

Oracle Identity Governance Bundle Patch Readme

This document is intended for users of OIM BUNDLE PATCH 12.2.1.4.200206. It contains the following sections:

 **Note:**

For issues documented after the release of OIM BUNDLE PATCH 12.2.1.4.200206, see My Oracle Support Document 2602696.1 at <https://support.oracle.com/>.

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

Understanding Bundle Patches

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

- [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.

Recommendations

Oracle has certified the dependent Middleware component patches for Identity Management products and recommends that you apply these certified patches. For

more information about these patches, see *Certification of Underlying or Shared Component Patches for Identity Management Products (Doc ID 2627261.1)* at <https://support.oracle.com>.

Bundle Patch Requirements

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

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



Note:

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

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

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

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

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

Then run the following command in OPatch inventory

```
opatch lsinventory
```

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

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

```
which opatch  
which unzip
```

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

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

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 OIM BUNDLE PATCH 12.2.1.4.200206 is done in the following stages:

 **Note:**

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

- [Patching the Oracle Binaries \(OPatch Stage\)](#)
- [Understanding the Process Sequence With an Example](#)

Patching the Oracle Binaries (OPatch Stage)

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

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

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

```
unzip -d PATCH_TOP p30864282_122140_Generic.zip
```

 **Note:**

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

Run the below command to unzip the file:

```
"c:\Program Files\7-Zip\7z.exe" x p30864282_122140_Generic.zip
```

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

```
cd PATCH_TOP/30864282
```

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.

Understanding the Process Sequence With an Example

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

1. Shutdown the Oracle Identity Governance, and ensure that the WebLogic Admin Server and SOA managed servers are running.
2. Run 'Opatch apply' on ORACLE_HOME_A. See [Patching the Oracle Binaries \(OPatch Stage\)](#) for more information.

3. Run 'Opatch apply' on ORACLE_HOME_B. See [Patching the Oracle Binaries \(OPatch Stage\)](#) for more information.
4. 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/30864282
```

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

```
opatch rollback -id 30864282
```

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 OIM BUNDLE PATCH 12.2.1.4.200206](#)
- [Postinstallation Configuration](#)
- [Updating Oracle Identity Governance Web Applications](#)

Installing a New Oracle Identity Governance Instance with OIM BUNDLE PATCH 12.2.1.4.200206

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

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

Using the Quickstart Installer

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

Note:

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

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

Note:

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

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

Using the Generic Installer

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

 **Note:**

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

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

 **Note:**

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

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

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.

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 reportees are displayed.

 **Note:**

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

Resolved Issues

The following section lists the issues resolved in OIM BUNDLE PATCH 12.2.1.4.200206:

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

Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200206

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

Table 1-1 Resolved Issues in OIM BUNDLE PATCH 12.2.1.4.200206

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

Known Issues and Workarounds

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

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

 **Note:**

Some known issues listed in the Release Notes for Oracle Identity Management may have been resolved by this Bundle Patch (OIM BUNDLE PATCH 12.2.1.4.200206). Compare the issues listed in [Resolved Issues](#) of this document when reviewing the *Release Notes for Oracle Identity Management*.

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

- [Errors Related to the For Reportees Feature](#)

Errors Related to the For Reportees Feature

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

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

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

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

Related Documents

For more information, see the following resources:

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Oracle® Fusion Middleware Oracle Identity Governance Bundle Patch Readme, OIM BUNDLE PATCH 12.2.1.4.200206
F25558-03

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

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

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

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

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

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

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

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

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