Oracle® Fusion Middleware

Oracle Identity Governance Bundle Patch Readme OIM Bundle Patch 14.1.2.1.250328 G30319-01

Oracle Identity Governance Bundle Patch Readme

This document is intended for users of OIM BUNDLE PATCH 14.1.2.1.250328. It contains the following sections:

- Understanding Bundle Patches
- Recommendations
- Bundle Patch Requirements
- Prerequisites of Applying the Bundle Patch
- Applying the Bundle Patch to an Existing Instance
- Applying the Bundle Patch to a New Instance
- Removing the Bundle Patch
- Resolved Issues
- Known Issues and Workarounds
- Related Documents
- Documentation Accessibility

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
- Bundle Patch
- Interim Patch
- 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 *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.



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



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 14.1.2.1.250328 is done in the following stages:



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)

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 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. 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 all Oracle Identity Governance managed servers, all SOA managed servers and the Admin Server in this order.
- Create a directory for storing the unzipped Bundle Patch. This document refers to this directory as PATCH_TOP.
- 3. Unzip the patch zip file into the PATCH_TOP directory you created in step 2 by using the following command:

unzip -d PATCH_TOP p37765984_141210_Generic.zip



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 p37765984_141210_Generic.zip

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

cd PATCH_TOP/37765984

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

 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" (which translates as "OPatch cannot find a valid oralnst.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.



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 Servers and Oracle Identity Governance Servers.

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
 14.1.2.1.250328

Installing a New Oracle Identity Governance Instance with OIM BUNDLE PATCH 14.1.2.1.250328

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

- Using the Quickstart Installer
- Using the Generic Installer

Using the Quickstart Installer

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

Note:

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

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



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

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 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.

- 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/37765984

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

opatch rollback -id 37765984

- 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 14.1.2.1.250328

Resolved Issues in OIM BUNDLE PATCH 14.1.2.1.250328



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

Table 1-1Resolved 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

In this release we do not have any known issues and work around.

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 14c 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 14.1.2.1.250328

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, including any operating system, integrated software, duplication, event 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 thirdparty content, products, or services, except as set forth in an applicable agreement between you and Oracle.

