPTED/ COMPLETED EVEN AFTER DOING CLEAN RESTART

Copyright © 2025, Oracle and/or its affiliates.

Table 1-2 (Cont.) Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.251017

Bug	Description
38243277	CERTIFICATION ELEVATED USER (CERTFICATIONADMINUSER) IS ABLE TO SELF CERTIFY
38235447	DISCONNECTED APP ENTITLEMENT IS GETTING REMOVED BEFORE REVOKE MFT IS COMPLETED
37233015	508: GROUP ASSOCIATION FOR ADF COMPONENTS OF OIG/OIM UI PAGES
38145967	DUPLICATE OUD ACCOUNTS CREATED ON RETRY OF FAILED RECONCILIATION EVENTS IN OIG
37943741	POLICY VIOLATION IS NOT RAISED FOR ROLES AND ACCOUNTS FOR INFLIGHT REQUESTS.
38070770	ATPD 23AI DURING OIM SCHEMA CREATION USING RCU NOTICIED ERROR ORA-01031: INSUFFICIENT PRIVILEGES
38197180	SET ACCESS POLICY EVALUATE FLAG WHEN USER IS ENABLED AND RESOURCE DEPENDENCY IS SETUP
37472016	SCHEDULER JOBS OCCASIONALLY FIRE TWICE SINCE INSTALLING IDM_SPB_12.2.1.4.240415
38077593	OJET PAGES ARE LOADING FOR END USERS WITH OUT ANY PRIVILEGES
38078989	ACCESS POLICY FAILS TO PROVISON DEPENDENT APPLICATION WHEN THE START DATE IS FUTURE
38001573	NO FORM ASSOCIATED WITH THE PROVISIONING PROCESS OF THE PROVISIONED RESOURCE
37985881	BULK LOAD UTILITY FOR GOOGLE APPS FAILS WITH "ORA-00907: MISSING RIGHT PARENTHESIS" ERROR
37774569	CUSTOM UDFS TAKE PREVIOUS VALUES ON CERT PAGE IF THE CURRENT VALUE IS BLANK
38040150	FUTURE START DATE CAUSES OIG TRUSTED RECON FAILURE AND DUPLICATE OUD PROVISIONING
38023420	ENTITLEMENT CERTIFICATION FAILS FOR DYNAMIC ORG
37984958	HOW TO CONFIGURE OAM/OIM INTEGRATION WHEN NO OAP IS USED.
37926326	EVAL USER POLICY ATTEMPTING TO DISABLE TARGETS THAT DO NOT SUPPORT DISABLE

Copyright © 2025, Oracle and/or its affiliates.

Table 1-2 (Cont.) Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.251017

Bug	Description
37479113	ERROR!!RECON DATA PURGE CANNOT BE COMPLETED DUE TO EXCEEDING THE THRESHOLD VALUE
37564661	RESET PASSWORD FOR XELSYSADM FAILS WHEN LDAPADMINUSER HAS SPACE CHARACTER
37288812	DAYS BETWEEN RUNS REMAINS EMPTY AFTER OCT 24 SPB

Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.250708

Applying this Bundle Patch resolves the issues described in the following table.

Table 1-3 Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.250708

Bug	Description
37912966	PROV TASKS GOES REJECTED STATUS WHEN THE VALUE IS REMOVED FROM DATE FIELDS (SSO SETUP)
37593041	USER CERTIFICATION JOBS ARE FAILING
37916124	ADDING CUSTOM FIELDS TO APPLICATION SCHEMA IS FAILING
37949703	ROLE CERT REPORTS SHOWING INVALID DATA AFTER OCT 24 STACK PATCH BUNDLE
37838929	Fix for Bug 37838929
36460208	UI- ISS APPLICATION AND SYSTEM CONFIGURATION LIMITED TO A SMALL FRAME WINDOW.
37603463	OIG12CPS4: PROBLEM WITH ASSIGNING A GROUP OF ACCEPTANCE WHEN HAVING A PROXY
37604877	DISABLE JOB RUNS AUTOMATICALLY OFTEN
37623243	CONNECTOR ERRORS ARE NOT BEING LOGGED
37815446	IGNORE RESOURCE LIST FOR ENTITLEMENT LIST JOB IS NOT WORKING
37640708	CERTS "PREVENT SELF CERTIFICATION" NOT WORK FOR ENTITLEMENT TYPE CERTIFICATION WITH PROXY USERS
37567925	ACC: OATB TABLE HAS ERRORS IN CERTIFICATION DASHBOARD
36575454	MANUAL FULFILLMENT TASKS GOING TO "STALE" STATE

Copyright © 2025, Oracle and/or its affiliates.

Table 1-3 (Cont.) Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.250708

Bug	Description
37235779	GENERIC REST CONNECTOR THROWS GENERIC MESSAGE FOR 409 EXCEPTIONS
37263547	CUSTOM UDFS DON'T CHANGE VALUE ON THE CERTIFICATION USER DETAIL PAGE
37659461	USER PROXIES ALLOWS OVERLAPPING DATES FOR MANAGER AND OTHER TYPE PROXIES
37810395	PASSWORD RESET POPUP - PROPOSAL TO IMPROVE CLARITY
37790603	UPDATE OF START DATE AND END DATE TRIGGERING DUPLICATE PROV TASKS IN OIM-OAM ENV
34812616	USER WITH ADMIN ROLE IS UNABLE TO LOCK/UNLOCK USERS IN OIM.
36874561	ASTERISK SIGN AND HEADING ARE NOT COMPLIANT WITH WCAG 2.1 LEVEL A 1.3.1INFO AND RELATIONSHIPS
37203068	MANUALLY LOCKED USERS BEING UPDATED FROM OUD TRUSTED RECON
37349902	OIG12CPS4:DIAGNOSTIC_MAINT JOB IS NOT PURGING DATA ON DIAG_LOG AND DIAG_LOG_DTLS
37461743	APPROVAL TASK OF APPROVAL DETAILS SECTION ARE NOT GETTING LOADED ON REFRESHING REQUEST PAGE
37639701	ACCESSIBILITY ISSUES: KEYBOARD NAVIGATION NOT WORKING AS EXPECTED
37651931	37197658 REGRESSION: WHEN REMEDIATOR ROLE SET IS DELETED, IDA POLICY DO NOT OPEN ON UI.
37386262	QUERY BY EXAMPLE IS NOT ENABLED FOR ACCOUNT STATUS COLUMN IN USERS PAGE
37257293	MODIFYING THE 'USE BULK' FLAG DOES NOT MAKE ANY CHANGES IN THE BACKGROUND
37473491	ROLEUSERMEMBERSHIPRULESQLSUPPORTED SHOULD NOT LIMITED TO ACTIVE USERS
37008610	SSO GROUP MEMBERSHIP INCREMENTAL RECON DOESN'T WORK FOR ALL SPECIAL CHARACTERS
36891740	OIG12CPS4: AOB UI DOES NOT PROVIDE SEPARATE REQUIRED/OPTIONAL OPTION FOR RECONCILIATION FIELDS

Copyright © 2025, Oracle and/or its affiliates.

Table 1-3 (Cont.) Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.250708

Bug	Description
37465786	ADDING "STATUS" COLUMN IN HOMPAGE WORKFLOW FOR DIRECT REPORTS CAUSES DUPLICATES

Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.250328

Applying this Bundle Patch resolves the issues described in the following table.

Table 1-4 Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.250328

Bug	Description
37621708	FMW 14121 : OIM : SYSADMIN PAGE : HELP PAGE IN LOGIN SCREEN : COPYRIGHT UPDATE REQUIRED
37621784	FMW 14121 : OIM : IDENTITY PAGE : HELP PAGE IN LOGIN SCREEN : COPYRIGHT UPDATE REQUIRED

Known Issues and Workarounds

Known issues and their workarounds in Oracle Identity Governance Release 14.1.2 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/14.1.2/idmrn/index.html

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

- ANT Location Updated for Windows

ANT Location Updated for Windows

Copyright © 2025, Oracle and/or its affiliates.

For Windows, before running patch_oim_wls.bat, the ANT location must be updated from

%MW_HOME%
\oracle_common\modules\thirdparty\org.apache.ant\1.10.5.0.0\apache-ant-1.10.5

to the following location:

%MW_HOME%\oracle_common\modules\thirdparty\org.apache.ant\apache-ant.

Related Documents

For more information, see the following resources:

- Following is the list of guides for this release:
  - Administering Oracle Identity Governance
  - Developing and Customizing Applications for Oracle Identity Governance
  - Upgrading Oracle Identity Manager
  - Performing Self Service Tasks with Oracle Identity Governance
- This contains documentation for all Oracle Fusion Middleware 14*c* products.

  Oracle Fusion Middleware Documentation
- This site contains additional documentation that is not included as part of the documentation libraries.

  Oracle Technology Network

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 14.1.2.1.251017
G36971-02

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

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

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